МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ

(СамГУПС)

Филиал СамГУПС в г. Нижнем Новгороде

РАССМОТРЕНА
на заседании Ученого совета филиала
СамГУПС в г. Нижнем Новгороде
протокол от 22 июня 2021 г. № 3

УТВЕРЖДАЮ:
и.о. директора филиала
Н.Н. Маланичева
12 июля 2021 г.

Информационная безопасность

рабочая программа дисциплины

Специальность 38.05.01 Экономическая безопасность

Специализация: Экономико-правовое обеспечение экономической безопасности

Форма обучения: заочная

Нижний Новгород 2021

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

1.1. Цели и задачи дисциплины

Целями освоения учебной дисциплины являются:

- ознакомление студентов с содержательной стороной проблемы информационной безопасности как основной составляющей национальной безопасности;
- изучение возможных путей обеспечения информационной безопасности применительно к экономическим информационным системам.

При изучении дисциплины «Информационная безопасность» основное внимание акцентируется на понимании сущности информационной безопасности и основных принципах ее обеспечения.

1.2. Требования к уровню освоения дисциплины

В ходе освоения дисциплины у студента должны быть сформированы знания, умения и навыки, соотнесенные с планируемыми результатами освоения образовательной программы.

Компетенции, формируемые в процессе изучения дисциплины	**Планируемые результаты освоения дисциплины**
ПСК-3 способность организовать делопроизводственный процесс и документооборот на предприятии независимо от форм собственности, осуществлять ревизию и аудит делопроизводственного процесса, обучать сотрудников и обеспечивать внедрение современных методов и технических средства бумажного и электронного документооборота, самостоятельно осуществлять все делопроизводственные функции, обеспечивая информационную безопасность предприятия	**Знать:** 1) нормативно-методические основы делопроизводства и ДОУ; 2) классификацию документов организации, 3) требования к оформлению документов, основные положения и содержание актуальных действующих ГОСТов по делопроизводству и документоведению, структуру и особенности корпоративных систем электронного документооборота
	Уметь: 1) разрабатывать, формировать, корректировать основные документы кадрового делопроизводства предприятия; 2) использовать современные методы организации и сотрудников службы делопроизводства; 3) использовать современные методы совершенствования деятельности сотрудников службы делопроизводства;
	Владеть: 1) навыками организации делопроизводственного процесса и документооборота на предприятии, 2) навыками самостоятельного осуществления всех делопроизводственных функций, с обеспечением информационной безопасности предприятия, 3) навыками оптимизации деятельности службы делопроизводства

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Информационная безопасность» относится к базовой части Блока Б1 «Дисциплины (модули)» специализации и является обязательной для обучения.

Код дисциплины	Наименование дисциплины	Коды формируемых компетенций
Осваиваемая дисциплина		
Б1.Б.30.04	Информационная безопасность	ПСК – 3
Предшествующие дисциплины		
	Нет	
Дисциплины, осваиваемые параллельно		
Б1.Б.29.03	Правовое и техническое обеспечение делопроизводства	ПСК-3
Последующие дисциплины		
Б2.Б.04(Пд)	Производственная практика, преддипломная практика	ПСК-3
Б3.Б.01	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	ПСК-3

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделяемых на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

3.1. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

Вид учебной работы	Всего часов по учебному плану	Курс
		5
Общая трудоемкость дисциплины: - часов - зачетных единиц	 144 4	 144 4
Контактная работа обучающихся с преподавателем (всего), часов	10	10
из нее аудиторные занятия, всего	10	10
в т.ч. лекции	4	4
практические занятия	6	6
Промежуточная аттестация, часов по учебному плану	9	9
Самостоятельная работа	125	125
Виды промежуточного контроля	Экз	Экз
Текущий контроль (вид, количество)	К	К

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества

академических часов и видов учебных занятий

4.1. Темы и краткое содержание курса

Раздел 1.

Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации.

Раздел 2.

Информационная безопасность личности, общества и государства: социально-правовые аспекты. Право на информацию в системе гражданских прав личности. Возможные ограничения данного права. Массовая информация и информация ограниченного доступа.

Раздел 3.

Системный анализ угроз безопасности в компьютерных системах. Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты. Содержательная сущность защиты КС.

Раздел 4.

Общая характеристика средств и методов защиты информации. Основные принципы реализации систем защиты информации. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.

Раздел 5.

Организационно-правовое обеспечение защиты информации Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима.

Раздел 6.

Защита информации от утечки по техническим каналам. Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект.

Раздел 7.

Защита информации в компьютерных системах от несанкционированного доступа. Защита от несанкционированного изменения структуры компьютерной системы. Противодействие программным и аппаратным закладкам на этапах разработки и производства систем.

Раздел 8.

Криптографические методы защиты информации. Введение в криптологию. Исторический обзор. Криптография и

криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования.

Раздел 9.

Компьютерные вирусы и антивирусные программные средства. Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки как форма нарушения информационной безопасности.

Раздел 10.

Комплексная система защиты информации в компьютерных системах. Концепция комплексной системы защиты информации (КСЗИ). Математическая формализация, моделирование и этапы создания КСЗИ.

4.2. Распределение часов по темам и видам учебной работы

Разделы и темы	Всего часов по учебному плану	Виды учебных занятий		
		Аудиторные занятия, в том числе		СРС
		ЛК	ПЗ	
Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации.	14	1	1	12
Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Право на информацию в системе гражданских прав личности. Возможные ограничения данного права. Массовая информация и информация ограниченного доступа.	14	1	1	12
Раздел 3. Системный анализ угроз безопасности в компьютерных системах. Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты. Содержательная сущность защиты КС.	14	1	1	12
Раздел 4. Общая характеристика средств и методов защиты информации. Основные принципы реализации систем защиты информации. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.	14	1	1	12

Раздел 5. Организационно-правовое обеспечение защиты информации Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима.	13		1	12
Раздел 6. Защита информации от утечки по техническим каналам. Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект.	13		1	12
Раздел 7. Защита информации в компьютерных системах от несанкционированного доступа. Защита от несанкционированного изменения структуры компьютерной системы. Противодействие программным и аппаратным закладкам на этапах разработки и производства систем.	12			12
Раздел 8. Криптографические методы защиты информации. Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования.	13			13
Раздел 9. Компьютерные вирусы и антивирусные программные средства. Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки как форма нарушения информационной безопасности.	14			14
Раздел 10. Комплексная система защиты информации в компьютерных системах. Концепция комплексной системы защиты информации (КСЗИ). Математическая формализация, моделирование и этапы создания КСЗИ.	14			14
Экзамен	9			
Итого	144	4	6	125

4.3. Тематика практических занятий

Тема практического занятия	Количество часов
Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации.	1
Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Право на информацию в системе гражданских прав личности. Возможные ограничения данного права. Массовая информация и информация ограниченного доступа.	1
Раздел 3. Системный анализ угроз безопасности в компьютерных системах. Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты. Содержательная сущность защиты КС.	1
Раздел 4. Общая характеристика средств и методов защиты информации. Основные принципы реализации систем защиты информации. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.	1
Раздел 5. Организационно-правовое обеспечение защиты информации Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима.	1
Раздел 6. Защита информации от утечки по техническим каналам. Инженерно-технические средства и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект.	1
Всего	6

4.4. Тематика лабораторных работ занятий

Лабораторные работы учебным планом не предусмотрены.

4.5. Примерная тематика курсовых проектов (работ)

Курсовая работа не предусмотрена учебным планом.

4.6. Примерная тематика контрольных работ

1. Теоретические и концептуальные основы защиты информации.
2. Принципы защиты информации.
3. Цели и значение защиты информации.
4. Задачи защиты информации и функции по их реализации.
5. Виды, методы и средства защиты информации.
6. Кадровое и ресурсное обеспечение защиты информации.
7. Источники дестабилизирующего воздействия на информацию.
8. Понятие утечки информации, виды и причины утечки информации.
9. Каналы утечки информации ограниченного доступа.
10. Аналитическая работа по предотвращению утраты и утечки информации.
11. Современные подходы к понятию угрозы защищаемой информации.

12. Объекты защиты информации.
13. Структура системы защиты информации, назначение составных частей системы.
14. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.
15. Состав и классификация носителей защищаемой информации.
16. Понятие и назначение технологического обеспечения защиты информации.
17. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.
18. Полномочия руководства предприятия в области защиты информации.
19. Полномочия специальных комиссий по защите информации.
20. Полномочия пользователей защищаемой информации.
21. Сущность и значение комплексной системы защиты информации как формы организации деятельности по защите информации.
22. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.
23. Собственники и владельцы информации, отнесенной к служебной и профессиональной тайне.
24. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.
25. Правовые и организационные принципы отнесения информации к защищаемой.
26. Криминалистическая характеристика компьютерной преступности в России.
27. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.
28. Способы совершения компьютерных преступлений.
29. Модели безопасного подключения к Интернет.
30. Организация противодействия вредоносным программам.
31. Компьютерные преступления, получившие мировую известность.
32. Кардерство, как вид компьютерных преступлений.
33. Проблемы ОВД по расследованию компьютерных преступлений.
34. Государственные органы управления в области информационной безопасности, их права и обязанности.
35. Понятие «информационная война», виды и средства, применяемые в информационной войне.
36. Основные понятия классической криптографии.
37. Требования к криптосистемам.

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

5.1. Распределение часов по темам и видам самостоятельной работы

Разделы и темы	Всего часов по учебному плану	Вид работы
Раздел 1. Защита информации как объективная закономерность эволюции постиндустриального общества. Информация и ее роль в современном обществе. Эволюция информационных процессов и информационных отношений. Сущность и цели информатизации.	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой. Выполнение контрольных работ. Подготовка к промежуточной аттестации
Раздел 2. Информационная безопасность личности, общества и государства: социально-правовые аспекты. Право на информацию в системе гражданских прав личности. Возможные ограничения данного права. Массовая информация и информация ограниченного доступа.	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой. Выполнение контрольных работ. Подготовка к промежуточной аттестации
Раздел 3. Системный анализ угроз безопасности в компьютерных системах. Структурная и функциональная организация информационных компьютерных систем (КС). КС как объект защиты. Содержательная сущность защиты КС.	12	Самостоятельное изучение отдельных тем учебной литературы, решение типовых задач. Работа со справочной и специальной литературой. Выполнение контрольных работ. Подготовка к промежуточной аттестации
Раздел 4. Общая характеристика средств и методов защиты информации. Основные принципы реализации систем защиты информации. Модели безопасности. Уровни иерархии в обеспечении информационной безопасности.	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой, решение типовых задач. Выполнение контрольных работ. Подготовка к промежуточной аттестации
Раздел 5. Организационно-правовое обеспечение защиты информации. Организационные мероприятия по защите информации. Назначение и задачи служб безопасности. Организация работ на информационном объекте. Создание контрольно-пропускного режима.	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой. Подготовка к промежуточной аттестации
Раздел 6. Защита информации от утечки по техническим каналам. Инженерно-технические средства	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной

и системы охраны объектов. Охранная сигнализация. Телевизионные системы видеоконтроля. Идентификация и аутентификация лиц, допускаемых на объект.		и специальной литературой, решение типовых задач решение типовых задач. Подготовка к промежуточной аттестации
Раздел 7. Защита информации в компьютерных системах от несанкционированного доступа. Защита от несанкционированного изменения структуры компьютерной системы. Противодействие программным и аппаратным закладкам на этапах разработки и производства систем.	12	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой, решение типовых задач решение типовых задач. Подготовка к промежуточной аттестации
Раздел 8. Криптографические методы защиты информации. Введение в криптологию. Исторический обзор. Криптография и криптоанализ. Понятие криптостойкости системы защиты информации. Шифрование как метод криптографического преобразования.	13	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой, решение типовых задач решение типовых задач. Подготовка к промежуточной аттестации
Раздел 9. Компьютерные вирусы и антивирусные программные средства. Компьютерные вирусы как специальный класс саморепродуцирующихся вредительских программ. Вирусные атаки как форма нарушения информационной безопасности.	14	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой, решение типовых задач решение типовых задач. Подготовка к промежуточной аттестации
Раздел 10. Комплексная система защиты информации в компьютерных системах. Концепция комплексной системы защиты информации (КСЗИ). Математическая формализация, моделирование и этапы создания КСЗИ.	14	Самостоятельное изучение отдельных тем учебной литературы. Работа со справочной и специальной литературой, решение типовых задач решение типовых задач. Подготовка к промежуточной аттестации
ИТОГО	125	

5.2. Перечень учебно-методического обеспечения для самостоятельной работы студентов с указание места их нахождения

- учебная литература – библиотека филиала;
- методические рекомендации по контрольным работам - ФОС;

- методические рекомендации по самостоятельному изучению теоретического материала – сайт филиала.

6. Фонд оценочных средств

Состав фонда оценочных средств

Вид оценочных средств	Количество
Текущий контроль	
Контрольная работа	1
Курсовая работа (курсовой проект)	Учебным планом не предусмотрено
Промежуточный контроль	
Экзамен	1

Фонд оценочных средств представлен в приложении к рабочей программе

7. Перечень основной и дополнительной литературы

7.1. Основная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Петренко В. И.	Защита персональных данных в информационных системах: учебное пособие	Ставрополь: СКФУ, 2016. — 201 с. — режим доступа: https://e.lanbook.com/book/155246	Электронный ресурс
Л1.2	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: НГТУ, 2019. — 83 с. — режим доступа: https://e.lanbook.com/book/152227	Электронный ресурс
7.2. Дополнительная литература				
Л2.1	Крыжановский А. В.	Информационная безопасность: методические указания	Самара: ПГУТИ, 2018. — 38 с. — режим доступа: https://e.lanbook.com/book/182282	Электронный ресурс
Л2.2	Барановская Т.П. и др.	Информационные системы и технологии в экономике : учебник	М.: Финансы и статистика, 2005. – 416 с.	22

8. Перечень ресурсов информационно - телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. Официальный сайт филиала СамГУПС в г. Нижнем Новгороде
2. Электронно-библиотечные системы

9. Методические указания для обучающихся по освоению дисциплины

В процессе освоения дисциплины студенты должны посетить лекционные и практические занятия, участвовать в дискуссиях по

установленным темам, проводить самостоятельную работу, выполнить и защитить контрольную работу, сдать экзамен.

Указания для освоения теоретического и практического материала:

1. Обязательное посещение лекционных и практических занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.

3. При подготовке к практическим занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.

4. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, использовать рекомендованные ресурсы информационно - телекоммуникационной сети «интернет», а также использование библиотеки филиала для самостоятельной работы.

5. В рамках самостоятельной работы студент должен выполнить контрольную работу. Выполнение и защита контрольной работы являются непременным условием для допуска к экзамену. Во время выполнения контрольной работы можно получить групповые или индивидуальные консультации у преподавателя.

6. Подготовка к экзамену предполагает:

- изучение конспектов лекций;
- изучение рекомендуемой литературы;
- выполнение и защита контрольной работы.

10. Перечень информационных технологий, программного обеспечения и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине

Программное обеспечение для проведения лекций, демонстрации презентаций: Microsoft Office 2003 и выше.

Профессиональные базы данных, используемые для изучения дисциплины (свободный доступ)

Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» - http://window.edu.ru/catalog/?p_rubr=2.2.75.6

База данных «Информационная безопасность» Совета Безопасности РФ - http://www.scrf.gov.ru/security/information/

11. Описание материально - технической базы, необходимой для осуществления образовательного процесса по дисциплине

11.1. Требования к аудиториям (помещениям, кабинетам) для проведения занятий с указанием соответствующего оснащения

Учебная аудитория для проведения занятий лекционного типа - аудитория № 401. Специализированная мебель: столы ученические - 32 шт., стулья ученические - 64 шт., доска настенная - 1 шт., стол преподавателя - 1 шт., стул преподавателя - 1 шт. Технические средства обучения, служащие для представления учебной информации большой аудитории: переносной экран, переносной проектор, ноутбук. Учебно-наглядные пособия, обеспечивающие тематические иллюстрации, соответствующие программе учебной дисциплины - комплект презентаций (хранится на кафедре).

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации - Лаборатория Компьютерный класс № 2, аудитория № 411. Специализированная мебель: столы ученические - 25 шт., стулья ученические - 31 шт., доска настенная - 1 шт., стол преподавателя - 1 шт., стул преподавателя - 1 шт. Технические средства обучения: компьютеры - 17 шт., видеопанель - 1 шт. Microsoft Office Professional 2010. Mathcad 14.

11.2. Перечень лабораторного оборудования

Лабораторное оборудование не предусмотрено.

Приложение к рабочей программе

ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Перечень компетенций с указанием этапов их формирования в процессе освоения учебной дисциплины

1.1. Перечень компетенций

- способность организовать делопроизводственный процесс и документооборот на предприятии независимо от форм собственности, осуществлять ревизию и аудит делопроизводственного процесса, обучать сотрудников и обеспечивать внедрение современных методов и технических средства бумажного и электронного документооборота, самостоятельно осуществлять все делопроизводственные функции, обеспечивая информационную безопасность предприятия (ПСК-3).

1.2. Этапы формирования компетенций в процессе освоения учебной дисциплины

Наименование этапа	**Содержание этапа (виды учебной работы)**	**Коды формируемых на этапе компетенций**
Этап 1. Формирование теоретической базы знаний	Лекции, самостоятельная работа студентов с теоретической базой, практические занятия	ПСК-3
Этап 2. Формирование умений	Практические занятия	ПСК-3
Этап 3. Формирование навыков практического использования знаний и умений	Выполнение контрольной работы	ПСК-3
Этап 4. Проверка усвоенного материала	Защита контрольной работы, экзамен	ПСК-3

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

2.1. Показатели и критерии оценивания компетенций на различных этапах их формирования

Этап формирования компетенции	Код компетенции	Показатели оценивания компетенций	Критерии	Способы оценки

Этап 1. Формирование теоретической базы знаний	ПСК-3	- посещение лекционных занятий, практических занятий; - ведение конспекта лекций; - участие в обсуждении теоретических вопросов тем на каждом практическом занятии	- наличие конспекта лекций по всем темам, вынесенным на лекционное обсуждение; - активное участие студента в обсуждении теоретических вопросов;	устный ответ
Этап 2. Формирование умений (решение задачи по образцу)	ПСК-3	- выполнение практических заданий	- успешное самостоятельное выполнение практических заданий	отчет по практическому занятию
Этап 3. Формирование навыков практического использования знаний и умений	ПСК-3	- наличие правильно выполненных контрольных работ	- контрольная работа имеет положительную рецензию и допущены к защите	контрольные работы
Этап 4. Проверка усвоенного материала	ПСК-3	- успешная защита контрольной работы; -экзамен	- ответы на все вопросы по контрольной работе; - ответы на вопросы к экзамену	устный ответ

2.2. Критерии оценивания компетенций по уровню их сформированности

Код компетенции	Уровни сформированности компетенций		
	базовый	средний	высокий
ПСК-3	**Знать:** 1) нормативно-методические основы делопроизводства и ДОУ; **Уметь:** 1) разрабатывать, формировать, корректировать основные документы кадрового делопроизводства	**Знать:** 2) классификацию документов организации, **Уметь:** 2) использовать современные методы организации и сотрудников службы делопроизводства;	**Знать:** 3) требования к оформлению документов, основные положения и содержание актуальных действующих ГОСТов по делопроизводству и документоведению, структуру и особенности

Код компетенции	Уровни сформированности компетенций		
	базовый	средний	высокий
	предприятия; **Владеть:** 1) навыками организации делопроизводственного процесса и документооборота на предприятии,	**Владеть:** 2) навыками самостоятельного осуществления всех делопроизводственных функций, с обеспечением информационной безопасности предприятия,	корпоративных систем электронного документооборота **Уметь:** 3) использовать современные методы совершенствования деятельности сотрудников службы делопроизводства; **Владеть:** 3) навыками оптимизации деятельности службы делопроизводства

2.2. Шкалы оценивания формирования компетенций

а) Шкала оценивания экзамена

Шкала оценивания	Критерии оценивания
оценка **«отлично»**	Студент обладает глубокими и прочными знаниями программного материала; демонстрирует полное соответствие знаний, умений и навыков показателям и критериям оценивания компетенций на формируемом дисциплиной уровне. При ответе на два теоретических вопроса продемонстрировал исчерпывающее, последовательное и логически стройное изложение; правильно сформулировал понятия и закономерности по вопросам; использовал примеры из дополнительной литературы и практики; сделал вывод по излагаемому материалу. Решил задачу правильно.
оценка **«хорошо»**	Студент обладает достаточно полным знанием программного материала; демонстрирует полное соответствие знаний, умений и навыков показателям и критериям оценивания компетенций на формируемом дисциплиной уровне. Его ответ представляет грамотное изложение учебного материала по существу; отсутствуют существенные неточности в формулировании понятий; правильно применены теоретические положения, подтвержденные примерами; сделан вывод; два теоретических вопроса освещены полностью или один вопрос освещён полностью, а второй доводится до логического завершения при наводящих вопросах преподавателя. Решил задачу. При ответе на дополнительные вопросы допускает неточности.
оценка **«удовлетворительно»**	Теоретическое содержание дисциплины освоено частично, но проблемы не носят принципиального характера. Студент демонстрирует неполное соответствие знаний, умений и навыков показателям и критериям оценивания компетенций на формируемом дисциплиной уровне: допускаются значительные ошибки, проявляется отсутствие знаний по ряду вопросов. Один вопрос разобран полностью, второй начат, но не завершен до конца. Решил задачу на 50%. Затрудняется

	отвечать на дополнительные вопросы.
оценка **«неудовлетворительно»**	Студент не знает значительную часть программного материала; допустил существенные ошибки в процессе изложения; не умеет выделить главное и сделать вывод; приводит ошибочные определения; ни один вопрос не рассмотрен до конца, наводящие вопросы не помогают. Студент демонстрирует явную недостаточность или полное отсутствие знаний, умений и навыков на заданном уровне сформированности компетенции.

б) Шкала оценивания контрольных работ

Шкала оценивания	Критерии оценивания
Зачтено	Все теоретические вопросы раскрыто полностью, изложены логично и последовательно. Проведен анализ, систематизация и обобщение литературных источников. Задания решены правильно.
Незачтено	Теоретические вопросы не раскрыты или имеются серьезные ошибки и неточности при изложении ответа на вопросы. Правильно решены менее 50 % заданий.

3. Типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций

Код компетенции	Этапы формирования компетенции	Типовые задания (оценочные средства)
ПСК-3	Этап 1. Формирование теоретической базы знаний	- устный ответ
	Этап 2. Формирование умений (решение задачи по образцу)	- практическое занятие (методические рекомендации для проведения лабораторных работ и практических занятий)
	Этап 3. Формирование навыков практического использования знаний и умений	- контрольные работы: перечень тем и заданий по вариантам (методические рекомендации по СРС)
	Этап 4. Проверка усвоенного материала	вопросы к экзамену (приложение 1)

4. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков

Экзамен

Проводится в заданный срок, согласно графику учебного процесса. Экзамен проходит в форме собеседования по билетам, в которые включаются теоретические вопросы. При выставлении оценок учитывается уровень приобретенных компетенций студента. Аудиторное время, отведенное студенту, на подготовку – 30 мин.

Контрольная работа

Во внеаудиторное время студент самостоятельно выполняет контрольную работу по своему варианту. Контрольная работа – вид самостоятельной письменной работы, направленный на творческое освоение общепрофессиональных и профильных профессиональных дисциплин (модулей) и выработку соответствующих профессиональных компетенций.

Защита контрольной работы проходит в устной форме по вопросам, раскрываемым в контрольной работе. В ходе защиты контрольной работы студент должен дать обязательные ответы на следующие вопросы:

- обоснование актуальности выбранной темы;
- цель работы;
- задачи**,** решаемые в процессе написания контрольной работы;
- основные выводы по существу темы контрольной работы;
- характеристика основных источников, использованных при написании контрольной работы.

Перед выполнением контрольной работы студент прослушивает цикл лекций по дисциплине и участвует в практических занятиях. Студент должен изучить научную, учебную, нормативную и другую литературу. Отобрать необходимый материал; сформировать выводы и разработать конкретные рекомендации по решению поставленной цели и задачи.

Тематика контрольных работ:

1. Теоретические и концептуальные основы защиты информации.
2. Принципы защиты информации.
3. Цели и значение защиты информации.
4. Задачи защиты информации и функции по их реализации.
5. Виды, методы и средства защиты информации.
6. Кадровое и ресурсное обеспечение защиты информации.
7. Источники дестабилизирующего воздействия на информацию.
8. Понятие утечки информации, виды и причины утечки информации.
9. Каналы утечки информации ограниченного доступа.
10. Аналитическая работа по предотвращению утраты и утечки информации.
11. Современные подходы к понятию угрозы защищаемой информации.
12. Объекты защиты информации.
13. Структура системы защиты информации, назначение составных частей системы.
14. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.
15. Состав и классификация носителей защищаемой информации.
16. Понятие и назначение технологического обеспечения защиты информации.
17. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.
18. Полномочия руководства предприятия в области защиты информации.

19. Полномочия специальных комиссий по защите информации.
20. Полномочия пользователей защищаемой информации.
21. Сущность и значение комплексной системы защиты информации как формы организации деятельности по защите информации.
22. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.
23. Собственники и владельцы информации, отнесенной к служебной и профессиональной тайне.
24. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.
25. Правовые и организационные принципы отнесения информации к защищаемой.
26. Криминалистическая характеристика компьютерной преступности в России.
27. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.
28. Способы совершения компьютерных преступлений.
29. Модели безопасного подключения к Интернет.
30. Организация противодействия вредоносным программам.
31. Компьютерные преступления, получившие мировую известность.
32. Кардерство, как вид компьютерных преступлений.
33. Проблемы ОВД по расследованию компьютерных преступлений.
34. Государственные органы управления в области информационной безопасности, их права и обязанности.
35. Понятие «информационная война», виды и средства, применяемые в информационной войне.
36. Основные понятия классической криптографии.
37. Требования к криптосистемам.

Практические занятия

Практические занятия — метод репродуктивного обучения, обеспечивающий связь теории и практики, содействующий выработке у студентов умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы. Цель работ – привить навыки решения задач и сформировать экономическое мышление в области финансовой безопасности национальной экономики.

Приложение 1

Вопросы к экзамену

Вопросы для проверки уровня обученности «ЗНАТЬ»

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе. Информатизация и компьютеризация. Информационные ресурсы, продукты и услуги. Объективная необходимость и общественная потребность защиты информации.
3. Информационная безопасность личности, общества и государства. Массовая и конфиденциальная информация. Виды тайн.
4. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области. Информационное оружие, информационные войны и терроризм. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
5. Компьютерная система (КС) как объект защиты информации. Угрозы информационной безопасности в КС. Классификация угроз.
6. Общая характеристика случайных угроз информационной безопасности в КС.
7. Общая характеристика преднамеренных угроз информационной безопасности в КС.
8. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС. Политика безопасности.
9. Реализация угроз информационной безопасности в КС путем несанкционированного доступа (НСД). Классификация каналов НСД. Собирательный образ потенциального нарушителя.
10. Обобщенные модели системы защиты информации в КС. Одноуровневые, многоуровневые и многозвенные модели. Общая характеристика средств и методов защиты информации в КС.
11. Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
12. Необходимость правового регулирования в области защиты информации. Информация как объект права собственности. Правоотношения собственника, владельца и пользователя информационных ресурсов.
13. Отечественное законодательство в области информации и защиты информации.
14. Ответственность за правонарушения при работе с компьютерными системами.

15. Эксплуатационная надежность КС как источник возникновения случайных угроз информационной безопасности. Пути ее повышения. Резервирование технических средств. Программно-аппаратный контроль и тестирование.
16. Оптимизация взаимодействия пользователя с КС как средство предотвращения ошибочных операций случайного характера.
17. Помехоустойчивое кодирование. Избыточные коды для обнаружения и исправления случайных ошибок в работе КС.
18. Дублирование информации как средство парирования угроз безопасности в КС. Многоуровневое дублирование. Технология RAID.
19. Минимизация ущерба, наносимого КС авариями и стихийными бедствиями.
20. Система охраны объектов КС.
21. Общая характеристика технических каналов утечки информации в КС.
22. Методы и средства защиты информации в КС от утечки по каналам побочных электромагнитных излучений и наводок.
23. Средства противодействия подслушивания и дистанционному наблюдению.
24. Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
25. Идентификация и аутентификация субъектов доступа к ресурсам КС. Парольные методы и оценка их эффективности. Биометрические методы.

Вопросы для проверки уровня обученности «УМЕТЬ»

26. Использовать средства и методы разграничения доступа к ресурсам КС.
27. Использовать защиту программных средств КС от несанкционированного копирования и исследования.
28. Использовать защиту от несанкционированного изменения структуры КС в процессе эксплуатации.
29. Применять контроль целостности программ и данных в процессе эксплуатации КС.
30. Применять общие понятия и классификацию криптографических средств.
31. Использовать различные методы шифрования. Криптосткость. Шифрование с симметричным и несимметричным ключами.
32. Применять шифрование методом замены. Простая, полиалфавитная и многозначная замена.
33. Применять шифрование методом перестановки. Маршрутные перестановки. Поворотные решетки.
34. Применять аналитические методы шифрования.
35. Применять шифрование методом гаммирования.

36. Использовать системы шифрования с открытым ключом. Односторонние функции. Электронная цифровая подпись. Алгоритм шифрования RSA.

37. Использовать отечественные и зарубежные стандарты шифрования.

38. Давать общую характеристика и классифицировать компьютерные вирусы.

39. Распознавать механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.

40. Применять средства, используемые для обнаружения компьютерных вирусов.

41. Проводить профилактику заражения компьютерными вирусами.

42. Применять антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.

43. Использовать стандарты по защите информации? Охарактеризуйте отечественные нормативы и зарубежные стандарты в этой области.

44. Применять основные принципы и положения, реализующие системный подход к построению КСЗИ.

45. Применять функции защиты, механизмы защиты, уровень защищенности, управление защитой и другие базовые понятия, используемые при формировании КСЗИ.

46. Првводить общетеоретическую постановку задачи оптимизации КСЗИ на основе выбранного критерия эффективности защиты.

47. Применять основные технологические этапы разработки КСЗИ.

48. Использовать средства моделирования, применяемые для оптимизации КСЗИ.

49. Проводить организационно-технические мероприятия, в процессе эксплуатации КСЗИ.

50. Анализировать задачи, решаемые подсистемой аудита в составе защищенных КС.

Проверка уровня обученности «ВЛАДЕТЬ»

Студент должен владеть способностью решать задачи профессиональной деятельности в области информационной безопасности.