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: Управление информационной безопасностью

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 «Управление информационной безопасностью»

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 знаний по основам управления информационной безопасностью.

Задачи дисциплины:

- знать основы информационной безопасности; **:**
- уметь организовать систему обеспечения информационной безопасности;
- владеть навыками 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:

знания:

- основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические;
- наиболее распространенные угрозы информационной безопасности, критерии их классификации. Основные составляющие информационной безопасности;
- основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах управления.

Умения:

- использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации при решении задач обеспечения ИБ;
- определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
- определять виды уязвимостей информационной безопасности;
- разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.

Владение:

- навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности;
- навыками применения мер для обеспечения информационной безопасности автоматизированных систем;
- навыками выявления основных угроз информационной безопасности в автоматизированных системах.

Содержание дисциплины является логическим продолжением содержания дисциплин Защита информации в автоматизированных системах управления, Организационное и правовое обеспечение информационной безопасности.

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

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	Знать: З1 системный подход при решении проблемы
		Уметь: У1 выявлять связи между составляющими проблемной ситуации
		Владеть: В1 навыками анализа проблемной ситуации
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации, определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке, предлагает способы их решения.	Знать: З2 алгоритмы решения проблемной ситуации
		Уметь: У2 критически оценивать надежность источников информации при поиске алгоритмов решения задачи
		Владеть: В2 навыком поиска вариантов решения проблемной ситуации
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 Законодательный уровень информационной безопасности
		Уметь: У3 использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ
		Владеть: В3 навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Знать: З4 основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)
		Уметь: У4 определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем
		Владеть: В4 навыками применения мер для обеспечения информационной безопасности автоматизированных систем
	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З5 виды схем защищённых автоматизированных информационных систем
		Уметь: У5 определять виды уязвимостей информационной безопасности
		Владеть: В5 навыками выявления потенциальных уязвимостей информационной безопасности
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З6 наиболее распространенные угрозы ИБ, критерии их классификации. Основные составляющие ИБ
		Уметь: У6 Анализировать основные угрозы информационной безопасности в автоматизированных системах
		Владеть: В6 навыками выявления основных угроз информационной безопасности в автоматизированных системах
	ПКС-2.5 Разрабатывает предложения по	Знать: З7 основные методы

	совершенствованию системы управления информационной безопасностью в автоматизированных системах	управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.
		Уметь: У7 разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.
		Владеть: В7 навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

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	2/4	22	22	-	100	экзамен
заочная	3/5	10	12	-	122	экзамен

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	Наиболее распространенные угрозы ИБ.	2	2	-	10	14	УК-1.1, УК-1.2 ПКС-2.4	Устный опрос
2	2	Законодательный уровень информационной безопасности	2	2	-	10	14	УК-1.1, УК-1.2 ПКС-2.1 ПКС-2.5	Устный опрос
3	3	Административный уровень информационной безопасности.	2	2	-	10	14	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.44 ПКС-2.5	Устный опрос
4	4	Процедурный уровень информационной безопасности.	4	4	-	16	24	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	Устный опрос

								ПКС-2.5	
5	5	Основные программно-технические меры. Идентификация и аутентификация, управление доступом.	4	4	-	16	24	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	Устный опрос
6	6	Протоколирование и аудит, шифрование и контроль целостности.	4	4	-	18	26	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	Устный опрос
7	7	Экранирование, анализ защищенности.	2	2	-	10	14	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	Устный опрос
8	8	Обеспечение высокой доступности. Туннелирование и управление.	2	2	-	10	14	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	Устный опрос
	экзамен		-	-	-	00	00		Вопросы к экзамену
		Итого:	22	22	-	100	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	Наиболее распространенные угрозы ИБ.	0,5	1	-	10	11,5	УК-1.1, УК-1.2 ПКС-2.4	*подготовка к практическим занятиям, контрольная работа*
2	2	Законодательный уровень информационной безопасности	0,5	1	-	15	16,5	УК-1.1, УК-1.2 ПКС-2.1	*подготовка к практическим занятиям, контрольная работа*
3	3	Административный уровень информационной безопасности.	0,5	1	-	15	16,5	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.44	*подготовка к практическим занятиям, контрольная работа*
4	4	Процедурный уровень информационной безопасности.	1,5	1	-	16	18,5	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4 ПКС-2.5	*подготовка к практическим занятиям, контрольная работа*
5	5	Основные программно-технические меры.	2	2	-	18	22	УК-1.1, УК-1.2 ПКС-2.2	*подготовка к практическим занятиям,*

		Идентификация и аутентификация, управление доступом.						ПКС-2.3 ПКС-2.4 ПКС-2.5	*контрольная работа*
6	6	Протоколирование и аудит, шифрование и контроль целостности.	2	2	-	18	22	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	*подготовка к практическим занятиям, контрольная работа*
7	7	Экранирование, анализ защищенности.	2	1	-	15	18	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	*подготовка к практическим занятиям, контрольная работа*
8	8	Обеспечение высокой доступности. Туннелирование и управление.	1	1	-	15	17	УК-1.1, УК-1.2 ПКС-2.2 ПКС-2.3 ПКС-2.4	*подготовка к практическим занятиям, контрольная работа*
	экзамен		-	-	-	00	00		Вопросы к эзкамену
Итого:			10	12	-	122	144		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Наиболее распространенные угрозы ИБ». Основные составляющие ИБ. Важность и сложность проблемы ИБ. Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.

.Раздел 2. «Законодательный уровень информационной безопасности».
Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон «Об информации, информатизации и защите информации». Обзор зарубежного законодательства в области информационной безопасности. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.

Раздел 3. «Административный уровень информационной безопасности». Управление рисками. Основные понятия. Политика и программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Раздел 4. «Процедурный уровень информационной безопасности». Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Раздел 5. «Основные программно-технические меры. Идентификация и аутентификация, управление доступом». Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Идентификация и аутентификация. Парольная аутентификация. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом.

Раздел 6. «Протоколирование и аудит, шифрование и контроль целостности». Протоколирование и аудит. Основные понятия. Активный аудит. Сигнатура атаки.

Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.

Раздел 7. «Экранирование, анализ защищенности». Экранирование (основные понятия, архитектурные аспекты). Классификация межсетевых экранов. Анализ защищенности.

Раздел 8. «Обеспечение высокой доступности. Туннелирование и управление». Доступность, основные понятия. Меры обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Программное обеспечение промежуточного слоя. Обеспечение обслуживаемости. Туннелирование. Управление. Основные понятия.

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	0,5	Наиболее распространенные угрозы ИБ. Основные составляющие ИБ. Важность и сложность проблемы ИБ. Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.
2	2	2	0,5	Законодательный уровень информационной безопасности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон «Об информации, информатизации и защите информации». Обзор зарубежного законодательства в области информационной безопасности. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.
3	3	2	0,5	Административный уровень информационной безопасности. Управление рисками. Основные понятия. Политика и программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Подготовительные этапы управления рисками. Основные этапы управления рисками.
4	4	4	1,5	Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
5	5	4	2	Основные программно-технические меры. Идентификация и аутентификация, управление доступом. Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Идентификация и аутентификация. Парольная аутентификация. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом.
6	6	4	2	Протоколирование и аудит, шифрование и контроль целостности. Протоколирование и аудит. Основные понятия. Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.
7	7	2	2	Экранирование, анализ защищенности. Экранирование (основные понятия, архитектурные аспекты). Классификация межсетевых экранов. Анализ защищенности.
8	8	2	1	Обеспечение высокой доступности. Туннелирование и управление. Доступность, основные понятия. Меры обеспечения высокой доступности. Отказоустойчивость и зона риска.

				Обеспечение отказоустойчивости. Программное обеспечение промежуточного слоя. Обеспечение обслуживаемости. Туннелирование. Управление. Основные понятия.
Итого:		22	10	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.		Тема практического занятия
		ОФО	ЗФО	
1	1	2	1	Наиболее распространенные угрозы ИБ. Основные составляющие ИБ. Важность и сложность проблемы ИБ. Основные определения и критерии классификации угроз. Наиболее распространенные угрозы доступности. Вредоносное программное обеспечение. Основные угрозы целостности. Основные угрозы конфиденциальности.
2	2	2	1	Законодательный уровень информационной безопасности. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон «Об информации, информатизации и защите информации». Обзор зарубежного законодательства в области информационной безопасности. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт.
3	3	2	1	Административный уровень информационной безопасности. Управление рисками. Основные понятия. Политика и программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Подготовительные этапы управления рисками. Основные этапы управления рисками.
4	4	4	1	Процедурный уровень информационной безопасности. Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.
5	5	4	2	Основные программно-технические меры. Идентификация и аутентификация, управление доступом. Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Идентификация и аутентификация. Парольная аутентификация. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом.
6	6	4	2	Протоколирование и аудит, шифрование и контроль целостности. Протоколирование и аудит. Основные понятия. Активный аудит. Сигнатура атаки. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.
7	7	2	1	Экранирование, анализ защищенности. Экранирование (основные понятия, архитектурные аспекты). Классификация межсетевых экранов. Анализ защищенности.
8	8	2	1	Обеспечение высокой доступности. Туннелирование и управление. Доступность, основные понятия. Меры обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Программное обеспечение промежуточного слоя. Обеспечение

				обслуживаемости. Туннелирование. Управление. Основные понятия.
Итого:		22	12	

Лабораторные работы

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	10	10	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме	*подготовка к практическим занятиям*
2	2	10	15	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной бразовательной среде или печатной форме	*подготовка к практическим занятиям*
3	3	10	15	Управление рисками. 1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной	*подготовка к практическим занятиям*
4	4	16	16	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме	*подготовка к практическим занятиям*
5	5	16	18	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме	*подготовка к практическим занятиям*
6	6	18	18	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме	*подготовка к практическим занятиям*
7	7	10	15	1. Работа с основной и дополнительной литературой 2. Выполнение практико-	*подготовка к практическим занятиям*

				ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме	
8	8	10	15	1. Работа с основной и дополнительной литературой 2. Выполнение практико-ориентированного задания с предоставлением ответа в электронной образовательной среде или печатной форме. 3. Подготовка к промежуточной аттестации.	*подготовка к практическим занятиям*
Итого:		100	122		

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 – 40 часов.

7.2. Тематика контрольных работ.

1. Серия стандартов по управлению информационной безопасностью;
2. Понятие политики информационной безопасности, принципы, ответственность, жизненный цикл;
3. Деятельность по обеспечению информационной безопасности предприятия;
4. Основные понятия Доктрины информационной безопасности в РФ;
5. Структура и содержание правового обеспечения информационной безопасности;
6. Структура и содержание организационного обеспечения информационной безопасности;
7. Основы управления рисками информационной безопасности;
8. Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»);

9. Международное сотрудничество в области информационной безопасности.

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	Практическая работа 1,2,3,4	32
2	Активная работа на занятиях	8
3	Устный опрос	10
	ИТОГО за первую текущую аттестацию	**50**
ИТОГО за вторую текущую аттестацию		
2 текущая аттестация		
1	Практическая работа 5,6,7,8	32
2	Устный опрос	10
3	Активная работа на занятиях	8
	ИТОГО за вторую текущую аттестацию	**50**
	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 1-8	64
2	Устный опрос	10
3	Проверка результатов выполнения контрольной работы	20
4	Активная работа на занятиях	6
	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

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	-	проектор, проекционный экран, акустическая система (колонки), документ-камера . Учебно-наглядные пособия: раздаточный материал по дисциплине «Управление информационной безопасностью».

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 «Управление информационной безопасностью».

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 Управление информационной безопасностью
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-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	Знать: З1 системный подход при решении проблемы	Не знает системный подход при решении проблемы	Знает частично системный подход при решении проблемы	Знает хорошо системный подход при решении проблемы	Знает в полном объеме системный подход при решении проблемы
		Уметь: У1 выявлять связи между составляющими проблемной ситуации	Не умеет выявлять связи между составляющими проблемной ситуации	Умеет с ошибками выявлять связи между составляющими проблемной ситуации	Умеет без существенных ошибок выявлять связи между составляющими проблемной ситуации	Умеет корректно пользоваться выявлять связи между составляющими проблемной ситуации
		Владеть: В1 навыками анализа проблемной ситуации	Не владеет навыками анализа проблемной ситуации	Слабо владеет навыками анализа проблемной ситуации	Хорошо владеет навыками анализа проблемной ситуации	Владеет в полной мере навыками анализа проблемной ситуации
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на основе доступных источников информации, определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке, предлагает способы их решения.	Знать: З2 алгоритмы решения проблемной ситуации	Не знает алгоритмы решения проблемной ситуации	Знает частично алгоритмы решения проблемной ситуации	Знает хорошо алгоритмы решения проблемной ситуации	Знает в полном объеме алгоритмы решения проблемной ситуации
		Уметь: У2 критически оценивать надежность источников информации при поиске алгоритмов решения задачи	Не умеет пользоваться технологиями расчетов надежности	Умеет с ошибками пользоваться технологиями расчетов надежности	Умеет без существенных ошибок пользоваться технологиям и расчетов надежности	Умеет корректно пользоваться технологиями расчетов надежности
		Владеть: В2 навыком поиска вариантов решения проблемной ситуации	Не владеет навыком анализа результатов расчета	Слабо владеет навыком анализа результатов расчета	Хорошо владеет навыком анализа результатов расчета	Владеет в полной мере навыком анализа результатов расчета

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-2	ПКС-2.1 Применяет действующую нормативную базу в области обеспечения информационной безопасности	Знать: З3 Законодательный уровень информационной безопасности	Не знает Законодательный уровень информационной безопасности	Знает частично Законодательный уровень информационной безопасности	Знает хорошо Законодательный уровень информационной безопасности	Знает в полном объеме Законодательный уровень информационной безопасности
		Уметь: У3 использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ	Не умеет использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ	Умеет с ошибками использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ	Умеет без существенных ошибок использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ	Умеет корректно использовать правовые акты общего назначения, затрагивающие вопросы информационной безопасности, оценочные стандарты и технические спецификации. при решении задач обеспечения ИБ
		Владеть: В3 навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности	Не владеет навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности	Слабо владеет навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности	Хорошо владеет навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности	Владеет в полной мере навыками нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих их реализацию технических мер защиты информации	Знать: З4 основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические технические)	Не знает основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)	Знает частично основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)	Знает хорошо основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)	Знает в полном объеме основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические)
		Уметь: У4 определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем	Не умеет определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем	Умеет с ошибками определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем	Умеет без существенных ошибок определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем	Умеет корректно пользоваться определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем
		Владеть: В4 навыками применения мер для обеспечения информационной безопасности автоматизированных систем	Не владеет навыками применения мер для обеспечения информационной безопасности автоматизированных систем	Слабо владеет навыками применения мер для обеспечения информационной безопасности автоматизированных систем	Хорошо владеет навыком навыками применения мер для обеспечения информационной безопасности автоматизированных систем	Владеет в полной мере навыками применения мер для обеспечения информационной безопасности автоматизированных систем

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З5 виды схем защищённых автоматизированных информационных систем	Не знает виды схем защищённых автоматизированных информационных систем	Знает частично виды схем защищённых автоматизированных информационных систем	Знает хорошо виды схем защищённых автоматизированных информационных систем	Знает в полном объеме виды схем защищённых автоматизированных информационных систем
		Уметь: У5 определять виды уязвимостей информационной безопасности	Не умеет определять виды уязвимостей информационной безопасности	Умеет с ошибками определять виды уязвимостей информационной безопасности	Умеет без существенных ошибок определять виды уязвимостей информационной безопасности	Умеет корректно определять виды уязвимостей информационной безопасности
		Владеть: В5 навыками выявления потенциальных уязвимостей информационной безопасности	Не владеет навыками выявления потенциальных уязвимостей информационной безопасности	Слабо владеет навыками выявления потенциальных уязвимостей информационной безопасности	Хорошо владеет навыками выявления потенциальных уязвимостей информационной безопасности	Владеет в полной мере навыками выявления потенциальных уязвимостей информационной безопасности
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З6 наиболее распространенные угрозы ИБ, критерии их классификации, основные составляющие ИБ	Не знает наиболее распространенные угрозы ИБ, критерии их классификации, основные составляющие ИБ	Знает частично наиболее распространенные угрозы ИБ, критерии их классификации, основные составляющие ИБ	Знает хорошо наиболее распространенные угрозы ИБ, критерии их классификации, основные составляющие ИБ	Знает в полном объеме наиболее распространенные угрозы ИБ, критерии их классификации, основные составляющие ИБ
		Уметь: У6 анализировать основные угрозы информационной безопасности в автоматизированных системах	Не умеет анализировать основные угрозы информационной безопасности в автоматизированных систем	Умеет с ошибками анализировать основные угрозы информационной безопасности в автоматизированных систем	Умеет без существенных ошибок анализировать основные угрозы информационной безопасности в автоматизированных систем	Умеет корректно анализировать основные угрозы информационной безопасности в автоматизированных систем

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть: В6 навыками выявления основных угроз информационной безопасности в автоматизированных системах	Не владеет навыками выявления основных угроз информационной безопасности в автоматизированных системах	Слабо владеет навыками выявления основных угроз информационной безопасности в автоматизированных системах	Хорошо владеет навыками выявления основных угроз информационной безопасности в автоматизированных системах	Владеет в полной мере навыками выявления основных угроз информационной безопасности в автоматизированных системах
	ПКС-2.5 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью в автоматизированных системах	Знать: З7 основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.	Не знает основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.	Знает частично основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.	Знает хорошо основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.	Знает в полном объеме основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах.
		Уметь: У7 разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.	Не умеет разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.	Умеет с ошибками разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем	Умеет без существенных ошибок разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.	Умеет корректно разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине (модулю)	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть: В7 навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	Не владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	Слабо владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	Хорошо владеет навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.	Владеет в полной мере навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

Приложение 2

КАРТА

обеспеченности дисциплины учебной и учебно-методической литературой

дисциплины: Управление информационной безопасностью

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	Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2018. — 120 с. — ISBN 978-5-9275-2742-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87643.html	ЭР*	30	100	+
2	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/432966	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.