

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Алейник Станислав Николаевич
Должность: Ректор
Дата подписания: 08.04.2021 18:21:19
Уникальный программный ключ:
5258223550ea9fbeb23726a1609b644b33d8986ab6255891f288f913a1351fae

1

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени В.Я.ГОРИНА»

УТВЕРЖДАЮ

Декан инженерного факультета
профессор  С.В. Стребков

« 07 » 07 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки: 09.03.03 - Прикладная информатика

Направленность (профиль): Прикладная информатика в АПК

Квалификация: бакалавр

Год начала подготовки: 2020

Майский, 2020

Рабочая программа дисциплины (модуля) 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 19 сентября 2017 г. № 922;
- 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;
- профессионального стандарта «Специалист по информационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н
- профессионального стандарта «Системный аналитик», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 28 октября 2014 г. № 809н

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

Рассмотрена на заседании кафедры информатики и информационных технологий

« 18 » 06 2020 г., протокол № 13

И.о. зав. кафедрой  Е.В. Голованова

Руководитель основной профессиональной образовательной программы  В.А. Игнатенко

1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

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»; понятии 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 дисциплинам обязательной части Б1.О.23 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. Алгоритмизация и программирование
Требования к предварительной подготовке обучающихся	<p><i>знать:</i></p> <ul style="list-style-type: none"> ➤ основные понятия, используемые в информатике и программировании; ➤ элементарные методы математики, эконо-

	<p>мико-статистические методы исследования;</p> <ul style="list-style-type: none"> ➤ понятия системы и системного анализа; <p>уметь:</p> <ul style="list-style-type: none"> ➤ применять средства компьютерной техники, пакеты прикладных программ для решения прикладных задач; ➤ пользоваться сетевыми информационными ресурсами, работать с сетевыми службами и сервисами; <p>владеть:</p> <ul style="list-style-type: none"> ➤ навыками использования офисных прикладных программ и информационных ресурсов сети Интернет
--	--

Освоение дисциплины «Информационная безопасность» необходимо для изучения других дисциплин профессионального цикла, а также для выполнения ВКР.

III. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Коды компетенций	Формулировка компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности	Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности
			Уметь: использовать принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности
			Владеть: навыками использования принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности

		<p>ОПК-3.2 Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности</p>	<p>Знать: стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности</p> <p>Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности</p> <p>Владеть: навыками решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности</p>
		<p>ОПК-3.3 Демонстрирует навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Знать: подготовку обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p> <p>Уметь: демонстрировать навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p> <p>Владеть: навыками демонстрации навыков подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической докумен-	ОПК=4.3 Составляет техническую документацию с учетом действующих правовых	Знать: техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы

	тации, связанной с профессиональной деятельностью	норм на различных стадиях жизненного цикла информационной системы	Уметь: составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы
			Владеть: навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы

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

4.1. Распределение объема учебной работы по формам обучения

Вид работы (в соответствии с учебным планом)	Объем учебной работы, час	
	Очная	Заочная
Формы обучения (вносятся данные по реализуемым формам)		
Семестр изучения дисциплины	6	6
Общая трудоемкость, всего, час	216	216
<i>зачетные единицы</i>	6	6
1. Контактная работа		
1.1. Контактная аудиторная работа (всего)	82,4	27,6
В том числе:		
Лекции (<i>Лек</i>)	16	4
Лабораторные занятия (<i>Лаб</i>)	32	8
Практические занятия (<i>Пр</i>)	32	-
Установочные занятия (<i>УЗ</i>)	-	2
Предэкзаменационные консультации (<i>Конс</i>)	2	
Текущие консультации (<i>ТК</i>)	-	9
1.2. Промежуточная аттестация		
Зачет (<i>КЗ</i>)	-	-
Экзамен (<i>КЭ</i>)	0,4	0,4
Выполнение курсовой работы (проекта) (<i>КНKP</i>)	-	-
Выполнение контрольной работы (<i>ККН</i>)	-	0,2
1.3. Контактная внеаудиторная работа (контроль)	16	4
2. Самостоятельная работа обучающихся (всего)	117,6	188,4
в том числе:		
Самостоятельная работа по проработке лекционного материала	10	2
Самостоятельная работа по подготовке к лабораторно-практическим занятиям	35	4
Работа над темами (вопросами), вынесенными на самостоятельное изучение	40	145
Самостоятельная работа по видам индивидуальных заданий : подготовка реферата (контрольной работы)	20	20
Подготовка к экзамену	12,6	17,4

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-практич. занятия	Самостоятельная работа	Всего	Лекции	Лабораторно-практич. занятия	Самостоятельная работа
1	2	3	4	6	7	8	9	11
Модуль 1 «Составляющие, уровни обеспечения и угрозы ИБ»	65	4	22	39	66	-	4	62
1. Введение в ИБ и составляющие ИБ.	14	1	4	9	16,5	-	1	15,5
2. Формирование режима ИБ	16	1	6	9	16,5	-	1	15,5
3. Нормативно правовые основы ИБ в РФ. Стандарты ИБ.	16	1	6	9	16,5	-	1	15,5
4. Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ.	16	1	5	10	16,5	-	1	15,5
<i>Итоговое занятие по модулю 1</i>	3	-	1	2				
Модуль 2 «Вирусы и удаленные угрозы в сетях»	65	6	20	39	66	2	2	62
1. Вирусы как угроза ИБ. Классификация компьютерных вирусов.	14	1	4	9	16,5	0,5	0,5	15,5
2. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак.	14	1	4	9	16,5	0,5	0,5	15,5
3. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.	17	2	6	9	16,5	0,5	0,5	15,5
4. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях	17	2	5	10	16,5	0,5	0,5	15,5
<i>Итоговое занятие по модулю 2</i>	3		1	2				
Модуль 3 «Принципы и методы защиты в вычислительных сетях»	67,6	6	22	39,6	68,4	2	2	64,4
1. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях	15	2	4	9	16,5	0,5	0,5	15,5
2. Принципы защиты распределенных	17	2	6	9	16,5	0,5	0,5	15,5

Наименование модулей и разделов дисциплины	Объемы видов учебной работы по формам обучения, час							
	Очная форма обучения				Заочная форма обучения			
	Всего	Лекции	Лабораторно-практич. занятия	Самостоятельная работа	Всего	Лекции	Лабораторно-практич. занятия	Самостоятельная работа
1	2	3	4	6	7	8	9	11
вычислительных сетей. Идентификация и аутентификация.								
3. Криптография и шифрование. Методы разграничения доступа.	16,6	1	6	9,6	16,5	0,5	0,5	15,5
4. Регистрация и аудит. Межсетевое экранирование.	16	1	5	10	18,9	0,5	0,5	17,9
<i>Итоговое занятие по модулю 3</i>	3		1	2				
<i>Выполнение контрольной работы (ККН)</i>					0,2			
<i>Предэкзаменационные консультации</i>	2				-			
<i>Текущие консультации</i>	-				9			
<i>Установочные занятия</i>	-				2			
<i>Промежуточная аттестация</i>	0,4				0,4			
<i>Контроль</i>	16				4			
<i>Контактная аудиторная работа (всего)</i>	82,4	16	64	-	12	4	8	-
<i>Контактная внеаудиторная работа (всего)</i>	16				4			
<i>Самостоятельная работа (всего)</i>	117,6				188,4			
<i>Общая трудоемкость</i>	216				216			

4.3 Содержание дисциплины

Наименование и содержание модулей и разделов дисциплины
Модуль 1
«Составляющие, уровни обеспечения и угрозы ИБ»
1. Введение в ИБ и составляющие ИБ.
2. Формирование режима ИБ
3. Нормативно правовые основы ИБ в РФ. Стандарты ИБ.
4. Административный уровень обеспечения информационной безопасности. Классификация угроз ИБ.
<i>Итоговое занятие по модулю 1</i>
Модуль 2
«Вирусы и удаленные угрозы в сетях»
1. Вирусы как угроза ИБ. Классификация компьютерных вирусов.
2. Характеристика «вирусоподобных» программ. Антивирусные программные средства. Обнаружение и профилактика вирусных атак.
3. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных.
4. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях
<i>Итоговое занятие по модулю 2</i>
Модуль 3
«Принципы и методы защиты в вычислительных сетях»
1. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях
2. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация.
3. Криптография и шифрование. Методы разграничения доступа.
4. Регистрация и аудит. Межсетевое экранирование.
<i>Итоговое занятие по модулю 3</i>
<i>Подготовка реферата в форме презентации (контрольной работы)</i>
Зачет

**V. ОЦЕНКА ЗНАНИЙ И ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУ-
ЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

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

№ п/п	Наименование рейтингов, модулей и блоков	Формируемые компетенции	Объем учебной работы				Форма контроля знаний	Количество баллов (min)	Количество баллов (max)
			Общая трудоемкость	Лекции	Лабор.-практ. занятия	Самост. работа			
	Всего по дисциплине	<i>ОПК-2.3</i> <i>ОПК-3.1</i> <i>ОПК-3.2</i> <i>ОПК-3.3</i>	216	16	64	117,6	Зачет	51	100
	<i>I. Рубежный рейтинг</i>					Сумма баллов за модули	31	60	
	Модуль 1 «Информационные технологии. Виды и особенности примене- ния»	<i>ОПК-2.3</i> <i>ОПК-3.1</i> <i>ОПК-3.2</i> <i>ОПК-3.3</i>	65	4	22	39		10	20
1.	Введение в дисциплину. Направления развития информационных технологий и систем. Требования ГОС по специальности.		14	1	4	9	Устный опрос		
2.	Правовое регулирование информационной сферы. Государственные программы «Информационное общество» и «Цифровая экономика».		16	1	6	9	Устный опрос		
3.	Нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий		16	1	6	9	Устный опрос		
4.	Естественнонаучные, технические и гуманитарные знания в профессиональной деятельности.		16	1	5	10	Устный опрос		
	Итоговый контроль знаний по темам модуля 1		3	-	1	2	Устный опрос, тестирование		

Модуль 2. «Информационные системы и технологии. Интеграция и классификация информационных систем»		ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	65	6	20	39		10	20
1.	1. Рынок труда в сфере информационных технологий и информационных систем. Сценарий анализа карьеры и разработки личного плана развития.		14	1	4	9	Устный опрос		
2.	2. Система образования, повышения квалификации, сертификации специалистов в сфере информационных технологий и информационных систем.		14	1	4	9	Устный опрос		
3.	3. Основы организации презентаций профессиональных достижений и результатов работы.		17	2	6	9	Устный опрос		
4.	4. Поиск, анализ и использование электронных информационных ресурсов в профессиональной деятельности.		17	2	5	10	Устный опрос		
	Итоговый контроль знаний по темам модуля 2.		3		1	2	Устный опрос, тестирование		
Модуль 3 «Современные информационные системы. Автоматизация документооборота и организация совместной работы»		ОПК-2.3 ОПК-3.1 ОПК-3.2 ОПК-3.3	67,6	6	22	39,6		11	20
1.	1. Системы автоматизации документооборота (системы управления документооборотом)		15	2	4	9			
2.	2. Системы автоматизации делопроизводства и документооборота отечественных производителей		17	2	6	9			
3.	3. Системы групповой работы над документами (groupware)		16,6	1	6	9,6			
4.	4. Системы управления деловыми процессами (workflow management)		16	1	5	10			
	Итоговый контроль знаний по темам модуля 3.		3		1	2	Устный опрос, тестирование		
	II. Творческий рейтинг							2	5
	III. Рейтинг личностных качеств							3	10
	IV. Рейтинг сформированности прикладных практических требований							+	+
	V. Промежуточная аттестация							15	25

*Указана трудоемкость без учета внеаудиторной работы и промежуточной аттестации

5.2. Оценка знаний студента

5.2.1. Основные принципы рейтинговой оценки знаний

Оценка знаний по дисциплине осуществляется согласно Положению о балльно-рейтинговой системе оценки обучения в ФГБОУ Белгородского ГАУ.

Уровень развития компетенций оценивается с помощью рейтинговых баллов.

Рейтинги	Характеристика рейтингов	Максимум баллов
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
Рейтинг личностных качеств	Оценка личностных качеств обучающихся, проявленных ими в процессе реализации дисциплины (модуля) (дисциплинированность, посещаемость учебных занятий, сдача вовремя контрольных мероприятий, ответственность, инициатива и др.)	10
Рейтинг сформированности прикладных практических требований	Оценка результата сформированности практических навыков по дисциплине (модулю), определяемый преподавателем перед началом проведения промежуточной аттестации и оценивается как «зачтено» или «не зачтено».	+
Промежуточная аттестация	Является результатом аттестации на окончательном этапе изучения дисциплины по итогам сдачи зачета или экзамена. Отражает уровень освоения информационно-теоретического компонента в целом и основ практической деятельности в частности.	25
Итоговый 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	67,1-85 баллов	85,1-100 баллов

5.2.2. Критерии оценки знаний студента на экзамене

На экзамене студент отвечает в письменно-устной форме на вопросы экзаменационного билета (2 вопроса 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.

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.

6.2 Дополнительная литература

1. Миронов, А.Л. Информационная безопасность: Учебное пособие [Текст]/ А.Л. Миронов // Изд. Белгородского ГАУ, 2014. – 46 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

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

6.3.3. Печатные периодические издания

1. Журнал «Информационные технологии».
2. Журнал «Моделирование и анализ информационных систем».
3. Журнал «Information Security. Информационная безопасность».

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

1. Российское образование. Федеральный портал <http://www.edu.ru>
2. Национальный цифровой ресурс Руконт - межотраслевая электронная библиотека (ЭБС) на базе технологии Контекстум <http://rucont.ru>
3. Российская государственная библиотека <http://www.rsl.ru>
4. Сайт журнала «Information Security/Информационная безопасность» <http://www.itsec.ru>
5. Сайт «Информационная безопасность. Защита информации» <http://all-ib.ru/>

Вид учебных занятий	Организация деятельности студента
Лекция	<p>Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.</p>
Лабораторно-практические занятия	<p>Проработка рабочей программы, уделяя особое внимание целям и задачам структуре и содержанию дисциплины. Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом (методика полевого опыта), решение задач по алгоритму и решение ситуационных задач Прослушивание аудио- и видеозаписей по заданной теме.</p>
Самостоятельная работа	<p>Знакомство с электронной базой данных кафедры морфологии и физиологии, основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующих для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др. Решение ситуационных задач по своему индивидуальному варианту, в которых обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы. Тестирование - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний</p>

Вид учебных занятий	Организация деятельности студента
	и умений обучающегося. Контрольная работа - средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.
Подготовка к экзамену	При подготовке к экзамену необходимо ориентироваться на конспекты лекций, рекомендуемую литературу, полученные навыки по решению ситуационных задач

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1. Помещения, укомплектованные специализированной мебелью, оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории

Виды помещений	Оборудование и технические средства обучения
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель для обучающихся. Рабочее место преподавателя: стол, стул, кафедра-трибуна напольная, доска меловая настенная. Набор демонстрационного оборудования: Ноутбук, проектор, экран для демонстрации, 2 акустические колонки. Информационные стенды (планшеты настенные):
Учебная аудитория для проведения занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Специализированная мебель для обучающихся на 50 посадочных мест. Рабочее место преподавателя: стол, стул, кафедра-трибуна напольная, доска меловая настенная. Набор демонстрационного оборудования: - проектор; - экран для проектора; - 2 акустические колонки. Информационные стенды (планшеты настенные)
Помещения для самостоятельной работы обучающихся с возможностью подключения к Интернету и обеспечением доступа в электронную информационно-образовательную среду Белгородского ГАУ (читальные залы библиотеки)	Специализированная мебель; комплект компьютерной техники в сборе (системный блок: Asus P4BGL-MX\Intel Celeron, 1715 MHz\256 Мб PC2700 DDR SDRAM\ST320014A (20 Гб, 5400 RPM, Ultra-ATA/100)\ NEC CD-ROM CD-3002A\Intel(R) 82845G/GL/GE/PE/GV Graphics Controller, монитор: Proview 777(N) / 786(N) [17" CRT], клавиатура,

	мышь.) в количестве 10 единиц с возможностью подключения к сети Интернет и обеспечения доступа в электронную информационнообразовательную среду Белгородского ГАУ; настенный плазменный телевизор SAMSUNG PS50C450B1 Black HD (диагональ 127 см); аудиовидео кабель HDMI
Помещение для хранения и профилактического обслуживания учебного оборудования	Специализированная мебель: 3 стола, 2 полумягких стула, 3 тумбочки, 2 книжных шкафа, 1 шкаф платяной двухстворчатый, 1 сейф. Рабочее место лаборанта: компьютер (системный блок, монитор клавиатура мышь), МФУ BROTHER (принтер, сканер, ксерокс).

7.2. Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Виды помещений	Оборудование
Учебная аудитория для проведения занятий лекционного типа	MS Windows WinStrtr 7 Acdmc Legalization RUS OPL NL. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; MS Office Std 2010 RUS OPL NL Acdmc. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; Anti-virus Kaspersky Endpoint Security для бизнеса (Сублицензионный договор №28 от 08.11.2018) - 522 лицензия. Срок действия лицензии с 08.11.2018 по 08.11.2019
Учебная аудитория для проведения занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации №	MS Windows WinStrtr 7 Acdmc Legalization RUS OPL NL. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; MS Office Std 2010 RUS OPL NL Acdmc. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; Anti-virus Kaspersky Endpoint Security для бизнеса (Сублицензионный договор №28 от 08.11.2018) - 522 лицензия. Срок действия лицензии с 08.11.2018 по 08.11.2019
Помещения для самостоятельной работы обучающихся с возможностью подключения к Интернету и обеспечением доступа в электронную информационнообразовательную среду Белгородского ГАУ (читальные залы библиотеки)	Microsoft Imagine Premium Electronic Software Delivery. Сублицензионный договор №937/18 на передачу неисключительных прав от 16.11.2018. Срок действия лицензии- бессрочно. MS Office Std 2010 RUSOPLNL Acdmc. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно. Anti-virus Kaspersky Endpoint Security для бизнеса (Сублицензионный договор №28 от 08.11.2018).Срок действия лицензии с 08.11.2018 по 08.11.2019 Ин-

	формационно правовое обеспечение "Гарант" (для учебного процесса). Договор №ЭПС-12-119 от 01.09.2012. Срок действия - бессрочно. СПС КонсультантПлюс: Версия Проф. Консультант Финансист. КонсультантПлюс: Консультации для бюджетных организаций. Договор от 01.01.2017. Срок действия - бессрочно. RHVoice-v0.4-a2 синтезатор речи Программа Balabolka (portable) для чтения вслух текстовых файлов. Программа экранного доступа NDVA
Помещение для хранения и профилактического обслуживания учебного оборудования №	MS Windows WinStrtr 7 Acdmc Legalization RUS OPL NL. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; MS Office Std 2010 RUS OPL NL Acdmc. Договор №180 от 12.02.2011. Срок действия лицензии – бессрочно; Anti-virus Kaspersky Endpoint Security для бизнеса (Сублицензионный договор №28 от 08.11.2018) - 522 лицензия. Срок действия лицензии с 08.11.2018 по 08.11.2019

7.3. Электронные библиотечные системы и электронная информационно-образовательная среда

– ЭБС «ZNANIUM.COM», договор на оказание услуг № 0326100001919000019 с Обществом с ограниченной ответственностью «ЗНАНИУМ» от 11.12.2019

– ЭБС «AgriLib», лицензионный договор №ПДД 3/15 на предоставление доступа к электронно-библиотечной системе ФГБОУ ВПО РГАЗУ от 15.01.2015

– ЭБС «Лань», договор №27 с Обществом с ограниченной ответственностью «Издательство Лань» от 03.09.2019

– ЭБС «Рукопт», договор №ДС-284 от 15.01.2016 с открытым акционерным обществом «ЦКБ»БИБКОМ», с обществом с ограниченной ответственностью «Агентство «Книга-Сервис»;

VIII. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае обучения в университете инвалидов и лиц с ограниченными возможностями здоровья учитываются особенности психофизического развития, индивидуальные возможности и состояние здоровья таких обучающихся.

Образование обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах. Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья. Обучение инвалидов осуществляется также в со-

ответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с ограниченными возможностями здоровья по слуху возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий). На аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и (или) тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с ограниченными возможностями здоровья по зрению университетом обеспечивается выпуск и использование на учебных занятиях альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы) а также обеспечивает обучающихся надлежащими звуковыми средствами воспроизведения информации (диктофонов и т.д.). Допускается присутствие ассистента, оказывающего обучающемуся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата материально-технические условия университета обеспечивают возможность беспрепятственного доступа обучающихся в учебные помещения, а также пребывания в них (наличие пандусов, поручней, расширенных дверных проемов, лифтов; наличие специальных кресел и других приспособлений). На аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации лицам с ограниченными возможностями здоровья, имеющим нарушения опорно-двигательного аппарата могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬ-
НОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУ-
ДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени В.Я.ГОРИНА»**

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся
по дисциплине «Информационная безопасность»**

Направление подготовки: 09.03.03 - Прикладная информатика

Направленность (профиль): Прикладная информатика в АПК

Квалификация: бакалавр

Год начала подготовки: 2020

Майский, 2020

1. Перечень компетенций, соотнесенных с индикаторами достижения 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-3.1	Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности	Первый этап (пороговый уровень)	знать: основные требования информационной безопасности при решении стандартных задач профессиональной деятельности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету, реферат	
					тестовый контроль		
				Модуль 2.	устный опрос		итоговое тестирование, вопросы к зачету, реферат
					тестовый контроль		
		Второй этап (продвинутый уровень)	уметь: выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету, реферат	
					тестовый контроль		
				Модуль 2.	устный опрос		итоговое тестирование, вопросы к зачету, реферат
					тестовый контроль		
		Третий этап (высокий уровень)	владеть: навыками обеспечения безопасного использования	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету,	
					тестовый		

			информационно-коммуникационных технологий, применения способов и средств защиты информации		контроль	
				Модуль 2.	устный опрос	итоговое тестирование, вопросы к зачету
					тестовый контроль	
ОПК-3.2	Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом требований информационной безопасности	Первый этап (пороговый уровень)	знать: основные требования информационной безопасности при решении стандартных задач профессиональной деятельности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету, реферат
					тестовый контроль	
		Второй этап (продвинутый уровень)	уметь: выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Модуль 2.	устный опрос	итоговое тестирование, вопросы к зачету, реферат
					тестовый контроль	
		Третий этап (высокий уровень)	владеть: навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения способов и средств защиты информации	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету
					тестовый контроль	
ОПК-3.3	Демонстрирует навыки подготовки обзоров, аннотаций,	Первый этап (пороговый уровень)	знать: основные требования информационной безопасно-	Модуль 1.	устный опрос	итоговое тестирование, вопросы к зачету, реферат

	составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности		сти при решении стандартных задач профессиональной деятельности, способы решения задач обеспечения информационной безопасности, типовые средства и системы защиты информации		тестовый контроль				
				Модуль 2.	устный опрос		итоговое тестирование, вопросы к зачету, реферат		
		Второй этап (продвинутый уровень)	уметь: выявлять угрозы информационной безопасности, обосновывать и реализовывать организационно-технические мероприятия по защите информации в ИС, применять программные средства защиты информации.	Модуль 1.	тестовый контроль	устный опрос		итоговое тестирование, вопросы к зачету, реферат	
					Модуль 2.		тестовый контроль		устный опрос
				Третий этап (высокий уровень)		владеть: навыками обеспечения безопасного использования информационно-коммуникационных технологий, применения способов и средств защиты информации	Модуль 1.	тестовый контроль	
ОПК-4.3	Составляет техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	Первый этап (пороговой уровень)	знать: нормативно-правовые акты, регулирующие вопросы информационной безопасности, действующие правовые нормы по защите информации, учитываемые на различных стадиях жизненного цикла информационной системы	Модуль 1.	тестовый контроль	устный опрос	итоговое тестирование, вопросы к зачету, реферат		
					Модуль 2.			тестовый контроль	устный опрос
							тестовый контроль	устный опрос	

		Второй этап (продвину- тый уровень)	уметь: разрабатывать техниче- скую документацию на различных стадиях жиз- ненного цикла информа- ционной системы с учетом действующих правовых норм в области информа- ционной безопасности и защите информации.	Модуль 1.	устный опрос	итоговое тестиро- вание, вопросы к зачету, реферат
					тестовый контроль	
		Третий этап (высокий уровень)	владеть: навыками подготовки тех- нической документации на различных стадиях жиз- ненного цикла информа- ционной системы с учетом действующих правовых норм в области информа- ционной безопасности и защите информации.	Модуль 2.	устный опрос	итоговое тестиро- вание, вопросы к зачету, реферат
					тестовый контроль	
				Модуль 1.	устный опрос	итоговое тестиро- вание, вопросы к зачету,
					тестовый контроль	
				Модуль 2.	устный опрос	
					тестовый контроль	

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Компетен- ция	Планируемые резуль- таты обучения, соотне- сенные с индикаторами достижения компетен- ции (показатели до- стижения заданного уровня компетенции)	Уровни и критерии оценивания результатов обучения, шкалы оценивания			
		<i>Компетентность не сформирована</i>	<i>Пороговый уровень компетентности</i>	<i>Продвинутый уровень компетентности</i>	<i>Высокий уровень</i>
		<i>Не зачтено/ неудовле- творительно</i>	<i>Зачтено/ удовлетво- рительно</i>	<i>Зачтено/ хорошо</i>	<i>Зачтено/ отлично</i>
ОПК-3 Способен ре-	ОПК-3.1 Использует принципы, ме-	<i>Не способен использовать принципы, ме-</i>	<i>Частично способен использовать принципы,</i>	<i>Владеет способно- стью использовать</i>	<i>В совершенстве использует принципы,</i>

	ставления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	ления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	ций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	ций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.3 Составляет техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	<i>Не способен</i> составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	<i>Частично способен</i> составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	<i>Владеет способностью</i> составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	<i>В совершенстве</i> составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы требований информационной безопасности
Знать: техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	Не знает техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	Имеет не полные знания об технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	Знает навыки подготовки техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	Имеет четкие знания об навыках техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы	В совершенстве знает навыки техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы
Уметь: составлять техническую документацию с уче-	Не умеет составлять техническую документацию с учетом действующих правовых норм на различных стадиях жиз-	Допускает ошибки при составлении технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла ин-	Умеет составлять техническую документацию с учетом действующих правовых норм на различных стадиях жизненного цикла инфор-	Умеет правильно и эффективно составлять техническую документацию с учетом действующих правовых норм на различных стадиях	Уметь: составлять техническую документацию с учетом действующих правовых норм на различных

том действующих правовых норм на различных стадиях жизненного цикла информационной системы	женного цикла информационной системы	формационной системы и	мационной системы	жизненного цикла информационной системы	стадиях жизненного цикла информационной системы
<p>Владеть: навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Не владеет навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Не полностью владеет навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Владеет навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>Хорошо владеет навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>	<p>В совершенстве владеет навыками составления технической документации с учетом действующих правовых норм на различных стадиях жизненного цикла информационной системы и библиографии по научно-исследовательской работе с учетом требований информационной безопасности</p>

3. 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. Вопросы 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 надёжности: 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 надёжности 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. Оpozнaвание 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 защита 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.

3.1.3. Темы рефератов (примерные)

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.

3.2. 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

1.2.1. Тестовые задания

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

1. **информационная война**
2. информационное оружие
3. информационное превосходство

2. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. **конфиденциальность**
2. целостность
3. доступность
4. аутентичность
5. апеллируемость

4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано

1. **надежность**
2. точность
3. контролируемость
4. устойчивость
5. доступность

5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

1. принцип системности
2. принцип комплексности
3. принцип непрерывной защиты
4. принцип разумной достаточности
5. **принцип гибкости системы**
6. В классификацию вирусов по способу заражения входят
 1. опасные
 2. файловые
 3. **резидентные**
 4. загрузочные
 5. файлово -загрузочные
 6. **нерезидентные**
7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...
 1. **комплексное обеспечение ИБ**
 2. безопасность АС
 3. угроза ИБ
 4. атака на АС
 5. политика безопасности
 8. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
 1. компаньон - вирусами
 2. **черви**
 3. паразитические
 4. студенческие
 5. призраки
 6. стелс - вирусы
 7. макровирусы
 9. К видам системы обнаружения атак относятся :
 1. системы, обнаружения атаки на ОС
 2. системы, обнаружения атаки на конкретные приложения
 3. системы, обнаружения атаки на удаленных БД
 4. **все варианты верны**
 10. Автоматизированная система должна обеспечивать
 1. надежность
 2. **доступность**
 3. **целостность**
 4. контролируемость
 11. Основными компонентами парольной системы являются
 1. **интерфейс администратора**
 2. хранимая копия пароля
 3. **база данных учетных записей**
 4. все варианты верны
 12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это
 1. идентификатор пользователя
 2. **пароль пользователя**
 3. учетная запись пользователя

4. парольная система
13. К принципам информационной безопасности относятся
 1. скрытость
 2. масштабность
 3. **системность**
 4. **законность**
 5. **открытости алгоритмов**
14. К вирусам изменяющим среду обитания относятся:
 1. черви
 2. студенческие
 3. **полиморфные**
 4. спутники
15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...
 1. **Защита информации**
 2. Компьютерная безопасность
 3. Защищенность информации
 4. Безопасность данных
16. Система физической безопасности включает в себя следующие подсистемы:
 1. **оценка обстановки**
 2. скрытность
 3. **строительные препятствия**
 4. **аварийная и пожарная сигнализация**
17. Какие степени сложности устройства Вам известны
 1. упрощенные
 2. **простые**
 3. **сложные**
 4. оптические
 5. встроенные
18. К механическим системам защиты относятся:
 1. **проволока**
 2. **стена**
 3. сигнализация
 4. **вы**
19. Какие компоненты входят в комплекс защиты охраняемых объектов:
 1. **сигнализация**
 2. **охрана**
 3. **датчики**
 4. **телевизионная система**
20. К выполняемой функции защиты относится:
 1. внешняя защита
 2. внутренняя защита
 3. **все варианты верны**
21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
 1. Защита информации
 2. **Компьютерная безопасность**
 3. Защищенность информации
 4. Безопасность данных
22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:

1. информационная война
2. **информационное оружие**
3. информационное превосходство
23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
 1. государственная тайна
 2. **коммерческая тайна**
 3. банковская тайна
 4. конфиденциальная информация
24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
 1. конфиденциальность
 2. **целостность**
 3. доступность
 4. аутентичность
 5. апеллируемость
25. Гарантия точного и полного выполнения команд в АС:
 1. надежность
 2. **точность**
 3. контролируемость
 4. устойчивость
 5. доступность
26. Уровень 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, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
 1. Комплексное обеспечение информационной безопасности
 2. Безопасность АС
 3. Угроза информационной безопасности
 4. атака на автоматизированную систему
 5. **политика безопасности**
28. Особенности информационного оружия являются:
 1. системность
 2. открытость
 3. **универсальность**
 4. **скрытность**
29. К функциям информационной безопасности относятся:
 1. **совершенствование законодательства РФ в сфере обеспечения информационной безопасности**
 2. **выявление источников внутренних и внешних угроз**
 3. **Страхование информационных ресурсов**
 4. **защита государственных информационных ресурсов**
 5. **подготовка специалистов по обеспечению информационной безопасности**
30. К типам угроз безопасности парольных систем относятся
 1. словарная атака
 2. тотальный перебор

3. атака на основе психологии
4. разглашение параметров учетной записи
5. **все варианты ответа верны**
31. К вирусам не изменяющим среду обитания относятся:
 1. **черви**
 2. студенческие
 3. полиморфные
 4. **спутники**
32. Хранение паролей может осуществляться
 1. **в виде сверток**
 2. **в открытом виде**
 3. в закрытом виде
 4. **в зашифрованном виде**
 5. все варианты ответа верны
33. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
 1. ревизором
 2. иммунизатором
 3. **сканером**
 4. доктора и фаги
34. Выбрать недостатки имеющиеся у антивирусной программы ревизор:
 1. **неспособность поймать вирус в момент его появления в системе**
 2. **небольшая скорость поиска вирусов**
 3. **невозможность определить вирус в новых файлах (в электронной почте, на дискете)**
35. В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
 1. вирусы изменяющие среду обитания, но не распространяющиеся
 2. **вирусы изменяющие среду обитания при распространении**
 3. **вирусы не изменяющие среду обитания при распространении**
 4. вирусы не изменяющие среду обитания и не способные к распространению

в дальнейшем
36. К достоинствам технических средств защиты относятся:
 1. регулярный контроль
 2. **создание комплексных систем защиты**
 3. степень сложности устройства
 4. Все варианты верны
37. К тщательно контролируемым зонам относятся:
 1. **рабочее место администратора**
 2. **архив**
 3. **рабочее место пользователя**
38. К системам оповещения относятся:
 1. **инфракрасные датчики**
 2. **электрические датчики**
 3. электромеханические датчики
 4. электрохимические датчики
39. К оборонительным системам защиты относятся:
 1. **проволочные ограждения**
 2. **звуковые установки**
 3. датчики
 4. **световые установки**
40. Охранное освещение бывает:

- a. **дежурное**
- b. световое
- c. **тревожное**
- 41. К национальным интересам РФ в информационной сфере относятся:
 - 1. **Реализация конституционных прав на доступ к информации**
 - 2. Защита информации, обеспечивающей личную безопасность
 - 3. Защита независимости, суверенитета, государственной и территориальной целостности
 - 4. Политическая экономическая и социальная стабильность
 - 5. Сохранение и оздоровлении окружающей среды
- 42. Информационная безопасность это:
 - 1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
 - 2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
 - 3. Состояние, когда не угрожает опасность информационным системам
 - 4. Политика национальной безопасности России
- 43. Наиболее распространенные угрозы информационной безопасности:
 - 1. **угрозы целостности**
 - 2. угрозы защищенности
 - 3. угрозы безопасности
 - 4. **угрозы доступности**
 - 5. **угрозы конфиденциальности**
- 44. Что относится к классу информационных ресурсов:
 - 1. **Документы**
 - 2. **Персонал**
 - 3. **Организационные единицы**
 - 4. **Промышленные образцы, рецептуры и технологии**
 - 5. **Научный инструментарий**
- 45. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:
 - 1. **конфиденциальность**
 - 2. доступность
 - 3. аутентичность
 - 4. целостность
- 46. Устройства осуществляющие воздействие на человека путем передачи информации через вневещественное восприятие:
 - 1. Средства массовой информации
 - 2. Психотропные препараты
 - 3. Психотронные генераторы
 - 4. **Средства специального программно-технического воздействия**
- 47. Злонамеренные действия в нематериальной сфере могут быть подразделены на два класса, какие?
 - 1. **Информационный саботаж**
 - 2. **Физический саботаж**
 - 3. Информационные инфекции
- 48. Что не относится к информационной инфекции:
 - 1. Троянский конь
 - 2. **Фальсификация данных**
 - 3. Черви
 - 4. Вирусы
 - 5. Логическая бомба

49. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа
4. ***защита от утечки информации**

50. Идентификатор субъекта доступа, который является его секретом:

1. ***пароль**
2. ключ
3. электронно-цифровая подпись
4. сертификат ключа подписи

51. Исследование возможности расшифрования информации без знания ключей:

1. криптология
2. **криптоанализ**
3. взлом
4. несанкционированный доступ

52. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:

1. **Информационная безопасность**
2. Безопасность
3. Национальная безопасность
4. Защита информации

53. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации
5. **Безопасность данных**

54. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это:

1. Информационная война
2. **Информационное оружие**
3. Информационное превосходство

55. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:

1. Интересы государства
2. Интересы государства в информационной сфере
3. **Интересы личности**
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере

56. Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения, в преимущественное положение по сравнению с другими объектами:

1. Служебная информация
2. Коммерческая тайна
3. Банковская тайна
4. **Конфиденциальная информация**

57. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

1. Комплексное обеспечение информационной безопасности

2. Безопасность АС
3. Угроза информационной безопасности
4. **Атака на автоматизированную систему**
5. Политика безопасности
58. Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач
 1. **Информационные ресурсы**
 2. Информационная система
 3. Информационная сфера
 4. Информационные услуги
 5. Информационные продукты
59. К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан ...»
 1. **Информация без ограничения права доступа**
 2. Информация с ограниченным доступом
 3. Информация, распространение которой наносит вред интересам общества
 4. Объект интеллектуальной собственности
 5. Иная общедоступная информация
60. Состояние защищенности при котором не угрожает опасность это:
 1. Информационная безопасность
 2. ***Безопасность**
 3. Защита информации
 4. Национальная безопасность
61. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
 1. **Защита информации**
 2. Компьютерная безопасность
 3. Защищенность информации
 4. Защищенность потребителей информации
62. Особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств:
 1. **Информационная война**
 2. Информационное оружие
 3. Информационное превосходство
63. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности это:
 1. Интересы государства
 2. **Интересы государства в информационной сфере**
 3. Интересы личности
 4. Интересы личности в информационной сфере
 5. Интересы общества в информационной сфере
64. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
 1. Информационные ресурсы
 2. **Информационная система**
 3. Информационная сфера
 4. Информационные услуги

5. Информационные продукты
65. К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право...»
 1. Информация без ограничения права доступа
 2. Информация с ограниченным доступом
 3. Информация, распространение которой наносит вред интересам общества
 4. **Объект интеллектуальной собственности**
 5. Иная общедоступная информация
66. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:
 1. Информационная безопасность
 2. Безопасность
 3. Защита информации
 4. **Национальная безопасность**
67. Защита от случайных и преднамеренных воздействий, чреватых нанесением ущерба владельцам или пользователям информации это:
 1. Защита информации
 2. Компьютерная безопасность
 3. Защищенность информации
 4. **Защищенность потребителей информации**
68. Средства уничтожения, искажения, или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним это:
 1. Информационная война
 2. **Информационное оружие**
 3. Информационное превосходство
69. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:
 1. **Государственная тайна**
 2. Коммерческая тайна
 3. Банковская тайна
 4. Конфиденциальная информация
70. Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:
 1. Конфиденциальность
 2. Целостность
 3. **Доступность**
 4. Аутентичность
 5. Аппелируемость
71. Гарантия того, что в любой момент времени может быть произведена полноценная проверка любого компонента программного комплекса АС:
 1. Надежность
 2. Точность
 3. **Контролируемость**
 4. Устойчивость
 5. Доступность
72. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:
 1. Принцип системности
 2. Принцип комплексности
 3. **Принцип непрерывной защиты**
 4. Принцип разумной достаточности
 5. Принцип гибкости системы

73. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:
1. Комплексное обеспечение информационной безопасности
 2. Безопасность АС
 3. **Угрозы информационной безопасности**
 4. Атака на автоматизированную систему
 5. Политика безопасности
74. Совокупность информации, информационной структуры субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений
1. Информационные ресурсы
 2. Информационная система
 3. **Информационная сфера**
 4. Информационные услуги
 5. Информационные продукты
75. К какому уровню доступа информации относится следующая информация: «Ложная реклама, реклама со скрытыми вставками...»
1. Информация без ограничения права доступа
 2. Информация с ограниченным доступом
 3. **Информация, распространение которой наносит вред интересам общества**
 4. Объект интеллектуальной собственности
 5. Иная общедоступная информация
76. Защищенность страны от нападения извне, шпионажа, покушения на государственный и общественный строй:
1. Информационная безопасность
 2. Безопасность
 3. **Национальная безопасность**
 4. Защита информации
77. Защищенность от негативных информационно-психологических и информационно-технических воздействий:
1. Защита информации
 2. Компьютерная безопасность
 3. Защищенность информации
 4. **Защищенность потребителей информации**
78. Возможность сбора, обработки и распространения непрерывного потока информации при воспрепятствовании использованию информации противником это:
1. Информационная война
 2. Информационное оружие
 3. **Информационное превосходство**
79. Обобщение интересов личности в этой сфере, упрочнение демократии, создание правового государства это:
1. Интересы государства
 2. Интересы государства в информационной сфере
 3. Интересы личности в информационной сфере
 4. **Интересы общества**
 5. Интересы общества в информационной сфере
80. Защищаемые государством сведения в области военной, внешнеполитической и внешнеэкономической деятельности, распространение которых может нанести ущерб безопасности РФ.
1. **Государственная тайна**
 2. Коммерческая тайна
 3. Банковская тайна

4. Конфиденциальная информация
81. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор:
 1. Конфиденциальность
 2. Целостность
 3. Доступность
 4. **Аутентичность**
 5. Апеллируемость
82. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм АС будет вести себя так, как оговорено заранее:
 1. Надежность
 2. Точность
 3. Контролируемость
 4. **Устойчивость**
 5. Доступность
83. Согласование разнородных средств при построении целостной системы защиты, перекрывающий все существенные каналы реализации угроз и не содержащий слабых мест на стыках отдельных компонентов:
 1. Принцип системности
 2. **Принцип комплексности**
 3. Принцип непрерывной защиты
 4. Принцип разумной достаточности
 5. Принцип гибкости системы
84. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:
 1. Комплексное обеспечение информационной безопасности
 2. **Безопасность АС**
 3. Угроза информационной безопасности
 4. Атака на автоматизированную систему
 5. Политика безопасности
85. Действие субъектов по обеспечению пользователей информационными продуктами:
 1. Информационные ресурсы
 2. Информационная система
 3. Информационная сфера
 4. **Информационные услуги**
 5. Информационные продукты
86. К какому уровню доступа информации относится следующая информация: «Библиографические и опознавательные данные, личные характеристики, сведения о семейном положении, сведения об имущественном или финансовом состоянии...»
 1. Информация без ограничения права доступа
 2. **Информация с ограниченным доступом**
 3. Информация, распространение которой наносит вред интересам общества
 4. Объект интеллектуальной собственности
 5. Иная общедоступная информация
87. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов и требований:
 1. Защищенность информации
 2. **Защищаемая информация**
 3. Защищенность потребителей информации
 4. Защита информации

88. Действия предпринимаемые для достижения информационного превосходства в поддержке национальной информационной стратегии посредством воздействия на информацию и информационные системы противника:

1. **Информационная война**
2. Информационное оружие
3. Информационное превосходство

89. Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

1. Государственная тайна
2. Коммерческая тайна
3. **Банковская тайна**
4. Конфиденциальная информация

90. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно тот человек, который заявлен как ее автор и ни кто другой:

1. Конфиденциальность
2. Целостность
3. Доступность
4. Аутентичность
5. **Апеллируемость**

91. Системный подход к защите компьютерных систем предполагающий необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

1. **Принцип системности**
2. Принцип комплексности
3. Принцип непрерывной защиты
4. Принцип разумной достаточности
5. Принцип гибкости системы

92. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

1. **Комплексное обеспечение информационной безопасности**
2. Безопасность АС
3. Угроза безопасности
4. Атака на автоматизированную систему
5. Политика безопасности

93. Документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей:

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. **Информационные продукты**

94. К какому уровню доступа информации относится следующая информация: «Информация в области работ по хранению, перевозке, уничтожению химического оружия – сведения о состоянии здоровья граждан и объектов окружающей среды в районах размещения объектов по уничтожению химического оружия...»

1. Информация без ограничения права доступа
2. **Информация с ограниченным доступом**
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

95. Соотнесите интересы в области информационной безопасности:

1. **Национальные интересы**
2. Интересы личности
3. Интересы государства
4. Интересы общества

3.3. Третий этап (высокий уровень)

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

3.1. Ситуационные задачи

Задача 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

Задача 2

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

Задача 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.

Задача 4

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

Задача 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.

Задача 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.

Задача 7

При включении компьютера, находящегося в корпоративной сети, 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.

Задача 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.

Задача 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.

Задача 10

Разрабатывается информационная система, которая, в том числе, должна обеспе-

чить работу с информацией ограниченного доступа (коммерческой тайной). Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

Задача 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.

Задача 12

Пользователь получил сообщение от партнеров, зашифрованное. Как сообщалось в письме, алгоритмом BlowFish, хэш Naval. 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: bewdkbllvoJxe1laJmaqO1XMP5FvJeyrr5TV0OCzGvUNen6drkCOeiVeLbdstsUz5Pa9DJwI8FEiqVUDWdNT21BBEv+b

Задача 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.

Задача 14

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.

Задача 15

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

Пример экзаменационного билета

Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Белгородский государственный аграрный университет имени В.Я. Горина»
(ФГБОУ ВО Белгородский ГАУ)
Факультет инженерный
Кафедра информатики и информационных технологий

Экзаменационный билет № 1

Дисциплина **Информационная безопасность**
 по направлению 09.03.03 – Прикладная информатика
 направленность (профиль) – Прикладная информатика в АПК

1. Модель взаимодействия открытых систем OSI/ISO и проблемы ИБ..
2. Тест

Действующая государственная программа: 1) "Электронная Россия" 2) "Электронная среда"	Какой закон РФ дает определения информации, информационной технологии и информационной системы?
---	---

3) "Информационная среда" 4) "Информационное общество" 5) "Информационное государство"	1) «Об информации, информационных технологиях и о защите информации» 2) «Об информации, информационных технологиях и защите информации» 3) «Об информации, информационных технологиях и информационных системах» 4) «Об информационных технологиях»
Согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств, достаточный для построения вычислительной сети: 1) сетевая технология 2) интегрированная технология 3) универсальная технология 4) системная технология	Планируемое место РФ в международном рейтинге по индексу развития информационных технологий в 2020 году: 1) в числе 10 ведущих стран мира 2) в числе 15 ведущих стран мира 3) в числе 20 ведущих стран мира
Среда и метод общения человека с компьютером (совокупность приемов взаимодействия с компьютером): 1) пользовательский интерфейс 2) аппаратный интерфейс 3) программный интерфейс 4) буфер 5) шлюз	Корпоративные информационные системы (КИС) являются: 1) уникальными решениями, которые не могут быть тиражированы; 2) адаптируемыми, основанными на тиражных решениях разработчиков платформ; 3) имеют место оба подхода к созданию КИС.

3. Задача. 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

Преподаватель _____
 Эксперт _____

« ____ » _____ 202 ____ г.

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

Основными видами поэтапного контроля результатов обучения студентов являются: рубежный рейтинг, творческий рейтинг, рейтинг личностных качеств, рейтинг сформированности прикладных практических требований, промежуточная аттестация.

Уровень развития компетенций оценивается с помощью рейтинговых баллов.

Рейтинги	Характеристика рейтингов	Максимум баллов
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, <i>участие в различных конференциях и конкурсах на протяжении всего курса изучения дисциплины.</i>	5
Рейтинг личностных качеств	Оценка личностных качеств обучающихся, проявленных ими в процессе реализации дисциплины (модуля) (дисциплинированность, посещаемость учебных занятий, сдача вовремя контрольных мероприятий, ответственность, инициатива и др.)	10
Рейтинг сформированности прикладных практических требований	Оценка результата сформированности практических навыков по дисциплине (модулю), определяемый преподавателем перед началом проведения промежуточной аттестации и оценивается как «зачтено» или «не зачтено».	+
Промежуточная аттестация	<i>Является</i> результатом аттестации на окончательном этапе изучения дисциплины по итогам сдачи зачета или экзамена. Отражает уровень освоения информационно-теоретического компонента в целом и основ практической деятельности в частности.	25
Итоговый рейтинг	Определяется путём суммирования всех рейтингов	100

Общий рейтинг по дисциплине складывается из рубежного, творческого, рейтинга личностных качеств, рейтинга сформированности прикладных практических требований, промежуточной аттестации (экзамена или зачета).

Рубежный рейтинг – результат текущего 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.

Промежуточная аттестация – результат аттестации на окончательном этапе изучения дисциплины по итогам сдачи *зачета/ 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.

Рейтинг личностных качеств - оценка личностных качеств обучающихся, проявленных ими в процессе реализации дисциплины (модуля) (дисциплинированность, посещаемость учебных занятий, сдача вовремя контрольных мероприятий, ответственность, инициатива и др.

Рейтинг сформированности прикладных практических требований -

оценка результата сформированности практических навыков по дисциплине (модулю), определяемый преподавателем перед началом проведения промежуточной аттестации и оценивается как «зачтено» или «не зачтено».

В рамках балльно-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	67,1-85 баллов	85,1-100 баллов