Негосударственное частное некоммерческое
образовательное учреждение высшего образования
«Армавирский гуманитарно-социальный институт»

УТВЕРЖДАЮ:
Ректор НЧНОУ ВО «АГСИ»

Документ подписан электронной подписью
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 021CCAC2005AB11FBF4029C85F5CA97E72
Владелец: Токарь Александр Сергеевич
Действителен: с 22.04.2024 г. по 22.07.2025 г.

_____ А.С.Токарь

«24» июня 2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ Б1.В.ДВ.03.02 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки:
38.03.03 Управление персоналом
Направленность (профиль): Управление персоналом организации
Форма обучения: очная, заочная
(2023,2024 год набора)

Армавир, 2024

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Основы информационной безопасности» является формирование у обучающихся способности осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Цель изучения дисциплины «Основы информационной безопасности» достигается посредством решения в учебном процессе следующих **задач**:

- изучение основ риск-менеджмента в информационной безопасности;
- выявление угроз информации, исходящих от злоумышленников и вредоносных программ;
- использовать современный инструментарий и интеллектуальные информационно-аналитические системы защиты информации;
- изучение современных методов и средств защиты информации;
- умение собирать и анализировать информацию о источниках угроз, угрозах и уязвимостях информационных систем, с целью обеспечения их безопасности.

Воспитательной задачей является формирование российской гражданской идентичности, гражданской позиции активного и ответственного члена российского общества, осознающего свои конституционные права и обязанности, уважающего закон и правопорядок, обладающего чувством собственного достоинства, осознанно принимающего традиционные национальные и общечеловеческие гуманистические и демократические ценности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Основы информационной безопасности» относится к дисциплинам по выбору обязательной части блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы.

Дисциплина «Основы информационной безопасности» изучается в 8 семестре очной формы обучения, на 5 курсе заочной формы обучения, в 9 семестре очно-заочной формы обучения.

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

Код и наименование компетенции	**Наименование индикатора достижения компетенции**	**Планируемые результаты обучения, соотнесенные с индикаторами достижения компетенций**
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК 1.2. Применяет методы критического анализа и синтеза при работе с информацией, рассматривает и предлагает системные варианты для решения поставленных задач.	**Знать:** основные термины по проблематике информационной безопасности; **Уметь:** пользоваться нормативным актами и документами по защите информации; **Владеть:** навыками выявления и уничтожения компьютерных вирусов;

В результате освоения дисциплины обучающийся должен:

знать:

- о моральном аспекте информационной безопасности;

- о социальной значимости своей будущей профессии;
- о значении информации в развитии современного общества;

уметь:

- осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных норм;
- применять основные механизмы защиты информации на практике;
- применять достижения информационных технологий для защиты информации;

владеть:

- классификации информации;
- выделения объекта и предмета защиты в организации;
- основ построения модели нарушителя.

4. ОБЪЕМ ДИСЦИПЛИНЫ В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Очная форма обучения

Вид учебной работы	Всего часов	8 семестр
1.Контактная работа обучающихся с преподавателем:	**110.3**	**110.3**
Аудиторные занятия всего, в том числе:	104	104
Лекции	52	52
Лабораторные	-	
Практические занятия	52	52
Контактные часы на аттестацию (экзамен)	0,3	0.3
Консультация	4	4
Контроль самостоятельной работы	2	2
2. Самостоятельная работа	**105.7**	**105.7**
Контроль	36	36
ИТОГО:	**252**	**252**
Общая трудоемкость	**7**	**7**

Очно-заочная форма обучения

Вид учебной работы	Всего часов	9 семестр
1.Контактная работа обучающихся с преподавателем:	**74.3**	**74.3**
Аудиторные занятия всего, в том числе:	68	68
Лекции	34	34
Лабораторные	-	
Практические занятия	34	34
Контактные часы на аттестацию (экзамен)	0,3	0.3
Консультация	4	4
Контроль самостоятельной работы	2	2

2. Самостоятельная работа	**150.7**	**150.7**
Контроль	27	27
ИТОГО:	**252**	**252**
Общая трудоемкость	**7**	**7**

Заочная форма обучения

Вид учебной работы	Всего часов	5 курс
1.Контактная работа обучающихся с преподавателем:	**22.3**	**22.3**
Аудиторные занятия всего, в том числе:	16	16
Лекции	8	8
Лабораторные	-	
Практические занятия	8	8
Контактные часы на аттестацию (экзамен)	0,3	0.3
Консультация	4	4
Контроль самостоятельной работы	2	2
2. Самостоятельная работа	**220.7**	**220.7**
Контроль	9	9
ИТОГО:	**252**	**252**
Общая трудоемкость	**7**	**7**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование раздела (темы) дисциплины	Содержание раздела (темы разделов)	Индекс компетенции
Тема 1. Компьютерные преступления и их классификация.	Основные понятия и определения. Виды информации. Классификация компьютерных преступлений. Способы совершения компьютерных преступлений. Злоумышленники. Причины уязвимости сети Internet.	УК-1
Тема 2. Угрозы информации	Основные свойства информации. Угрозы информационной безопасности. Удаленные атаки на интрасети.	УК-1
Тема 3. Вредоносные программы и защита от них.	Признаки заражения компьютера вредоносными программами. Источники вредоносных программ. Методы обнаружения вредоносных программ. Антивирусные программы.	УК-1
Тема 4. Методы и средства защиты компьютерной информации.	Классификация мер безопасности компьютерных систем. Организационные методы, программно-технические методы и средства информационной безопасности.	УК-1

6. СТРУКТУРА ДИСЦИПЛИНЫ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

Очная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	12	-	12	26
Тема 2. Угрозы информации	12	-	12	26

Тема 3. Вредоносные программы и защита от них.	14	-	14	27
Тема 4. Методы и средства защиты компьютерной информации.	14	-	14	26.7
Итого (часов)	52		52	105.7
Форма контроля	экзамен			

Очно-заочная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	8	-	8	37
Тема 2. Угрозы информации	8	-	8	38
Тема 3. Вредоносные программы и защита от них.	8	-	8	38
Тема 4. Методы и средства защиты компьютерной информации.	10	-	10	37.7
Итого (часов)	34		34	150.7
Форма контроля	экзамен			

Заочная форма обучения

Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу (в часах)			
	Л	ЛР	ПЗ	СРС
Тема 1. Компьютерные преступления и их классификация.	2	-	2	55
Тема 2. Угрозы информации	2	-	2	55
Тема 3. Вредоносные программы и защита от них.	2	-	2	55
Тема 4. Методы и средства защиты компьютерной информации.	2	-	2	55.7
Итого (часов)	8		8	220.7
Форма контроля	экзамен			

7. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы и предполагает изучение литературных источников, выполнение домашних заданий и проведение исследований разного характера. Работа основывается на анализе литературных источников и материалов, публикуемых в интернете, а также реальных речевых и языковых фактов, личных наблюдений. Также самостоятельная работа включает подготовку и анализ материалов по темам пропущенных занятий.

Самостоятельная работа по дисциплине включает следующие виды деятельности:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, написание доклада, исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- самостоятельный поиск информации в Интернете и других источниках;
- выполнение домашней контрольной работы (решение заданий, выполнение упражнений);
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- написание рефератов;

- подготовка к тестированию;
- подготовка к практическим занятиям;
- подготовка к экзамену.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1 Основная литература:

1. Галатенко, В. А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / В. А. Галатенко. – 3-е изд. – Электрон. текстовые данные. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 266 с. – ISBN 978-5-4497-0675-1. – Режим доступа: http://www.iprbookshop.ru/97562.html. – ЭБС «IPRbooks», по паролю

2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: учебное пособие / А. Е. Фаронов. – 3-е изд. – Электрон. текстовые данные. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 154 с. – ISBN 978-5-4497-0338-5. – Режим доступа: http://www.iprbookshop.ru/89453.html. – ЭБС «IPRbooks», по паролю

3. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи [Электронный ресурс]: учебник / Б. И. Филиппов, О. Г. Шерстнева. – Электрон. текстовые данные. – Саратов: Ай Пи Эр Медиа, 2019. – 227 с. – ISBN 978-5-4486-0485-0. – Режим доступа: http://www.iprbookshop.ru/80290.html. – ЭБС «IPRbooks», по паролю

8.2.Дополнительная литература:

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]: учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. – 3-е изд. – Электрон. текстовые данные. – Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. – 431 с. – ISBN 978-5-4497-0935-6. – Режим доступа: https://www.iprbookshop.ru/102070.html. – ЭБС «IPRbooks», по паролю

2. Ревнивых, А. В. Информационная безопасность в организациях [Электронный ресурс]: учебное пособие / А. В. Ревнивых. – Электрон. текстовые данные. – Москва: Ай Пи Ар Медиа, 2021. – 83 с. – ISBN 978-5-4497-1164-9. – Режим доступа: https://www.iprbookshop.ru/108227.html. – ЭБС «IPRbooks», по паролю

3. Морозов, А. В. Информационное право и информационная безопасность. Часть 1 [Электронный ресурс]: учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. – Электрон. текстовые данные. – Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. – 436 с. – ISBN 978-5-00094-296-3. – Режим доступа: http://www.iprbookshop.ru/72395.html. – ЭБС «IPRbooks», по паролю

4. Морозов, А. В. Информационное право и информационная безопасность. Часть 2 [Электронный ресурс]: учебник для магистров и аспирантов / А. В. Морозов, Л. В. Филатова, Т. А. Полякова. – Электрон. текстовые данные. – Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. – 604 с. – ISBN 978-5-00094-297-0. – Режим доступа: http://www.iprbookshop.ru/66771.html. – ЭБС «IPRbooks», по паролю

5. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю. А. Семенов. – 3-е изд. – Электрон. текстовые данные. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 581 с. – ISBN 978-5-4497-0560-0. – Режим доступа: http://www.iprbookshop.ru/94863.html. – ЭБС «IPRbooks», по паролю

6. Суворова, Г. М. Информационная безопасность [Электронный ресурс]: учебное пособие / Г. М. Суворова. – Электрон. текстовые данные. – Саратов: Вузовское образование, 2019. – 214 c. – ISBN 978-5-4487-0585-4. – Режим доступа: http://www.iprbookshop.ru/86938.html. – ЭБС «IPRbooks», по паролю

7. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие / Ю. Н. Сычев. – Электрон. текстовые данные. – Саратов: Вузовское образование, 2018. – 195 c. – ISBN 978-5-4487-0128-3. – Режим доступа: http://www.iprbookshop.ru/72345.html. – ЭБС «IPRbooks», по паролю

8. Фомин, Д. В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения / Д. В. Фомин. – Электрон. текстовые данные. – Саратов: Вузовское образование, 2018. – 54 c. – ISBN 978-5-4487-0298-3. – Режим доступа: http://www.iprbookshop.ru/77320.html. – ЭБС «IPRbooks», по паролю

9. Формализация подхода к определению актуальности угроз информационной безопасности [Электронный ресурс]: монография / О. М. Голембиовская, М. Ю. Рытов, М. М. Голембиовский [и др.]. – Электрон. текстовые данные. – Саратов: Вузовское образование, 2022. – 147 c. – ISBN 978-5-4487-0840-4. – Режим доступа: https://www.iprbookshop.ru/121143.html. – ЭБС «IPRbooks», по паролю

10. Шилов, А. К. Управление информационной безопасностью [Электронный ресурс]: учебное пособие / А. К. Шилов. – Электрон. текстовые данные. – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. – 120 c. – ISBN 978-5-9275-2742-7. – Режим доступа: http://www.iprbookshop.ru/87643.html. – ЭБС «IPRbooks», по паролю

8.3 Лицензионное программное обеспечение

1.Windows 10 pro (договор № 7 от 02.03.2020 г)

2.Liber Office (free), Open Office.org (free).

3.Professional Edition,7Zip (free).

4. Google Chrome (free,).

5. Mozilla Firefox (free),

6.VLC player (видео плейер).

7.AIMP (аудио плейер) GIMP (Графический редактор).

8. K-Lite (кодеки для воспроизведения видео) Irfanview (просмотр фото) Adobe Flash Player.

9.Adobe Reader (просмотр PDF).

10.Система «Эдиторум» ЭБС-ВКР (договор № 0121/20180625 от 25.06.2018 г.) .

11. Программный продукт АСУ УЗ ‘Universys Web Server 5’ Лицензионный договор на использование программы для ЭВМ №13-П23-306 от 15.09.2023г.

12. КонсультантПлюс (договор от 01. 01.2016 г.

13. ЭПС «Система Гарант» договор № 12376/НК/2019 от 09.12.2019 г. Программа для ЭБС

14. IRRbooks. Лицензионный договор №11 506/24С от 08.04.2024г

8.4 Современные профессиональные базы данных и информационные справочные системы

1. Научная электронная библиотека www.elibrary.ru
2. Электронная библиотека по философии - http://www.filosof.historic.ru/
3. Российская государственная библиотека. - http://www.rsl.ru
4. Образовательные ресурсы федерального портала «Российское образование» http://www.edu.ru.
5. Электронно-библиотечная система IPRbooks- http://www.iprbookshop.ru.

6. Онлайн-справочник «Энциклопедия карьеры» - https://planetahr.ru/
7. Портал по вопросам управления персоналом- http://hrmaximum.ru/

Информационные справочные системы:

1. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru;
2. Информационно-правовой сервер «Гарант» http://www.garant.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Учебная аудитория для проведения: занятий лекционного типа, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 352905, Краснодарский край, г. Армавир, улица Урицкого, д. 117, помещение №7 (аудитория 6) общей площадью 25,8 кв.м.	**Учебная мебель:** - комплекты учебной мебели: стол на два посадочных места (6 шт.), стул ученический (12 шт.) - стол преподавателя (1 шт.) - кресло преподавателя (1 шт.) - доска классная (1 шт.) **Технические средства обучения:** набор демонстрационного оборудования: - мультимедиа проектор - компьютер (ноутбук) с подключением к сети «Интернет» и доступом к ЭИОС вуза, учебно-наглядные пособия, обеспечивающие тематические иллюстрации
Помещение для самостоятельной работы, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к ЭИОС вуза. 352905, Краснодарский край, г. Армавир, улица Тургенева, д. 147, 2 этаж, помещение №7 общей площадью 12,4 кв.м.	- комплекты учебной мебели; компьютерная техника с подключением к сети «Интернет» и доступом к ЭИОС вуза;
Помещение для хранения и профилактического обслуживания учебного оборудования 352905, Краснодарский край, г. Армавир, улица Урицкого, д. 117, помещение №7б общей площадью 3,5 кв.м.	Стеллажи, инвентарь, учебное оборудование

10.ОСОБЕННОСТИ ВЫПОЛНЕНИЯ ЗАДАНИЙ ОБУЧАЮЩИМИСЯ-ИНВАЛИДАМИ И ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (ПРИ НАЛИЧИИ)

Особые условия обучения и направления работы с инвалидами и лицами с ограниченными возможностями здоровья (далее обучающихся с ограниченными возможностями здоровья) определены на основании:

– Закона РФ от 29.12.2012г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Закона РФ от 24.11.1995г. № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

– Приказ Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

– методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса (утв. Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ограниченными возможностями здоровья понимаются условия обучения, воспитания и

развития таких обучающихся, включающие в себя использование адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания вуза и другие условия, без которых невозможно или затруднено освоение образовательных программ обучающимися с ограниченными возможностями здоровья.

В целях доступности изучения дисциплины инвалидами и обучающимися с ограниченными возможностями здоровья организацией обеспечивается:

1. Для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

−наличие альтернативной версии официального сайта организации в сети «Интернет» для слабовидящих:

−размещение в доступных для обучающихся, являющихся слепыми или слабовидящими, местах и в адаптированной форме (с учетом их особых потребностей) справочной информации (информация должна быть выполнена крупным рельефно-контрастным шрифтом (на белом или желтом фоне) и продублирована шрифтом Брайля);

−присутствие ассистента, оказывающего обучающемуся необходимую помощь:

−обеспечение выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

−обеспечение доступа обучающегося, являющегося слепым и использующего собаку-поводыря. к зданию организации;

2. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

−дублирование звуковой справочной информации визуальной (установка мониторов с возможностью трансляции субтитров (мониторы, их размеры и количество необходимо определять с учетом размеров помещения);

−обеспечение надлежащими звуковыми средствами воспроизведения информации:

3.Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата. Материально- технические условия обеспечивают возможность беспрепятственного доступа обучающихся в помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, локальное понижение стоек-барьеров, наличие специальных кресел и других приспособлений).

Обучение лиц организовано как инклюзивно, так и в отдельных группах.

11.ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

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

Этапы формирования компетенций в процессе освоения ОПОП прямо связаны с местом дисциплин в образовательной программе. Каждый этап формирования компетенции характеризуется определенными знаниями, умениями и навыками и (или) опытом профессиональной деятельности, которые оцениваются в процессе текущего контроля успеваемости, промежуточной аттестации по дисциплине (практике) и в процессе государственной итоговой аттестации.

Оценочные материалы включают в себя контрольные задания и (или) вопросы, которые могут быть предложены обучающемуся в рамках текущего контроля успеваемости и промежуточной аттестации по дисциплине. Указанные планируемые задания и (или) вопросы позволяют оценить достижение обучающимися планируемых результатов обучения по дисциплине, установленных в соответствующей рабочей программе дисциплины, а также сформированность компетенций, установленных в соответствующей

общей характеристике основной профессиональной образовательной программы.

На этапе текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине показателями оценивания уровня сформированности компетенций являются результаты устных и письменных опросов, написания рефератов, практических заданий, решения тестовых заданий.

Итоговая оценка сформированности компетенций определяется в период государственной итоговой аттестации.

Описание показателей и критериев оценивания компетенций

Показатели оценивания	Критерии оценивания компетенций	Шкала оценивания
Понимание смысла компетенции	Имеет базовые общие знания в рамках диапазона выделенных задач	Минимальный уровень
	Понимает факты, принципы, процессы, общие понятия в пределах области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию.	Базовый уровень
	Имеет фактические и теоретические знания в пределах области исследования с пониманием границ применимости	Высокий уровень
Освоение компетенции в рамках изучения дисциплины	Наличие основных умений, требуемых для выполнения простых задач. Способен применять только типичные, наиболее часто встречающиеся приемы по конкретной сформулированной (выделенной) задаче	Минимальный уровень
	Имеет диапазон практических умений, требуемых для решения определенных проблем в области исследования. В большинстве случаев способен выявить достоверные источники информации, обработать, анализировать информацию.	Базовый уровень
	Имеет широкий диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем. Способен выявлять проблемы и умеет находить способы решения, применяя современные методы и технологии.	Высокий уровень
Способность применять на практике знания, полученные в ходе изучения дисциплины	Способен работать при прямом наблюдении. Способен применять теоретические знания к решению конкретных задач.	Минимальный уровень
	Может взять на себя ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем. Затрудняется в решении сложных, неординарных проблем, не выделяет типичных ошибок и возможных сложностей при решении той или иной проблемы	Базовый уровень
	Способен контролировать работу, проводить оценку, совершенствовать действия работы. Умеет выбрать эффективный прием решения задач по возникающим проблемам.	Высокий уровень

1.2 Оценочные материалы для проведения текущего контроля

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (контролируемый индикатор достижения УК 1.2. Применяет методы критического анализа и синтеза при

работе с информацией, рассматривает и предлагает системные варианты для решения поставленных задач.)

Типовые задания, для оценки сформированности знаний

Результаты обучения
Знает основные термины по проблематике информационной безопасности;

Вопросы для устного опроса на практических занятиях

Тема 1. Компьютерные преступления и их классификация.

- Организация безопасного удаленного доступа к ЛВС предприятия.
- Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
- Автоматизация учета конфиденциальных документов на предприятии.
- Организация процессов мониторинга конфиденциального документооборота на предприятии.
- Автоматизация процесса проверок наличия конфиденциальных документов на предприятии.

Тема 2. Угрозы информации.

- Разработка комплексной системы защиты информации (КСЗИ) предприятия.
- Организация системы планирования и контроля функционирования КСЗИ на
- предприятии.
- Разработка основных направлений совершенствования КСЗИ предприятия.
- Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии.
- Разработка методологии проектирования КСЗИ.
- Разработка моделей процессов защиты информации при проектировании КСЗИ

Тема 3. Вредоносные программы и защита от них.

- Разработка проекта программно-аппаратной защиты информации предприятия.
- Разработка методов расчета экономической эффективности программно-аппаратной защиты информации предприятия.
- Криптографические средства защиты информации на основе дискретных носителей.
- Разработка игровой (дискретной) модели программно-аппаратной защиты информации предприятия.
- Разработка изолированной программно-аппаратной среды в Windows, Linux и т.д.
- Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
- Анализ нормативно-правовой базы по защите информации в сети Интернет. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет.

Тема 4 Методы и средства защиты компьютерной информации.

- Укажите основные отличия между современными и классическими блочными шифрами.
- Перечислите режимы работы ГОСТ 28147-89. Для чего служит каждый из данных режимов?
- Сравните DES и ГОСТ 28147-89.
- Сравните AES и ГОСТ 28147-89.
- Перечислите основные свойства хеш-функций.
- Чем хеширование отличается от выработки контрольных сумм?
- Чем хеширование отличается от выработки имитовставки?
- Укажите два подхода к построению функций хеширования

Критерии и шкала оценивания устного опроса

Оценка за ответ	Критерии

Отлично	выставляется обучающемуся, если: - теоретическое содержание курса освоено полностью, без пробелов; - исчерпывающее, последовательно, четко и логически излагает теоретический материал; - свободно справляется с решение задач, - использует в ответе дополнительный материал; - все задания, предусмотренные учебной программой выполнены; - анализирует полученные результаты; - проявляет самостоятельность при трактовке и обосновании выводов
Хорошо	выставляется обучающемуся, если: - теоретическое содержание курса освоено полностью; - необходимые практические компетенции в основном сформированы; - все предусмотренные программой обучения практические задания выполнены, но в них имеются ошибки и неточности; - при ответе на поставленный вопросы обучающийся не отвечает аргументировано и полно. - знает твердо лекционный материал, грамотно и по существу отвечает на основные понятия.
Удовлетворительно	выставляет обучающемуся, если: - теоретическое содержание курса освоено частично, но проблемы не носят существенного характера; - большинство предусмотренных учебной программой заданий выполнено, но допускаются не точности в определении формулировки; - наблюдается нарушение логической последовательности.
Неудовлетворительно	выставляет обучающемуся, если: - не знает значительной части программного материала; - допускает существенные ошибки; - так же не сформированы практические компетенции; - отказ от ответа или отсутствие ответа.

Тематика рефератов

1. Виды угроз безопасности информации.
2. Основные параметры системы защиты информации.
3. Распространение сигналов в технических каналах утечки информации.
4. Физические процессы подавления опасных сигналов.
5. Физические основы побочных электромагнитных излучений и наводок.
6. Защита информации в компьютерных системах от утечки по каналам ПЭМИН.
7. Основы защиты информации от фотографической и оптико-электронной разведок.
8. Основы защиты информации от радиотехнической разведки.
9. Процессы подавления опасных сигналов.
10. Основные определения и классификация радиоэлектронных помех.
11. Методы и средства инженерной защиты и технической охраны объектов.
12. Классификация и характеристика охранных, пожарно-охранных и пожарных извещателей.
13. Технические средства несанкционированного доступа к информации.
14. Направления обеспечения безопасности.
15. Аттестация объектов, лицензирование деятельности по защите информации и сертификации ее средств.
16. Особенности инструментального контроля эффективности инженерно-технической

защиты информации.

17. Классификация средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

18. Технические средства для тестирования и контроля систем обеспечения безопасности информации.

19. Принципы моделирования объектов защиты.

20. Стандартизация систем защиты информации.

Критерии оценивания выполнения реферата

Оценка	Критерии
Отлично	полностью раскрыта тема реферата; указаны точные названия и определения; правильно сформулированы понятия и категории; проанализированы и сделаны собственные выводы по выбранной теме; использовалась дополнительная литература и иные материалы и др.;
Хорошо	недостаточно полное, раскрытие темы; несущественные ошибки в определении понятий и категорий и т. п., кардинально не меняющих суть изложения; использование устаревшей литературы и других источников;
Удовлетворительно	реферат отражает общее направление изложения лекционного материала и материала современных учебников; наличие достаточного количества несущественных или одной-двух существенных ошибок в определении понятий и категорий и т. п.; использование устаревшей литературы и других источников; неспособность осветить проблематику дисциплины и др.;
Неудовлетворительно	тема реферата не раскрыта; большое количество существенных ошибок; отсутствие умений и навыков, обозначенных выше в качестве критериев выставления положительных оценок и др.

Тестовые задания

Тест № 1

1. Информация – это……

a. реквизит электронного документа, полученного в результате криптографического преобразования

b. данные, требующие защиты

c. сведения, независимо от формы их представления

2. Общедоступная информация – это …..

a. информация, доступ к которой не ограничен

b. информация, которая принадлежит общественной организации

c. информация, предназначенная для передачи по линиям связи, доступ к которой осуществляется с использованием средств вычислительной техники

3. Целостность информации – это …

a. документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

b. состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия

c. устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации

4. Персональные данные – это…

a. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

b. любая информация, которая хранится на персональном компьютере

c. любые сведения

5. Несанкционированный доступ к информации- это …

a. передача персональных данных на территорию иностранного государства органу власти иностранного государства

b. доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых

средствами вычислительной техники или автоматизированными системами

c. действия, в результате которых становится невозможным без использования

дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных

6. ФЗ №149 "Об информации, информационных технологиях и о защите информации" регулирует отношения:

a. связанные с обработкой персональных данных, осуществляемой федеральными

органами государственной власти, органами государственной власти субъектов

Российской Федерации, иными государственными органами

b. связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам

c. возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации.

7. Про какой руководящий документ идет речь:

«Настоящий руководящий документ устанавливает классификацию автоматизированных

систем, подлежащих защите от несанкционированного доступа к информации, и

требования по защите информации в автоматизированных системах различных классов»

a. РД «Защита от несанкционированного доступа к информации. Термины и

определения»

b. РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»

c. РД «Автоматизированные системы. Защита от несанкционированного доступа

к информации. Классификация автоматизированных систем и требования по

защите информации»

8. Согласно РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите

информации» устанавливается девять классов защищенности АС от НСД к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. Какие АС в себя включает первая группа?

a. в которых работает один пользователь, допущенный ко всей информации АС,

размещенной на носителях одного уровня конфиденциальности

b. многопользовательские АС, в которых одновременно обрабатывается и (или)

хранится информация разных уровней конфиденциальности

c. многопользовательские АС , в которых пользователи имеют одинаковые права

доступа (полномочия) ко всей информации АС

9. Расшифруйте аббревиатуру «РД ФСТЭК»

_____

_____

10. Область применения «ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»:

a. настоящий стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ

b. настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации

c. настоящий стандарт распространяется на испытания программных средств и их компонентов, цели которых - обнаружить в этих программных средствах и устранить из них компьютерные вирусы силами специальных предприятий (подразделений), и устанавливает общие требования к организации и проведению таких испытаний

Тест №2

1. Государственная тайна- это…

a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

b. сведения о сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам

c. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

2. Какие степени секретности бывают?

a. Важные, очень секретные, секретные

b. Особой важности, совершенно секретные, секретные

c. Совершенно важные, особо секретные, секретные

3. В соответствии со степенями секретности сведений, составляющих государственную тайну, устанавливаются три формы допуска первая, вторая, третья. Первая форма допуска:

a. для граждан, допускаемых к сведениям секретно

b. для граждан, допускаемых к сведениям совершенно секретно

c. для граждан, допускаемых к сведениям особой важности

4. Могут ли работать граждане, имеющие вторую форму допуска со сведениями «секретно»?_____

5. Перечислите не менее четырех органов безопасности РФ

1.

2.

3.

4.

6. Что означает допуск к сведениям составляющим государствую тайну?

a. процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

b. санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну

c. совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну,

и их осителей,

а также мероприятий, проводимых в этих целях

7. Укажите верную последовательность действий при оформлении допуска к государственной тайне

a. Отправка всех подготовленных документов и письменного обоснования о допуске в орган безопасности

b. Разработка номенклатуры должностей в режимно -секретном подразделении

c. Подготовка личных документов гражданина, на которого оформляется допуск

d. Знакомство гражданина с нормативной базой в области ГТ

8. Где проставляется отметка о допуске к ГТ

a. В анкете

b. В карточке

c. Нигде, в устной форме извещается гражданин

9. Какие документы необходимо подготовить гражданину, желающему получить допуск к ГТ

a. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы.

b. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы, все документы указанные в анкете, анкету

c. Документ удостоверяющий личность, медицинскую справку об отсутствии противопоказаний для работы, все документы указанные в анкете

10. Государственная тайна- это…

a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести

ущерб безопасности Российской Федерации

b. сведения о сферах деятельности государственных органов, доступ к которым

ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам

c. режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ,

услуг или получить иную коммерческую выгоду

Критерии оценивания образовательных достижений для тестовых заданий

Оценка	Коэффициент К (%)	Критерии оценки
Отлично	Свыше 80% правильных ответов	глубокое познание в освоенном материале
Хорошо	Свыше 70% правильных ответов	материал освоен полностью, без существенных ошибок
Удовлетворительно	Свыше 50% правильных ответов	материал освоен не полностью, имеются значительные пробелы в знаниях
Неудовлетворительно	Менее 50% правильных ответов	материал не освоен, знания обучающегося ниже базового уровня

11.3. Оценочные материалы для проведения промежуточной аттестации

Типовые задания, направленные на формирование профессиональных умений.

Результаты обучения

Результаты обучения
Умеет пользоваться нормативным актами и документами по защите информации;

Типовые задания для подготовки к экзамену

1. Дать определение информационной безопасности.
2. Какие виды компьютерных преступлений существуют?
3. Какие виды злоумышленников существуют?
4. В чем отличие злоумышленника от нарушителя?
5. Что входить в программно-аппаратные меры по защите информации?
6. Как на территории РФ законодательно регулируются вопросы по защите информации?
7. Цель защиты информации?
8. Что включает в себя экономическая безопасность компании?
9. Что такое кадровая безопасность?
10. Что входить в организационные меры по защите информации?
11. Методология построения и оценки СЗИ.
12. Дайте определение угрозы, актива, атаки, уязвимости. Обоснуйте их взаимосвязь.
13. Основные этапы атаки.
14. Определение нарушителя безопасности информации.
15. Инсайдер, работающий в интересах лица, находящегося вне информационной системы к какому типу нарушителей, относится?
16. Как описывается угроза безопасности информации в информационной системе?
17. Что содержит модель нарушителя безопасности информации?
18. Перечислите синонимы уязвимости, встречающиеся в нормативно-технических документах.
19. Назовите причины появления уязвимостей.
20. Какие существуют уровни (степени) опасности уязвимости?
21. Перечислить известные виды вредоносного программного обеспечения, дать краткое описание.
22. Описать способы заражения компьютера компьютерными вирусами?
23. Что такое программные и аппаратные закладки?
24. Классификация компьютерных вредоносных программ.
25. Методы обнаружения известных и неизвестных вирусов.
26. Профилактика заражению компьютеров вирусами.
27. Что такое сетевой червь, способы заражения и методы распространения?
28. Что такое программная уязвимость? Кем и как они могут быть использованы?
29. Как устроены и работают антивирусные программы? Какие существуют современные методы выявления вредоносных программ?
30. Что такое троянская программа, в чем отличие от программ шпионов?
31. Инженерно-техническое обеспечение компьютерной безопасности.
32. Что такое резервное копирование информации? Где и как применяется?
33. Организационное обеспечение компьютерной безопасности.
34. Политики компьютерной безопасности, инструкции, структуры политик.
35. Методы обеспечения безопасности операционных систем.
36. Безопасное использование и защита электронной почты.
37. Что такое межсетевой экран, принципы обеспечения безопасности с помощью МЭ?
38. Криптографические методы защиты компьютерной информации, плюсы и минусы.
39. Защиты информации в сети Интернет.

40. Что такое активный аудит информационной безопасности? Как, где и кем применяется?

Типовые практические задания, направленные на формирование профессиональных навыков, владений

Результаты обучения
Владеет навыками выявления и уничтожения компьютерных вирусов;

Типовые практические задания для подготовки к экзамену

Задание 1.

Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу. Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора

Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова? Ответ: согласно статьи №….

Задание 2.

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией. Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей.

Вопросы: – Какая статья УК РФ была нарушена? – Что послужило предметом преступления? – Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задание 3.

Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации.

Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задание 4.

Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Задание 5

Директор сельской школы Сорокоумова, историк по образованию, купила по безналичному расчёту для своих учеников 10 ПК IBM. При этом она, слабо разбираясь в технике, не осмотрела компьютеры, а поверила на слово продавцу, который расхваливал товар и не предоставил ей возможность получить соответствующую информацию о нём. При установке техники в школе специалисты выявили, что две машины разукомплектованы и в двух компьютерах разбиты экраны мониторов. Сорокоумова обратилась в магазин с просьбой заменить бракованные компьютеры, но там с ней отказались разговаривать. Она собрала необходимые документы и обратилась с иском в суд, утверждая, что при покупке компьютеров продавец не предоставил ей всю информацию о товаре. Правомерны ли действия Сорокоумовой и продавца компьютерной техники?

Задание 6.

Главный редактор журнала «Нефтяник» Щукин отказался публиковать решение Ступинского народного суда по гражданскому делу своего племянника - Антона Коробкина. Однако, когда председатель народного суда Рябинина потребовала, чтобы Щукин выполнил решение суда, содержащее прямое указание об опубликовании названного документа, главный редактор нехотя ответил: «Хорошо, мы опубликуем это решение, но за плату. Нашему журналу не на что жить». Рябинина возмутилась и пожаловалась на Щукина в Государственный комитет РФ по печати. Нарушен ли в этой ситуации закон?

Задание 7.

Вы руководитель фирмы Вам необходимо организовать процесс формирования «Перечня сведений конфиденциального характера». Опишите процесс организации.

Задание 8.

Вы руководитель фирмы Вам необходимо организовать конфиденциальное кадровое делопроизводство. Опишите процесс организации.

Задание 9.

Вы руководитель фирмы Вам необходимо организовать процесс осуществления защитных мер в отношении документопотоков. Опишите процесс организации.

Задание 10.

Вы руководитель фирмы и Вам необходимо организовать технологическую систему обработки конфиденциальных документов. Опишите процесс организации.

Задание 12.

Воспользуйтесь поиском для составления сводной таблицы документов, регламентирующих требования к информационной безопасности

2. Укажите, какие документы необходимо учитывать при проектировании защиты документации на электронном носителе.

3. Смоделируйте последовательность действий для защиты от копирования информации.

Задание 13.

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров - работники нотариальной конторы «ОКС» - внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации недвижимости за последний год и нарушена работа ПК. Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова. Есть ли в действиях Сальникова и Сабурова состав преступления?

Критерии оценивания практических заданий

Решения практического задания	Критерии оценивания
	«5» (отлично) – выставляется за полное, безошибочное выполнение задания
	«4» (хорошо) –в целом задание выполнено, имеются отдельные

	неточности или недостаточно полные ответы, не содержащие ошибок.
	«3» (удовлетворительно) – допущены отдельные ошибки при выполнении задания.
	«2» (неудовлетворительно) – отсутствуют ответы на большинство вопросов задачи, задание не выполнено или выполнено не верно.

Шкала оценки для проведения экзамена по дисциплине

Оценка за ответ	Критерии
Отлично	– полно раскрыто содержание материала; – материал изложен грамотно, в определенной логической последовательности; – продемонстрировано системное и глубокое знание программного материала; – точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; – ответ прозвучал самостоятельно, без наводящих вопросов; – продемонстрирована способность творчески применять знание теории к решению профессиональных задач; – продемонстрировано знание современной учебной и научной литературы; – допущены одна – две неточности при освещении второстепенных вопросов, которые исправляются по замечанию.
Хорошо	– вопросы излагаются систематизировано и последовательно; – продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; – продемонстрировано усвоение основной литературы. – ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.
Удовлетворительно	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – усвоены основные категории по рассматриваемому и дополнительным вопросам; – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; – при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации; – продемонстрировано усвоение основной литературы.
Неудовлетворительно	– не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов - не сформированы компетенции, умения и навыки, - отказ от ответа или отсутствие ответа

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ
рабочей программы дисциплины

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): ____

____

____

____

Заведующий кафедрой

____

(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): ____

____

____

____

Заведующий кафедрой

____

(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): ____

____

____

____

Заведующий кафедрой

____

(подпись, инициалы и фамилия)

Рабочая программа дисциплины рассмотрена на заседании кафедры (протокол от___________ №___) и одобрена на заседании Ученого совета (протокол от ____________ №____) для исполнения в 20__-20__ учебном году

Внесены дополнения (изменения): ____

____

____

Заведующий кафедрой

____

(подпись, инициалы и фамилия)
