МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Председатель КСН

_____ В. В. Пленкина
«31» мая 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: **Цифровая безопасность в управлении персоналом**
направление подготовки: **38.04.03 Управление персоналом**
направленность (профиль)/специализация: **Администрирование, консалтинг и кадровый аудит в условиях цифровизации**
форма обучения: **очная**

Рабочая программа разработана в соответствии с утвержденным учебным планом от 27.05.2021г. и требованиями ОПОП 38.04.03 Управление персоналом, направленность (профиль) «Администрирование, консалтинг и кадровый аудит в условиях цифровизации» к результатам освоения дисциплины

Рабочая программа рассмотрена
на заседании кафедры Менеджмента в отраслях ТЭК

Протокол № 8 от «31» мая 2021 г.

Заведующий кафедрой МТЭК _____ В. В. Пленкина

СОГЛАСОВАНО:
Руководитель образовательной программы _____ Л. С. Ковальжина
«31» мая 2021 г.

Рабочую программу разработал:
А.В. Ходяев, заместитель начальника Службы информационно-управляющих систем и связи ООО «Газпром недра»

Л.С. Ковальжина, доцент кафедры менеджмента в отраслях ТЭК,
канд. социол. наук

1. Цели и задачи освоения дисциплины

Цель дисциплины – формирование целостной системы знаний о цифровой безопасности, свойствах защищаемой информации, основных информационных угрозах, направлениях защиты и возможностях построения стратегий информационной защиты, а также формирование практических навыков по использованию компьютерных систем, сетевых технологий и современных средств для обеспечения информационной безопасности.

Задачи дисциплины:

– сформировать представление об основных направлениях государственной политики в области информационной безопасности, обозначить актуальные нормативно-правовые документы, регулирующие деятельность по защите информации;

– показать свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность;

– раскрыть основное содержание, средства и методы используемых на практике или развиваемых направлений информационной безопасности, показать принципы, стратегии и модели защиты информации;

– показать наиболее распространенные цели, способы и мотивы совершения преступлений с использованием компьютерных технологий;

– подготовить обучающихся к дальнейшему изучению, освоению и участию в разработке проектов обеспечения информационной безопасности при использовании локальных и глобальных сетей в профессиональной деятельности.

Изучение дисциплины в должной степени служит целям формирования компетенций ОПК-1, ОПК-5.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к относится к обязательной части дисциплин учебного плана.

Необходимыми условиями для освоения дисциплины являются:

знание: видов и особенностей корпоративных информационных систем; правил работы с корпоративной информацией; технологий работы с цифровыми ресурсами в управлении персоналом.

умения: работать с цифровыми ресурсами в профессиональной деятельности; анализировать корпоративную информационную систему.

владение: навыками обработки данных, анализа корпоративных информационных систем.

Содержание дисциплины является логическим продолжением курса «Информационно-коммуникационные технологии современной организации», служит основой для освоения для подготовки ВКР и дальнейшей профессиональной деятельности.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
ОПК-1	ОПК-1.5 Использует знания управленческой, социологической, психологической теорий и права при разработке предложений внедрения цифровых	Знать: З1 - основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации
		Уметь: У1 – выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
	инструментов в управлении персоналом	результативность
		Владеть: В1 – навыками разработки предложений по совершенствованию мер цифровой безопасности
ОПК-5	ОПК-5.5 Использует технологии цифровой безопасности в профессиональной деятельности	Знать: З2 - средства и методы обеспечения информационной безопасности; принципы, стратегии и модели защиты информации
		Уметь: У2 - выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачетные единицы, 108 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
очная	2/4	10	10	-	88	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

- очная форма обучения

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Основы информационной безопасности	4	2	-	20	26	ОПК 1.5, ОПК 5.5	Тест
2	2	Цифровая безопасность и защита информации	2	4	-	12	18	ОПК 1.5, ОПК 5.5	Тест Задание
3	3	Особенности обеспечения информационной безопасности	4	4	-	20	28	ОПК 1.5, ОПК 5.5	Задание
4	Экзамен		-	-	-	36	36	ОПК 1.5, ОПК 5.5	Вопросы
Итого:			10	10	-	88	108	-	-

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Основы информационной безопасности

Тема 1.1 Информация и безопасность

Основные понятия информационной безопасности. Свойства информации как объекта защиты. Угрозы и виды мер обеспечения информационной безопасности.

Тема 1.2 Правовые и организационные основы обеспечения информационной безопасности

Правовые основы обеспечения информационной безопасности (законы РФ и другие нормативно-правовые документы). Уровни защиты информации. Основные организационные меры защиты информации.

Раздел 2. Цифровая безопасность и защита информации

Тема 2.1 Принципы, стратегии и модели защиты информации

Общие понятия о принципах информационной защиты. Содержание и обоснование основных принципов. Классификация и категории информационных нарушителей.

Тема 2.2 Персонал и цифровая безопасность

Основные информационные и компьютерные преступления. Регламентация процессов и действий персонала. Обязанности сотрудников по обеспечению информационной безопасности.

Раздел 3. Особенности обеспечения информационной безопасности

Тема 3.1 Основные механизмы и технологии защиты информации

Применение электронной цифровой подписи. Инструменты информационной безопасности операционной системы Windows. Человеческий фактор и защита информации.

Тема 3.2 Средств защиты информации

Использование средств защиты информации в пакете программ MS Office и другие. Политика безопасности для работы в сети Интернет. Особенности организации антивирусной защиты.

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час. ОФО	Тема лекции
1	1	2	Информация и безопасность
2		2	Правовые и организационные основы обеспечения информационной безопасности
3	2	1	Принципы, стратегии и модели защиты информации
4		1	Персонал и цифровая безопасность
5	3	2	Основные механизмы и технологии защиты информации
6		2	Средств защиты информации
Итого:		10	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час. ОФО	Тема практического занятия
1	1	1	Информация и безопасность
2		1	Правовые и организационные основы обеспечения информационной безопасности
3	2	2	Принципы, стратегии и модели защиты информации
4		2	Персонал и цифровая безопасность
5	3	2	Основные механизмы и технологии защиты информации
6		2	Средств защиты информации
Итого:		10	

Лабораторные работы

Лабораторные занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час. ОФО	Тема лекции	Вид СРС
1	1	10	Информация и безопасность	Подготовка к тесту
2		10	Правовые и организационные основы обеспечения информационной безопасности	Подготовка к тесту
3	2	6	Принципы, стратегии и модели защиты информации	Выполнение задания
4		6	Персонал и цифровая безопасность	Выполнение задания
5	3	10	Основные механизмы и технологии защиты информации	Выполнение заданий
6		10	Средств защиты информации	Выполнение задания
7		36	Экзамен	Подготовка к экзамену
Итого:		88		

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);
- работа в малых группах (практические занятия);
- разбор практических ситуаций (практические занятия);
- метод проектов (практические занятия).

6. Тематика курсовых работ

Курсовые работы не предусмотрены учебным планом

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1 текущая аттестация		
1	Выполнение задания	0-30
2	Тестирование	0-20
	ИТОГО за первую текущую аттестацию	0-50

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
2 текущая аттестация		
3	Выполнение задания	0-50
	ИТОГО за вторую текущую аттестацию	0-50
	ВСЕГО	**0-100**

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы

1. ТИУ «Полнотекстовая БД» на платформе ЭБС ООО «Издательство ЛАНЬ»
2. Ресурсы научно-технической библиотеки ФГБОУ ВО РГУ Нефти и газа (НИУ) им. И.М. Губкина.
3. Ресурсы научно-технической библиотеки ФГБОУ ВО УГНТУ.
4. Ресурсы научно-технической библиотеки ФГБОУ ВО «Ухтинский государственный технический университет».
5. Предоставление доступа к ЭБС от ООО «Электронное издательство ЮРАЙТ».
6. Предоставление доступа к ЭБС от ООО «ЭБС ЛАНЬ».
7. Электронно-библиотечная система IPRbooks с ООО «Ай Пи Эр Медиа».
8. Предоставление доступа к ЭБС от ООО «Политехресурс».
9. Предоставление доступа к ЭБС от ООО «ПРОСПЕКТ».
10. Предоставление доступа к ЭБС от ООО «РУНЭБ».

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

1. Microsoft Windows
2. Microsoft Office Professional Plus
3. Zoom (свободно-распространяемое ПО)
4. Skype (свободно-распространяемое ПО)

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

№ п/п	Перечень оборудования, необходимого для освоения дисциплины	Перечень технических средств обучения, необходимых для освоения дисциплины (демонстрационное оборудование)
1	Microsoft Windows, Microsoft Office Professional Plus, Zoom	Комплект мультимедийного оборудования: проектор, экран, компьютер, акустическая система. Локальная и корпоративная сеть. Учебная мебель: столы, стулья. Компьютер в комплекте, проектор. Учебно-наглядные пособия: раздаточный материал

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим занятиям.

На практических занятиях обучающиеся изучают методику и выполняют типовые расчеты и кейс-задачи. Для эффективной работы обучающиеся должны иметь калькуляторы и соответствующие канцелярские принадлежности. В процессе подготовки к практическим занятиям обучающиеся могут прибегать к консультациям преподавателя. Наличие конспекта лекций на практическом занятии обязательно.

Задания на выполнение типовых расчетов на практических занятиях обучающиеся получают индивидуально.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа обучающихся заключается в получении заданий (тем) у преподавателя для индивидуального освоения. Преподаватель на занятии дает рекомендации необходимые для освоения материала. В ходе самостоятельной работы обучающиеся изучить теоретический материал по разделам дисциплины и подготовить доклад по указанным темам. Обучающиеся должны понимать содержание выполненной работы (знать определения понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п.).

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

дисциплины: **Цифровая безопасность в управлении персоналом**

направление подготовки: **38.04.03 Управление персоналом**

направленность (профиль)/специализация: **Администрирование, консалтинг и кадровый аудит в условиях цифровизации**

Код компетенции	Код и наименование индикатора достижения компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ОПК-1	ОПК-1.5 Использует знания управленческой, социологической, психологической теорий и права при разработке предложений внедрения цифровых инструментов в управлении персоналом	Знать: З1 - основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации	Не знает основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации	Демонстрирует отдельные знания основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации	Знает основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации, допуская незначительные ошибки	Знает основных направлениях государственной политики в области информационной безопасности, актуальные нормативно-правовые документы, регулирующие деятельность по защите информации
		Уметь: У1 – выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность	Не умеет выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность	Умеет выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность, допуская значительные ошибки	Умеет выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность, допуская незначительные ошибки	Умеет выявлять свойства информации, определяющие выбор средств и методов информационной защиты и влияющих на ее результативность
		Владеть: В1 – навыками разработки предложений по совершенствованию мер цифровой безопасности	Не владеет навыками разработки предложений по совершенствованию мер цифровой безопасности	Владеет фрагментарными навыками разработки предложений по совершенствованию мер цифровой безопасности	Владеет навыками разработки предложений по совершенствованию мер цифровой безопасности, допуская незначительные ошибки	Владеет навыками разработки предложений по совершенствованию мер цифровой безопасности

Код компетенции	Код и наименование индикатора достижения компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ОПК-5	ОПК-5.5 Использует технологии цифровой безопасности в профессио-нальной деятельности	Знать: З2 - средства и методы обеспечения информационной безопасности; принципы, стратегии и модели защиты информации	Не знает средства и методы обеспечения информационной безопасности; принципы, стратегии и модели защиты информации	Демонстрирует отдельные знания средств и методов обеспечения информационной безопасности; принципов, стратегии и моделей защиты информации	Знает средства и методы обеспечения информационной безопасности; принципы, стратегии и модели защиты информации, допуская незначительные ошибки	Знает средства и методы обеспечения информационной безопасности; принципы, стратегии и модели защиты информации
		Уметь: У2 - выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором	Не умеет выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором	Умеет выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором, допуская значительные ошибки	Умеет выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором, допуская незначительные ошибки	Умеет выявлять слабые стороны цифровой безопасности предприятия, связанные с человеческим фактором

Приложение 2

КАРТА
обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина «Цифровая безопасность в управлении персоналом»
Код, направление подготовки/специальность 38.04.03 Управление персоналом
направленность (профиль)/специализация: Администрирование, консалтинг и кадровый аудит в условиях цифровизации

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Семейкин, А. Ю. Современные цифровые методы и системы в управлении безопасностью труда : монография / А. Ю. Семейкин. — Белгород : БГТУ им. В.Г. Шухова, 2020. — 88 с. https://e.lanbook.com/book/162033	ЭР	15	100	+
2	Управление персоналом : учебник и практикум для вузов / А. А. Литвинюк [и др.] ; под редакцией А. А. Литвинюка. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 461 с. https://urait.ru/bcode/484938	ЭР	15	100	+
3	Шаповалова, Г. П. «Цифровая культура» в концепции глобального информационного общества: теоретико-правовой аспект : монография / Г. П. Шаповалова. — Владивосток : ВГУЭС, 2020. — 176 с. https://e.lanbook.com/book/170250	ЭР	15	100	+

ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ **http://webirbis.tsogu.ru/**

Руководитель образовательной программы _____ Л. С. Ковальжина
«27» мая 2021 г.

Директор БИК_____ Д. Х. Каюкова
«27» мая 2021 г.