ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПРИВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ»

Информационная безопасность

рабочая программа дисциплины (модуля)

Направление подготовки 09.03.03 Прикладная информатика
Направленность (профиль) Управление цифровой инфраструктурой организации

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Виды контроля в семестрах:

экзамены 7
курсовые работы 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	16 4/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Лабораторные	48	48	48	48
Конт. ч. на аттест.	1	1	1	1
Конт. ч. на аттест. в период ЭС	2,3	2,3	2,3	2,3
В том числе в форме практ.подготовки	82	82	82	82
Итого ауд.	64	64	64	64
Контактная работа	67,3	67,3	67,3	67,3
Сам. работа	124	124	124	124
Часы на контроль	24,7	24,7	24,7	24,7
Итого	216	216	216	216

Программу составил(и):
к.п.н., доцент, Додонов М.В.

Рабочая программа дисциплины
Информационная безопасность

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

составлена на основании учебного плана: 09.03.03-25-1-ПИб.plm.plx
Направление подготовки 09.03.03 Прикладная информатика Направленность (профиль) Управление цифровой инфраструктурой организации

Рабочая программа одобрена на заседании кафедры
Цифровые технологии

Зав. кафедрой Ефимова Т.Б.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью изучения дисциплины "Безопасность информационных технологий и систем" является формирование у обучаемых знаний, умений и навыков (уровня сформированности соответствующих компетенций) в результате последовательного изучения содержательно связанных между собой разделов (тем) учебных занятий, а также подготовить студентов к организации и эксплуатации средств защиты компьютерной информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.20

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2 Применяет методы защиты информации при выполнении задач профессиональной деятельности

ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы

ОПК-4.2 Оформлеет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	принципы и методы организации угроз, компьютерных атак и несанкционированного вторжения;
3.1.2	способы и средства защиты информации от утечки по техническим каналам;
3.1.3	
3.2	**Уметь:**
3.2.1	прогнозировать угрозы, обнаруживать атаки и вторжения, шифровать данные
3.2.2	оценивать коррупционные риски в части защиты информации на объектах информатизации
3.3	**Владеть:**
3.3.1	организационными,нормативно-правовыми, программными и техническими средствами защиты компьютерной информации
3.3.2	методами и средствами технической защиты информации на объектах информатизации
3.3.3	методами выявления проблем в организации технической защиты информации

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Примечание
	Раздел 1. Основные понятия и положения защиты информации в компьютерных системах			
1.1	Введение. Доктрина информационной безопасности России. Основные понятия и определения информационной безопасности. /Лек/	7	1	
1.2	Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Экономическая и информационная безопасность. Составляющие информационной безопасности. /Лек/	7	1	
1.3	Предмет и объект защиты. Угрозы безопасности информации в компьютерных системах. /Лек/	7	1	
1.4	Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. /Лек/	7	1	
1.5	Краткий обзор зарубежного законодательства в области информационной безопасности. Российское законодательство в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты. /Лаб/	7	2	Практическая подготовка
1.6	Основы законодательства в области обеспечения информационной безопасности /Лаб/	7	2	Практическая подготовка
	Раздел 2. Направления обеспечения информационной безопасности.			

2.1	Правовая защита. Организационная защита. Инженерно-техническая защита. /Лек/	7	2	
2.2	Программные средства защиты. Криптографические средства защиты. /Лаб/	7	2	Практическая подготовка
2.3	Хакерские утилиты и прочие вредоносные программы. Классические компьютерные вирусы. Скрипт-вирусы. Троянские программы. Сетевые черви. /Лаб/	7	2	Практическая подготовка
2.4	Обеспечение антивирусной защиты операционных систем на основе продуктов компании «Лаборатория Касперского». /Лаб/	7	4	Практическая подготовка
2.5	От чего надо защищаться в первую очередь? Как надо защищаться? Антивирусная защита. Современные средства биометрической идентификации. /Лаб/	7	4	Практическая подготовка
2.6	Идентификация и аутентификация. Парольная зашита. /Лаб/	7	4	Практическая подготовка
2.7	Классические методы шифрования. /Лаб/	7	2	Практическая подготовка
2.8	Изучение криптографического стандарта DES /Лаб/	7	4	Практическая подготовка
2.9	Изучение криптографического стандарта ГОСТ 28147-89 /Лаб/	7	4	Практическая подготовка
	Раздел 3. Построения системы информационной безопасности			
3.1	Основные аспекты построения системы информационной безопасности. Программа информационной безопасности. Модели ИБ, требования и основные этапы реализации информационной безопасности. /Лек/	7	2	
3.2	Мероприятия по защите информации. Политика информационной безопасности. /Лаб/	7	2	Практическая подготовка
3.3	Анализ и управление рисками при реализации информационной безопасности. Соотношение эффективности и рентабельности систем информационной безопасности. /Лаб/	7	2	Практическая подготовка
	Раздел 4. Защита информации в информационных системах и компьютерных сетях			
4.1	Определение защищенной информационной системы. Требования к архитектуре ИС для обеспечения безопасности ее функционирования. /Лек/	7	2	
4.2	Методология анализа защищенности информационной системы. Концепция защищенных виртуальных частных сетей. /Лаб/	7	2	Практическая подготовка
	Раздел 5. Защита информации от утечки по техническим каналам			
5.1	Способы защиты информации. Характеристика защитных действий. /Лаб/	7	2	Практическая подготовка
5.2	Защита информации от утечки по визуально-оптическим каналам. Защита информации от утечки по акустическим каналам. Защита информации от утечки по электромагнитным. Защита информации от утечки по материально-вещественным каналам. /Лаб/	7	2	Практическая подготовка
	Раздел 6. Противодействие несанкционированному доступу к источникам конфиденциальной информации			
6.1	Способы несанкционированного доступа. Технические средства несанкционированного доступа к информации. Защита от наблюдения и фотографирования. Защита от подслушивания. /Лек/	7	2	
6.2	Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра. /Лек/	7	2	
6.3	Защита от копирования. /Лаб/	7	2	Практическая подготовка
6.4	Передача зашифрованных сообщений по электронной почте /Лаб/	7	4	Практическая подготовка
	Раздел 7. Защита информации в электронных платежных системах			
7.1	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. /Лек/	7	2	
7.2	Персональный идентификационный номер. Универсальная электронная платежная система UEPS. Обеспечение безопасности электронных платежей через сеть Internet. /Лаб/	7	2	Практическая подготовка

	Раздел 8. Самостоятельная работа			
8.1	Подходы и методология оценки рисков информационной безопасности /Ср/	7	9	
8.2	Обеспечение безопасности электронных платежей через сеть Internet. /Ср/	7	4	
8.3	Особенности DoS и DDoS, характеристика атак. /Ср/	7	4	
8.4	Анализ уязвимостей в сетевой инфраструктуре предприятия /Ср/	7	4	
8.5	Разработка политики защиты информации в организации /Ср/	7	4	
8.6	Исследование методов обнаружения и предотвращения кибератак /Ср/	7	4	
8.7	Оценка эффективности механизмов шифрования данных /Ср/	7	4	
8.8	Аудит безопасности информационных систем и разработка рекомендаций по улучшению /Ср/	7	6	
8.9	Сравнительный анализ методов аутентификации и их применение в современных системах безопасности /Ср/	7	6	
8.10	Анализ угроз и уязвимостей в облачных вычислениях и разработка мер по защите данных /Ср/	7	6	
8.11	Тестирование системы мониторинга безопасности сетевого трафика /Ср/	7	6	
8.12	Подготовка к лекциям /Ср/	7	8	
8.13	Подготовка к лабораторным занятиям /Ср/	7	24	
8.14	Выполнение КР /Ср/	7	35	Практическая подготовка
	Раздел 9. Контактные часы на аттестацию			
9.1	Экзамен /КЭ/	7	2,3	
9.2	Курсовая работа /КА/	7	1	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Оценочные материалы для проведения промежуточной аттестации обучающихся приведены в приложении к рабочей программе дисциплины.

Формы и виды текущего контроля по дисциплине (модулю), виды заданий, критерии их оценивания, распределение баллов по видам текущего контроля разрабатываются преподавателем дисциплины с учетом ее специфики и доводятся до сведения обучающихся на первом учебном занятии.

Текущий контроль успеваемости осуществляется преподавателем дисциплины (модуля) в рамках контактной работы и самостоятельной работы обучающихся. Для фиксирования результатов текущего контроля может использоваться ЭИОС.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л1.1	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: чебник для вузов	Москва: Юрайт, 2021	tps://urait.ru/bcode/46986

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Внуков А. А.	Защита информации: учебное пособие для вузов	Москва: Юрайт, 2021	tps://urait.ru/bcode/47013

6.2 Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)

6.2.1 Перечень лицензионного и свободно распространяемого программного обеспечения

6.2.1.1	Операционная система Microsoft® Windows Professional 8 Russian Upgrade OLP NL Academic Edition Договор на поставку № 0342100004813000011 от года.
6.2.1.2	Microsoft Office 2013 Professional Договор № 0342100004814000045

6.2.2 Перечень профессиональных баз данных и информационных справочных систем

6.2.2.1	Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/
6.2.2.2	База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru
6.2.2.3	Портал для разработчиков электронной техники: http://www.espec.ws/
6.2.2.4	База данных «Библиотека программиста» https://proglib.io/
6.2.2.5	База данных «Отраслевой портал специалистов» http://www.connect-wit.ru/
6.2.2.6	Гарант.ру https://www.garant.ru/
6.2.2.7	КонсультантПлюс http://www.consultant.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Учебные аудитории для проведения занятий лекционного типа, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование для предоставления учебной информации большой аудитории и/или звукоусиливающее оборудование (стационарное или переносное).
7.2	Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения: мультимедийное оборудование и/или звукоусиливающее оборудование (стационарное или переносное)
7.3	Помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.
7.4	Помещения для хранения и профилактического обслуживания учебного оборудования

Приложение
к рабочей программе дисциплины

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационная безопасность

(наименование дисциплины (модуля)

Направление подготовки / специальность

09.03.03 Прикладная информатика

(код и наименование)

Направленность (профиль) / специализация

«Управление цифровой инфраструктурой организации»

(наименование)

Содержание

1. Пояснительная записка

Цель промежуточной аттестации – оценивание промежуточных и окончательных результатов обучения по дисциплине, обеспечивающих достижение планируемых результатов освоения образовательной программы.

Формы промежуточной аттестации: **экзамен, курсовая работа в 7 семестре.**

Перечень компетенций, формируемых в процессе освоения дисциплины

Код и наименование компетенции	Код индикатора достижения компетенции
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 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
	ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности
ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1 ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
	ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам

Результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные материалы
ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Обучающийся знает: знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Вопросы 11-19
	Обучающийся умеет: решать стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с	Задания 13-15

	учетом основных требований информационной безопасности	
	Обучающийся владеет: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Задания 16-20
ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности	Обучающийся знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации	Вопросы 1-10
	Обучающийся умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения	Задания 1-6
	Обучающийся владеет: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации	Задания 7-12
ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	Обучающийся знает: основные стандарты оформления технической документации на различных стадиях жизненного цикла	Вопросы 19-25
	Обучающийся умеет: применять стандарты оформления технической документации на различных стадиях жизненного цикла	
	Обучающийся владеет: методами выявления проблем в организации технической защиты информации	
ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	Обучающийся знает: основные стандарты оформления технической документации при выполнении задач профессиональной деятельности	Задания 21-23
	Обучающийся умеет: применять стандарты оформления технической документации при выполнении задач профессиональной деятельности	
	Обучающийся владеет: навыками составления технической документации	

Промежуточная аттестация (экзамен) проводится в одной из следующих форм:
1) ответ на билет, состоящий из теоретических вопросов и практических заданий;
2) выполнение заданий в ЭИОС Университета.

Промежуточная аттестация (Курсовая работа) проводится в одной из следующих форм:
1) Подготовка отчета по курсовой работе с загрузкой в ЭИОСУниверситета
2) исправление замечаний по отчету;
3) ответ, состоящий из теоретических вопросов и практических заданий по теме курсовой работе.

2. Типовые[1] контрольные задания или иные материалы для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих уровень сформированных компетенций

2.1 Типовые вопросы для оценки знаний образовательного результата

Проверяемый образовательный результат:

<table>
<tr><th>Код и наименование компетенции</th><th>Образовательный результат</th></tr>
<tr><td>ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности</td><td>Обучающийся знает: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации</td></tr>
<tr><td colspan="2">Вопросы:
1. Основы шифрования и алгоритма RSA
2. Сравнения по модулю и арифметика остатков
3. Алгоритм Эвклида
4. Расширенный алгоритм Эвклида
5. Разложение на множители
6. Алгоритм Ферма разложения на множители
7. Фундаментальное свойство простых чисел
8. Числа Кармайкла и тест Миллера
9. Числа Мерсенна. Числа Ферма
10. Решето Эратосфена</td></tr>
<tr><td>ОПК-3.1 Решает стандартные задачи профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</td><td>Обучающийся знает: знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</td></tr>
<tr><td colspan="2">Примерные вопросы:
11. Анализ уязвимостей системы
12. Классификация угроз информационной безопасности
13. Основные направления и методы реализации угроз
14. Неформальная модель нарушителя
15. Методы оценки уязвимости системы
16. Причины и виды утечки информации
17. Классификация каналов утечки информации
18. Технические каналы утечки информации
19. Информационные каналы утечки информации</td></tr>
<tr><td>ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы
ОПК-4.2 Оформлеет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам</td><td>Обучающийся знает: основные стандарты оформления технической документации на различных стадиях жизненного цикла тайны, нормативно-справочные документы; основные стандарты оформления технической документации при выполнении задач профессиональной деятельности</td></tr>
<tr><td colspan="2">Примерные вопросы:
20. Содержание антикоррупционных стандартов.
21. Обязанности государственных служащих в сфере противодействия коррупции
22. Ограничения
23. Запреты
24.Требования к служебному поведению
25. Ответственность за несоблюдение ограничений, запретов, обязанностей, установленных в целях противодействия коррупции</td></tr>
</table>

[1] Приводятся типовые вопросы и задания. Оценочные средства, предназначенные для проведения аттестационного мероприятия, хранятся на кафедре в достаточном для проведения оценочных процедур количестве вариантов. Оценочные средства подлежат актуализации с учетом развития науки, образования, культуры, экономики, техники, технологий и социальной сферы. Ответственность за нераспространение содержания оценочных средств среди обучающихся университета несут заведующий кафедрой и преподаватель – разработчик оценочных средств.

2.2 Типовые задания для оценки навыков образовательного результата

Проверяемый образовательный результат:

<table>
<tr><td>Код и наименование индикатора достижения компетенции</td><td>Образовательный результат</td></tr>
<tr><td>ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности</td><td>Обучающийся умеет: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения</td></tr>
<tr><td colspan="2">Задания:
1 Определение простых чисел
Задание: выбрать алгоритм факторизации и тест факторизации
Задание: Получить модуль числа и сформировать классы; показать приемами модальной арифметики корректную принадлежность результатов к классам
3 Китайская теорема об остатках
Задание: решить модальное уравнение
4. Тема «Вычисление символа Якоби»
Задание: решить представление числа, определить четность чисел и значение символа Якоби
5. Тема «Криптография с открытым ключом»
Задание: выбрать основание и модуль; сгенерировать закрытый ключ; провести факторизацию ключа; формировать открытый ключ-
6. Тема «Тест Соловэя-Штрассена»
Задание: вычислить «вероятностно-простое» свойство числа, вычислить символ Якоби и сделать заключение о результате теста</td></tr>
<tr><td>ОПК-3.2: Применяет методы защиты информации при выполнении задач профессиональной деятельности</td><td>Обучающийся владеет: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации</td></tr>
<tr><td colspan="2">Задания:
7. Тема «Метод квадратичного решета»
Задание: вычислить факторную базу, составить элементы решета
8. Тема «Криптография с открытым ключом»
Задание: решение НОД алгоритмом Евклида, шифрование/дешифрование сообщений
9. Тема «Факторизация методом Ферма»
Задание: факторизовать заданное число, оформить ход факторизации таблично.
10. Тема «Тест Миллера-Рабина»
Задание: подготовить предварительные данные для итераций метода, показать, что тест Миллера-Рабина эффективней, чем тест Ферма
11. Тема «Факторизация (p-1) – метод Полларда»
Задание: решить каноническое разложение числа на простые множители, выполнить НОД факторизации по Полларду
12 Тема «Криптографическая обработка блока текста»
Задание: выбрать блок текста; назначить символ-разделения блоков; указать на соизмеримость модуля кодировки и длины кодируемого блока</td></tr>
<tr><td>ОПК-4.1 Применяет стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы</td><td>Обучающийся умеет: применять стандарты оформления технической документации на различных стадиях жизненного цикла</td></tr>
<tr><td colspan="2">Задания:
13. Определите наиболее коррупционно ёмкие направления деятельности организации N.
14. Составьте Формализованное описание (карту) направлений деятельности организации N и составляющих их бизнес-процессов и подпроцессов. Карту рекомендуется дополнить результатами предварительного анализа возможных коррупционных правонарушений.
15. Предложите модель угроз информационной безопасности организации N, описывающую угрозы информационной безопасности для всех выделенных в организации типов объектов среды и на всех уровнях иерархии информационной инфраструктуры.</td></tr>
<tr><td>ОПК-4.1 Применяет стандарты оформления технической документации на различных</td><td>Обучающийся владеет: методами выявления проблем в организации технической защиты информации</td></tr>
</table>

стадиях жизненного цикла информационной системы	
Задания: 16. Тема Математическая модель канала акустической утечки информации. 17. Тема Математическая модель канала утечки информации применительно к техническим разведкам. 18. Тема Автоматизация процессов охраны. 19. Тема Система контроля и управления доступом. 20. Тема Принципы работы системы видеонаблюдения и ее проектирование.	
ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	Обучающийся умеет: применять стандарты оформления технической документации при выполнении задач профессиональной деятельности идентифицировать коррупционные риски в части защиты информации на объектах информатизации
Ситуационная задача На основе процессной модели представьте все направления деятельности организации N в форме бизнес-процессов. Идентифицируйте коррупционных риски путем выделения в каждом анализируемом бизнес-процессе критических точек и общего описания возможностей для реализации коррупционных рисков в каждой критической точке.	
ОПК-4.2 Оформляет техническую документацию при выполнении задач профессиональной деятельности согласно стандартам	Обучающийся владеет: навыками составления технической документации методами выявления проблем в организации технической защиты информации
Задания: 21. Тема Звукоизоляция помещений системы зашумления. 22. Тема Реализация защиты от утечки по цепям электропитания и заземления. 23. Тема Разработка основной документации по инженерно-технической защите информации.	

2.3. Перечень вопросов для подготовки обучающихся к промежуточной аттестации

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности. |
5. Понятие угрозы и характеристика угроз безопасности информации.
6. Несанкционированный доступ (НСД) к информации и его цели.
7. Способы НСД к информации.
8. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
9. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
10. Компьютерные вирусы и их классификация.
11. Антивирусные программы и их классификация.
12. Понятие защиты информации.
13. Информационная безопасность в условиях функционирования в России глобальных сетей. ,
14. Международные стандарты информационного обмена. t
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
16. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
17. Требования к безопасности компьютерных сетей в Российской Федерации.
18. Основные положения теории информационной безопасности корпоративных информационных систем (КИС). I
19. Краткая история создания глобальной информационной сети INTERNET.
20. Стек протоколов TCP/IP. i
21. Проблемы безопасности IP-сетей: варианты распространенных атак на IP-сети и основные причины, порождающие возможность атаки на 1P-сети.
22. Причины уязвимости сети Интернет и сетей, и компьютеров, имеющих выход в Интернет.
23. Модель корпоративной сети. I
24. Причины, способствующие атаке информации в корпоративных сетях.
25. Модель угроз и модель противодействия угрозам безопасности корпоративной сети.
26. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.

27. Концепция информационной безопасности в РФ.
28. Защита файлов и папок путем назначения пароля экранной зЬставке,
29. Способы ограничения доступа к информации в MSWord. ,
30. Способы ограничения доступа к информации в MSExcel. '
31. Работа с ключами реестра WindowsXP/7/Ю : создание предупреждающего окна перед входом в систему.
32. Работа с ключами реестра WindowsXP/7/lO: отключение контекстного меню на панели задач и рабочем столе (отключение меню правой кнопки).
33. Понятие браузера. Браузер InternetExplorer.
34. Защита электронной почты от спама.
35. Понятие Cookies. Группы Cookies.
36. Сертификаты безопасности и их виды.
37. Вопросы, на которые нужно ответить, прежде чем электронной почты.
38. Защита файлов и папок от изменения: только чтение.
39. Защита файлов и папок от изменения: скрытый.
40. Шифрование данных с помощью архиваторов WinRar и PkZip.

Примерные темы курсовой работы

1. Математическая модель канала акустической утечки информации.
2. Математическая модель канала утечки информации применительно к техническим разведкам.
3. Автоматизация процессов охраны.
4. Система контроля и управления доступом.
5. Принципы работы системы видеонаблюдения и ее проектирование безопасности.
6. Звукоизоляция помещений системы зашумления
7. Реализация защиты от утечки по цепям электропитания и заземления
8. Разработка основной документации по инженерно-технической защите информации

3. Методические материалы, определяющие процедуру и критерии оценивания сформированных компетенций при проведении промежуточной аттестации

Критерии формирования оценок по ответам на вопросы, выполнению тестовых заданий

- оценка **«отлично»** выставляется обучающемуся, если количество правильных ответов на вопросы составляет 100 – 90% от общего объёма заданных вопросов;

- оценка **«хорошо»** выставляется обучающемуся, если количество правильных ответов на вопросы – 89 – 76% от общего объёма заданных вопросов;

- оценка **«удовлетворительно»** выставляется обучающемуся, если количество правильных ответов на тестовые вопросы –75–60 % от общего объёма заданных вопросов;

- оценка **«неудовлетворительно»** выставляется обучающемуся, если количество правильных ответов – менее 60% от общего объёма заданных вопросов.

Критерии формирования оценок по результатам выполнения заданий

«Отлично/зачтено» – ставится за работу, выполненную полностью без ошибок и недочетов.

«Хорошо/зачтено» – ставится за работу, выполненную полностью, но при наличии в ней не более одной негрубой ошибки и одного недочета, не более трех недочетов.

«Удовлетворительно/зачтено» – ставится за работу, если обучающийся правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой ошибки и двух недочетов.

«Неудовлетворительно/не зачтено» – ставится за работу, если число ошибок и недочетов превысило норму для оценки «удовлетворительно» или правильно выполнено менее 2/3 всей работы.

Виды ошибок:

- *грубые ошибки: незнание основных понятий, правил, норм; незнание приемов решения задач; ошибки, показывающие неправильное понимание условия предложенного задания.*

- негрубые ошибки: неточности формулировок, определений; нерациональный выбор хода решения.

- недочеты: нерациональные приемы выполнения задания; отдельные погрешности в формулировке выводов; небрежное выполнение задания.

Критерии формирования оценок по экзамену

«Отлично» (5 баллов) – обучающийся демонстрирует знание всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; умение излагать программный материал с демонстрацией конкретных примеров. Свободное владение материалом должно характеризоваться логической ясностью и четким видением путей применения полученных знаний в практической деятельности, умением связать материал с другими отраслями знания.

«Хорошо» (4 балла) – обучающийся демонстрирует знания всех разделов изучаемой дисциплины: содержание базовых понятий и фундаментальных проблем; приобрел необходимые умения и навыки, освоил вопросы практического применения полученных знаний, не допустил фактических ошибок при ответе, достаточно последовательно и логично излагает теоретический материал, допуская лишь незначительные нарушения последовательности изложения и некоторые неточности. Таким образом данная оценка выставляется за правильный, но недостаточно полный ответ.

«Удовлетворительно» (3 балла) – обучающийся демонстрирует знание основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. Однако знание основных проблем курса не подкрепляются конкретными практическими примерами, не полностью раскрыта сущность вопросов, ответ недостаточно логичен и не всегда последователен, допущены ошибки и неточности.

«Неудовлетворительно» (0 баллов) – выставляется в том случае, когда обучающийся демонстрирует фрагментарные знания основных разделов программы изучаемого курса: его базовых понятий и фундаментальных проблем. У экзаменуемого слабо выражена способность к самостоятельному аналитическому мышлению, имеются затруднения в изложении материала, отсутствуют необходимые умения и навыки, допущены грубые ошибки и незнание терминологии, отказ отвечать на дополнительные вопросы, знание которых необходимо для получения положительной оценки.

Критерии формирования оценок по написанию и защите курсовой работы

«Отлично» (5 баллов) – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы, а также грамотно и исчерпывающе ответившие на все встречные вопросы преподавателя.

«Хорошо» (4 балла) – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями, в которой отражены все необходимые результаты проведенного анализа, сделаны обобщающие выводы и предложены рекомендации в соответствии с тематикой курсовой работы. При этом при ответах на вопросы преподавателя обучающийся допустил не более двух ошибок.

«Удовлетворительно» (3 балла) – получают обучающиеся, оформившие курсовую работу в соответствии с предъявляемыми требованиями. При этом при ответах на вопросы преподавателя обучающийся допустил более трёх ошибок.

«Неудовлетворительно» (0 баллов) – ставится за курсовую работу, если число ошибок и недочетов