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

УТВЕРЖДАЮ

Председатель КСН
_____ О.Н. Кузяков
«28» мая 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: Организационное и правовое обеспечение информационной безопасности

направление подготовки 27.04.04 Управление в технических системах

направленность (профиль): Информационная безопасность автоматизированных систем управления технологическими процессами

форма обучения: очная, заочная

Рабочая программа разработана в соответствии с утвержденным учебным планом от 27.05.2021 г. и требованиями ОПОП 27.04.04 Управление в технических системах к результатам освоения дисциплины «Организационное и правовое обеспечение информационной безопасности»

Рабочая программа рассмотрена
на заседании кафедры кибернетических систем

Протокол № 9 от «28» мая 2021 г.

Заведующий кафедрой _____ О.Н Кузяков

СОГЛАСОВАНО:
Заведующий выпускающей кафедрой_____ О.Н. Кузяков

«28» мая 2021 г.

Рабочую программу разработал:

Х.Н. Музипов, доцент кафедры КС, к.т.н.

1. Цели и задачи освоения дисциплины

Цель дисциплины: формирование у обучающихся знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи дисциплины:

знать и понимать сущность информационной безопасности;

понимать принципы организации защиты информации на предприятиях; выявлять основные виды угроз информационной безопасности;

применять программно-аппаратные средства для обеспечения информационной безопасности.

Изучение дисциплины служит целям формирования мировоззрения, развития интеллекта, инженерной эрудиции, формированию компетенций.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части, формируемой участниками образовательных отношений учебного плана.

Необходимыми условиями для освоения дисциплины являются:

Знать:

- основы информационной безопасности и защиты информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;
- правовые нормы информационной безопасности
- методы и средства проектирования БД, особенности администрирования БД в локальных и глобальных сетях;
- виды угроз ИС и методы обеспечения информационной безопасности;

Уметь:

- реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации;

Владеть:

- навыками разработки технической документации;
- использования функциональных и технологических стандартов ИС; методами работы с инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации;
- иметь представление о типовых разработанных средствах защиты информации и возможностях их использования в реальных задачах создания и внедрения информационных систем.

Содержание дисциплины служит основой для освоения дисциплины «Управление информационной безопасностью»

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)[1]	Код и наименование результата обучения по дисциплине (модулю)
УК-3. Способен организовать	УК-3.1 Учитывает в своей социальной и	Знать:

и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	профессиональной деятельности интересы, особенности поведения и мнения (включая критические) людей, с которыми работает/взаимодействует, в том числе посредством корректировки своих действий.	З1 особенности командных ролей с точки зрения различных концепций
		Уметь: У1 оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия
		Владеть: В1 методами сплочения группы для повышения ее эффективности
	УК-3.2 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. Организует обсуждение разных идей и мнений.	Знать: З2 знает типы команд и способы социального взаимодействия
		Уметь: У2 принимать решение, согласованное с членами команды
		Владеть: В2 навыками распределения ролей в практической деятельности командного взаимодействия
ПКС -2 Способен тестировать системы защиты информации и разрабатывать проектные решения по защите информации в автоматизированных системах	ПКС-2.1 Применяет действующую нормативную базу в области обеспечения информационной безопасности	Знать: З3 понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации
		Уметь: У3 находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации
		Владеть: В3 навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Знать: З4 Принципы построения средств защиты информации от «утечки» по техническим каналам
		Уметь: У4 анализировать средства защиты информации
		Владеть:

		В4 Навыками использования различных видов и типов средств защиты информации
	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З5 принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем
		Уметь: У5 Проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
		Владеть: В5 Навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З6 Принципы построения и функционирования систем и сетей передачи информации
		Уметь: У6 эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах
		Владеть: В6- навыками определения основных угрозы информационной безопасности в автоматизированных системах
	ПКС-2.5 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью в автоматизированных системах	Знать: З7 основные меры обеспечения информационной безопасности АС
		Уметь: У7 разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ
		Владеть: В7 навыками обоснования, выбора, реализации и контроля результатов управленческого решения

4. Объем дисциплины

Общий объем дисциплины составляет 4 зачетных единиц, 144 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
очная	1/2	36	36	-	72	з
заочная	3/5	6	8	-	130	з

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины/модуля		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства[1]
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение	2	-	-	2	4	УК-3.1 УК-3.2 ПКС-2.1	Устный опрос
2	2	Актуальность информационной безопасности, понятия и определения	4	6	-	14	24	ПКС-2.1	Устный опрос
3	3	Основы защиты информации	6	4	-	14	24	ПКС-2.1	Устный опрос
4	4	Правовое обеспечение информационной безопасности	4	2	-	14	20	ПКС-2.1	Устный опрос
5	5	Организационные основы защиты информации	4	4	-	14	22	УК-3.1 УК-3.2 ПКС-2.1	Устный опрос
6	6	Обеспечение безопасности автоматизированных систем	4	5	-	14	23	ПКС-2.1 ПКС-2.2 ПКС-2.3 ПКС-2.4 ПКС-2.5	Устный опрос
…	Зачет		-	-	-	00	00		Вопросы к зачету
Итого:			36	36	-	72	144		

заочная форма обучения (ЗФО)

Таблица 5.1.3

№ п/п	Структура дисциплины/модуля		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение	1	-	-	10	11	УК-3.1 УК-3.2 ПКС-2.1	-
2	2	Актуальность информационной безопасности, понятия и определения	1	1,5	-	24	26,5	ПКС-2.1	Устный опрос, контрольная работа
3	3	Основы защиты информации	1	1,5	-	24	26,5	ПКС-2.1	Устный опрос, контрольная работа
4	4	Правовое обеспечение информационной	1	1	-	24	26	ПКС-2.1	Устный опрос,

[1] Эссе, реферат, тест, типовой расчет, опрос (устный или письменный), собеседование, РГР, контрольная работа, творческое задание, кейс-задача, деловая игра, презентация доклада, отчет и т.д. Указываются ссылки на конкретные задания, представленные в ФОС, т.е. тест №1, контрольная работа № 1 и т.д.

		безопасности							контрольная работа
5	5	Организационные основы защиты информации	1	1,5	-	24	26,5	УК-3.1 УК-3.2 ПКС-2.1	Устный опрос, контрольная работа
6	6	Обеспечение безопасности автоматизированных систем	1	2,5	-	20	23,5	ПКС-2.1 ПКС-2.2 ПКС-2.3 ПКС-2.4 ПКС-2.5	Устный опрос, контрольная работа
	Зачет		-	-	-	00	00		Вопросы к зачету
		Итого:	6	8	-	130	144		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Введение». Цели и задачи дисциплины. Законодательство РФ о вопросах защиты информации.

Раздел 2. «Актуальность информационной безопасности, понятия и определения». Понятие информационной безопасности. Виды угроз. Предпосылки появления угроз. Возможные пути получения конфиденциальной информации. Каналы утечки информации. Целостность. Оценка уязвимости.

Раздел 3. «Основы защиты информации». Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации. Виды и схемы сертификации средств защиты информации. Классы защищенности автоматизированных систем. Политика безопасности в РФ, США.

Раздел 4. «Правовое обеспечение информационной безопасности». ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

Раздел 5. «Организационные основы защиты информации». Конфиденциальность информации. Политика безопасности автоматизированных систем.

Раздел 6. «Обеспечение безопасности автоматизированных систем». Требования к защите информации. Обеспечение безопасности автоматизированных систем

5.2.2. Содержание дисциплины по видам учебных занятий.

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.		Тема лекции
		ОФО	ЗФО	
1	1	2	1	Цели, задачи дисциплины; Законодательство РФ о вопросах защиты информации.
2	2	6	1	Понятие информационной безопасности. Виды угроз. Предпосылки появления угроз. Возможные пути получения конфиденциальной информации. Каналы утечки информации. Целостность. Оценка уязвимости.
3	3	6	1	Организационная структура системы сертификации

				средств защиты информации по требованиям безопасности информации. Виды и схемы сертификации средств защиты информации. Классы защищенности автоматизированных систем. Политика безопасности в РФ, США.
4	4	6	1	ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
5	5	6	1	Конфиденциальность информации. Политика безопасности автоматизированных систем.
6	6	10	1	Требования к защите информации. Обеспечение безопасности автоматизированных систем.
Итого:		36	6	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.		Тема практического занятия
		ОФО	ЗФО	
1	2	2	0,5	Анализ источников, каналов распространения и каналов утечки информации
2		2	0,5	Проведение анализа информации на предмет целостности
3		2	0,5	Основы защиты информации. Оценка уязвимости информации
4	3	2	0,5	Требования к безопасности информационных систем в России. Оценка состояния безопасности ИС США
5		2	1	Определение классов защищенности средств вычислительной техники от несанкционированного доступа. Определение требований к защите информации
6	4	2	1	Анализ терминов и определений информационной безопасности. Работа с ГОСТами в области информационной безопасности
7	5	2	1	Составление инструкции по обработке и хранению конфиденциальных документов
8		2	0,5	Оценка безопасности информации на объектах ее обработки
9	6	2	0,5	Классификация автоматизированных систем обработки информации по классу защиты информации
10		2	0,5	Планирование, создание и изменение учетных записей пользователей
11		2	0,5	Создание и администрирование групп пользователей
12		2	0,5	Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам
13		2	0,5	Наследование разрешений в NTFS
14		2	0,5	Изменение параметров учетных записей

				пользователей
15		2	0,5	Настройка политики учетных записей
16		2	0,5	Настройка параметров безопасности операционных систем
17		4	0,5	Настройка параметров безопасности Windows. Настройка параметров безопасности Интернет
Итого:		36	8	

Лабораторные работы

Таблица 5.2.3

Лабораторные работы учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины	Объем, час.		Тема	Вид СРС
		ОФО	ЗФО		
1	1	2	10	Цели, задачи дисциплины Актуальность информационной безопасности, понятия и определения Основы защиты информации	подготовка к практическим занятиям
2	2	14	24	Анализ источников, каналов распространения и каналов утечки информации	подготовка к практическим занятиям
3	3	14	24	Угрозы информации Правовое обеспечение информационной безопасности	подготовка к практическим занятиям
4	4	14	24	Вредоносные программы Защита от компьютерных вирусов.	подготовка к практическим занятиям
5	5	14	24	Обеспечение безопасности автоматизированных систем	подготовка к практическим занятиям
6	6	14	20	Средства и методы защиты информации и программного обеспечения от несанкционированного доступа и копирования. Организационные основы защиты информации	подготовка к практическим занятиям
	1-6	-	4	Контроль	Подготовка к зачету
Итого:		72	130		

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).

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены

7. Контрольные работы

7.1. Методические указания для выполнения контрольных работ.

Контрольные работы предусмотрены для обучающихся заочной формы обучения.

Цель выполнения контрольной работы – закрепление теоретической и практической подготовки обучающихся заочной формы.

После теоретического лекционного курса и обсуждения вопросов на практических занятиях каждый обучающийся выполняет индивидуальное задание. Контрольная работа выполняется обучающимся самостоятельно и сдается в установленные кафедрой сроки (но не позднее дня сдачи зачета или экзамена по дисциплине).

Выполнение контрольной работы обучающийся должен начинать с изучения задания, методических указаний к ее выполнению и курса лекционных и практических занятий. По требованию руководителя следует собрать и изучить рекомендуемую литературу, выполнить патентный и тематический поиск информации, в том числе через информационно - телекоммуникационные сети общего доступа. Трудоемкость выполнения контрольной работы – 34 часа.

7.2. Тематика контрольных работ.

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Субъекты и объекты правоотношений в области информационной безопасности.
3. Отрасли законодательства, регламентирующие деятельность по защите информации. Конфиденциальная информация. Виды тайн.
4. Система защиты государственной тайны. Органы защиты государственной тайны и их компетенции.
5. Правовая основа лицензирования и сертификации в области защиты информации, в том числе защиты государственной тайны.
6. Преступления в сфере компьютерной информации. Экспертиза компьютерных преступлений.
7. Административные правонарушения.
8. Задачи организационного обеспечения информационной безопасности.
9. Роль нормативных документов в защите информации.
10. Инвентаризация информационных ресурсов организации.
11. Анализ и оценка угроз информационной безопасности объекта.
12. Нормативное обеспечение работы сотрудников организации с информацией ограниченного доступа.
13. Основные принципы организации и обеспечения секретного документооборота.

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		
	Практическая работа № 1,2, 3,4,5	20
	Активная работа на занятиях	5
	Проверка результатов самостоятельной работы	5
	ИТОГО за первую текущую аттестацию	**30**
2 текущая аттестация		
	Практическая работа № 6,7,8,9	20
	Активная работа на занятиях	5
	Проверка результатов самостоятельной работы	5
	ИТОГО за вторую текущую аттестацию	**30**
3 текущая аттестация		
	Практическая работа № 10-17	5
	Активная работа на занятиях	5
	Проверка результатов самостоятельной работы	10
	Тестирование	10
	ИТОГО за третью текущую аттестацию	**40**
	ВСЕГО	**100**

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

Таблица 8.2

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1.	Практическая работа 1-3	10
2.	Практическая работа 4-5	10
3.	Практическая работа 6	15
4.	Практическая работа 7-8	10
5.	Практическая работа 9-17	15
6.	Активная работа на занятиях	15
7.	Проверка результатов выполнения контрольной работы	25
	ВСЕГО	**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

Сайт ФГБОУ ВО ТИУ http://www.tyuiu.ru

- Система поддержки учебного процесса ТИУ https://educon2.tyuiu.ru/login/index.php
- Электронный каталог Библиотечно-издательского комплекса http://webirbis.tsogu.ru/
- Электронная библиотечная система eLib http://elib.tsogu.ru/
- ЭБС «Издательства Лань» – http://e.lanbook.com
- ЭБС «Электронного издательства ЮРАЙТ»–www. https://urait.ru
- Научная электронная библиотека ELIBRARY.RU;
- ЭБС «IPRbooks»– http://www.iprbookshop.ru/
- Научно-техническая библиотека ФГБОУ ВО РГУ нефти и газа имени И.М. Губкина - http://elib.gubkin.ru/
- Научно-техническая библиотека ФГБОУ ВПО УГНТУ (г. Уфа) -http://bibl.rusoil.net

- Научно-техническая библиотека ФГБОУ ВПО УГТУ (г. Ухта) - http://lib.ugtu.net/books
- ЭБС «Проспект» – http://ebs.prospekt.org
- ЭБС «Консультант студент» 1– http://www.studentlibrary.ru
- Справочно-информационная база данных «Техэксперт»

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства: Adobe Acrobat Reader DC, Свободно-распространяемое ПО; Microsoft Office Professional Plus; Microsoft Windows; Scilab, Свободно- распространяемое ПО; Zoom (бесплатная версия), 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/модуля	Перечень технических средств обучения, необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
1	-	Интерактивная сенсорная доска, моноблок; проектор, акустическая система (колонки)

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим занятиям.

Проведение практических занятий направлено на закрепление полученных теоретических знаний по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Каждое практическое занятие имеет наименование и цель работы, основные теоретические положения, методику решения практического задания, а также контрольные вопросы. После выполнения практического задания, каждый из обучающихся представляет преподавателю отчет, отвечает на теоретические вопросы, демонстрирует уровень сформированности компетенций. Отчет о проделанной работе должен быть представлен обучающимся либо в день выполнения задания, либо на следующем занятии. Отчеты о проделанных работах следует выполнять на отдельных листах формата А4; схемы, графики, рисунки необходимо выполнять простым карандашом либо с использованием графических редакторов в соответствии с требованиями стандартов ЕСКД. На выполнение каждой работы отводится определенное количество часов в соответствии с тематическим планом изучения дисциплины. Отчет включает в себя: титульный лист, цель работы, решение практического задания со всеми необходимыми пояснениями, графики и векторные диаграммы при необходимости, вывод по работе.

11.2. Методические указания по организации самостоятельной работы.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его непосредственного участия. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий. Самостоятельная работа может осуществляться

индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение заданий по образцу, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Самостоятельная работа с преподавателем включает в себя индивидуальные консультации студентов в течение семестра.

Самостоятельная работа с группой включает проведение текущих консультаций перед промежуточными видами контроля или итоговой аттестации.

Самостоятельная работа студента без преподавателя включает в себя подготовку к различным видам контрольных испытаний, подготовку и написание самостоятельных видов работ.

Перед выполнением внеаудиторной самостоятельной работы студент должен внимательно выслушать инструктаж преподавателя по выполнению задания, который включает определение цели задания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. В методических указаниях к практическим занятиям приведены как индивидуальные, так и групповые задания в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности. В качестве форм и методов контроля внеаудиторной самостоятельной работы студентов используются аудиторные занятия, аттестационные мероприятия, самоотчеты.

Критериями оценки результатов внеаудиторной самостоятельной работы студента являются:

– уровень освоения студентом учебного материала;

– умение студента использовать теоретические знания при выполнении практических заданий;

– обоснованность и четкость изложения ответа;

– оформление материала в соответствии с требованиями.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина Организационное и правовое обеспечение информационной безопасности

направление подготовки 27.04.04 Управление в технических системах
направленность (профиль): Информационная безопасность
автоматизированных систем управления технологическими процессами

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК-3	УК-3.1 Учитывает в своей социальной и профессиональной деятельности интересы, особенности поведения и мнения (включая критические) людей, с которыми работает/взаимодействует, в том числе посредством корректировки своих действий.	Знать: З1 особенности командных ролей с точки зрения различных концепций	Не знает особенности командных ролей с точки зрения различных концепций	Частично знает особенности командных ролей с точки зрения различных концепций	Знает особенности командных ролей с точки зрения различных концепций	В совершенстве знает особенности командных ролей с точки зрения различных концепций
		Уметь: У1 оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия	Не способен оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия	Частично умеет оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия	Способен оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия	В совершенстве может оценивать сплоченность группы (команды); использовать в социальной и профессиональной деятельности стратегию сотрудничества для достижения поставленной цели; эффективно работать в команде; определять свою роль в команде, при этом проявлять уважение к мнению и культуре других, принимать решения с соблюдением этических принципов их реализации, определять цели и корректировать свои действия

		Владеть: В1 методами сплочения группы для повышения ее эффективности	Не владеет методами сплочения группы для повышения ее эффективности	Частично владеет методами сплочения группы для повышения ее эффективности	Владеет методами сплочения группы для повышения ее эффективности	В полном объеме владеет методами сплочения группы для повышения ее эффективности
	УК-3.2 Планирует командную работу, распределяет поручения и делегирует полномочия членам команды. Организует обсуждение разных идей и мнений.	Знать: З2 типы команд и способы социального взаимодействия	Не знает типы команд и способы социального взаимодействия	Частично знает типы команд и способы социального взаимодействия	Знает типы команд и способы социального взаимодействия	В полном объеме знает типы команд и способы социального взаимодействия
		Уметь: У2 принимать решение, согласованное с членами команды	Не умеет принимать решение, согласованное с членами команды	Частично умеет принимать решение, согласованное с членами команды	Умеет принимать решение, согласованное с членами команды	В полном объеме умеет принимать решение, согласованное с членами команды
		Владеть: В2 навыками распределения ролей в практической деятельности командного взаимодействия	Не владеет навыками распределения ролей в практической деятельности командного взаимодействия	Частично владеет навыками распределения ролей в практической деятельности командного взаимодействия	Владеет навыками распределения ролей в практической деятельности командного взаимодействия	В совершенстве владеет навыками распределения ролей в практической деятельности командного взаимодействия
ПКС-2	ПКС-2.1 Применяет действующую нормативную базу в области обеспечения информационной безопасности	Знать: З3 понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации	Не знает понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации	Частично знает понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации	Знает понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации	В совершенстве знает понятие и виды защищаемой информации по законодательству РФ; нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; организационные принципы защиты информации

		Уметь: У3 находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	Не умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	Частично умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	Умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации	В совершенстве умеет находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации
		Владеть: В3 навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации	Не владеет навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации	Частично владеет навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации	Владеет навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации	В полном объеме владеет навыками использования нормативно-методических материалов по регламентации системы организационной защиты информации
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Знать: З4 Принципы построения средств защиты информации от «утечки» по техническим каналам	Не знает принципы построения средств защиты информации от «утечки» по техническим каналам	Частично знает принципы построения средств защиты информации от «утечки» по техническим каналам	Знает принципы построения средств защиты информации от «утечки» по техническим каналам	В полном объеме знает принципы построения средств защиты информации от «утечки» по техническим каналам
		Уметь: У4 анализировать средства защиты информации	Не умеет анализировать средства защиты информации	Частично умеет анализировать средства защиты информации	Умеет анализировать средства защиты информации	В полном объеме умеет анализировать средства защиты информации
		Владеть: В4 Навыками использования различных видов и типов средств защиты информации	Не владеет навыками использования различных видов и типов средств защиты информации	Частично владеет навыками использования различных видов и типов средств защиты информации	Владеет навыками использования различных видов и типов средств защиты информации	В полном объеме владеет навыками использования различных видов и типов средств защиты информации

	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З5 принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем	Не знает принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем	Частично знает принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем	Знает принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем	В полном объеме знает принципы построения основных функциональных и структурных схем защищенных автоматизированных информационных систем
		Уметь: У5 Проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Не умеет проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Частично умеет проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Умеет проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	В полном объеме умеет проводить анализ схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
		Владеть: В5 Навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем	Не владеет навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем	Частично владеет навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем	Владеет навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем	В полном объеме владеет навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З6 Принципы построения и функционирования систем и сетей передачи информации	Не знает принципы построения и функционирования систем и сетей передачи информации	Частично знает принципы построения и функционирования систем и сетей передачи информации	Знает принципы построения и функционирования систем и сетей передачи информации	В полном объеме знает принципы построения и функционирования систем и сетей передачи информации
		Уметь: У6 эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	Не способен эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	Частично умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	Умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах	В полном объеме умеет эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах

		Владеть: В6- навыками определения основных угрозы информационной безопасности в автоматизированных системах	Не владеет навыками определения основных угрозы информационной безопасности в автоматизированных системах	Частично владеет навыками определения основных угрозы информационной безопасности в автоматизированных системах	Владеет навыками определения основных угрозы информационной безопасности в автоматизированных системах	В полном объеме владеет навыками определения основных угрозы информационной безопасности в автоматизированных системах
	ПКС-2.5 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью в автоматизированных системах	Знать: З7 основные меры обеспечения информационной безопасности АС	Не знает основные меры обеспечения информационной безопасности АС	Частично знает основные меры обеспечения информационной безопасности АС	Знает основные меры обеспечения информационной безопасности АС	В полном объеме знает основные меры обеспечения информационной безопасности АС
		Уметь: У7 разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ	Не умеет разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ	Частично умеет разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ	Умеет разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ	В полном объеме умеет разрабатывать организационно-распорядительные документы по обеспечению информационной безопасности АС с учётом требований нормативно-правовых актов РФ
		Владеть: В7 навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Не владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Частично владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения	Владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения	В полном объеме владеет навыками обоснования, выбора, реализации и контроля результатов управленческого решения

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

дисциплины: Организационное и правовое обеспечение информационной безопасности
направление подготовки 27.04.04 Управление в технических системах
направленность (профиль): Информационная безопасность автоматизированных систем управления технологическими процессами

№ 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	**Башлы, П. Н.** Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : Евразийский открытый институт, 2012. - 311 с. - ЭБС "IPR BOOKS". Режим доступа: lUtD://\vww.iDrbookshoD.ru/cDcl-reader?miblicationId= 10677	ЭР*	30	100	+
2	**Тумбинская, М. В.** Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2019. — 344 с. Режим доступа httos ://e. lanbook.eom/book/l2573 9	ЭР*	30	100	+
3	**Коваленко, Ю. И.** Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю. И. Коваленко. — Москва : Горячая линия-Телеком,	ЭР*	30	100	+

Заведующий кафедрой
кибернетических систем О.Н. Кузяков
«28» 05 2021 г.

Директор БИК Д.Х. Каюкова
«28» 05 2021 г.
М.П.