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: Защита информации в автоматизированных системах управления

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 «Защита информации в автоматизированных системах управления»

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 изучения дисциплины - ознакомление обучающихся с аппаратными и программными средствами защиты компьютерной информации и с защитой информационных процессов в компьютерных сетях.

Задачи дисциплины:

–изучение современных методов и средств защиты информации в компьютерных системах и сетях;

–приобретений практических навыков по применению полученных знаний для защиты компьютерной информации.

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:

знание структур и принципов организации операционных систем; основы администрирования вычислительных сетей; основы управления базами данных ; эталонную модель взаимодействия открытых систем.,

умения применять методы настройки операционных систем, вычислительных сетей и баз данных;

владение стандартными методами и средствами защиты информации в компьютерных системах и сетях.

Содержание дисциплины служит основой для освоения дисциплин Управление информационной безопасностью и прохождения производственной практики (эксплуатационной)

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 проблемных ситуаций; методы анализа своих проблемных ситуаций
		Уметь: У1- принимать решения при проблемных ситуациях
		Владеть: В1 методами решения проблемных ситуациях
	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 актуальность и важность проблем защиты информации
		Уметь: У2 пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
		Владеть: В2 терминологией в области защиты информации

УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1 Разрабатывает концепцию проекта в рамках обозначенной проблемы, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения, разрабатывает план реализации проекта и осуществляет мониторинг хода его реализации	Знать: З3 основные правила обеспечения информационной безопасности при разработке методик и инструкций
		Уметь: У3 разрабатывать рекомендации и методики, позволяющих обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения
		Владеть: В3 навыками применения рекомендаций и методик по совершенствованию информационной безопасности
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: З4 - нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		Уметь: У4 применять действующую нормативную базу в области обеспечения безопасности информации
		Владеть: В4 - навыками применения действующей нормативной базы в области обеспечения информационной безопасности
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Знать: З5 - принципы организации и структуру систем защиты информации автоматизированных систем
		Уметь: У5 - определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
		Владеть: В5 - методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации
	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З6 - принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
		Уметь: У6 - анализировать основные узлы и устройства современных автоматизированных систем
		Владеть:

		В6 - навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З7 - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
		Уметь: У7 - анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации
		Владеть: В7 - навыком выявлять основные угрозы информационной безопасности в автоматизированных системах
	ПКС-2.5 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью в автоматизированных системах	Знать: З8 - принципы подбора инструментальных средств тестирования систем защиты информации в АСУ
		Уметь: У8 - определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем
		Владеть: В8 - составлением методик тестирования систем защиты информации автоматизированных 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	2/3	22	22	-	100	Зачет
заочная	1/2	4	4	-	136	Зачет

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
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в курс.	2	2	-	10	14	УК-1.1, УК-1.2, УК-2.1 , ПКС-2.1,	устный опрос
2	2	Источники, риски и формы атак на информацию	4	4	-	18	26		устный опрос

3	3	Криптографические модели, алгоритмы шифрования	4	4	-	18	26	ПКС-2.2, ПКС-2.3, ПКС-2.4, ПКС-2.5	устный опрос
4	4	Политика безопасности, стандарты безопасности	4	4	-	18	26		устный опрос
5	5	Защита данных в операционных системах	4	4	-	18	26		устный опрос
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях	4	4	-	18	26		устный опрос
	зачёт		-	-	-	-	-		
		Итого:	22	22	-	100	144		

заочная форма обучения (ЗФО)

Таблица 5.1.2

№ 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 в курс.	0,5	-	-	16	16,5	УК-1.1, УК-1.2, УК-2.1 , ПКС-2.1, ПКС-2.2, ПКС-2.3, ПКС-2.4, ПКС-2.5	устный опрос, контрольная работа
2	2	Источники, риски и формы атак на информацию	0,5	0,5	-	24	25		устный опрос, контрольная работа
3	3	Криптографические модели, алгоритмы шифрования	0,5	1,	-	24	25,5		устный опрос, контрольная работа
4	4	Политика безопасности, стандарты безопасности	0,5	0,5	-	24	25		устный опрос, контрольная работа
5	5	Защита данных в операционных системах	1	1	-	24	26		устный опрос, контрольная работа
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях	1	1	-	20	22		устный опрос, контрольная работа
	зачёт		-	-	-	4	4		Подготовка к зачету
		Итого:	4	4	-	136	144		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Введение в курс». Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты. Дидактическая единица.

Раздел 2. «Источники, риски и формы атак на информацию». Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС

Раздел 3. «Криптографические модели, алгоритмы шифрования». Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.

Раздел 4. «Политика безопасности, стандарты безопасности». Понятие политики безопасности, основные типы политики безопасности. Дискреционная и мандатная модели безопасности. Концепция защиты средств вычислительной техники и АС от НСД. Классификация АС и требования по защите информации. Классы и группы защищенности средств вычислительной техники и АС от НСД и требования к ним. Руководящие документы России по защите от НСД к информации.

Раздел 5. «Защита данных в операционных системах». Модели безопасности и типовая архитектура подсистемы защиты операционной системы, основные функции. Разграничение доступа к объектам операционной системы, идентификация, аутентификация, авторизация субъектов доступа. Аудит. Основные компоненты системы безопасности ОС на примере семейств ОС Windows / Unix.

Раздел 6. «Многоуровневая защита корпоративных сетей; защита информации в сетях». Многоуровневая зашита корпоративных сетей. Сетевые протоколы защиты информации. Сканирование и мониторинг информационной безопасности.

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	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.
2	2	4	0,5	Источники, риски и формы атак на информацию
3	3	4	0,5	Криптографические модели, алгоритмы шифрования
4	4	4	0,5	Политика безопасности, стандарты безопасности
5	5	4	1	Защита данных в операционных системах
6	6	4	1	Многоуровневая защита корпоративных сетей; защита информации в сетях
Итого:		22	4	

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.		Тема практического занятия
		ОФО	ЗФО	
1	1	2	0,5	Источники, риски и формы атак на информацию
2	2	6	1	Криптографические модели, алгоритмы шифрования
3	3	4	0,5	Политика безопасности, стандарты безопасности
4	4	4	0,5	Защита данных в операционных системах
5	5	6	1,5	Многоуровневая защита корпоративных сетей; защита информации в сетях
Итого:		22	4	

Лабораторные работы

Лабораторные работы учебным планом не предусмотрены

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.		Тема	Вид СРС
		ОФО	ЗФО		
1	1	10	16	Введение в курс	подготовка к практическим занятиям
2	2	18	24	Источники, риски и формы атак на информацию	подготовка к практическим занятиям
3	3	18	24	Криптографические модели, алгоритмы шифрования	подготовка к практическим занятиям
4	4	18	24	Политика безопасности, стандарты безопасности	подготовка к практическим занятиям
5	5	18	24	Защита данных в операционных системах	подготовка к практическим занятиям
6	6	18	20	Многоуровневая защита корпоративных сетей; защита информации в сетях	подготовка к практическим занятиям
	1-6	-	4	Контроль	Подготовка к зачету
Итого:		100	136		

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

лекция-визуализация;

проблемная задача.

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 – 28 часов.

7.2. Тематика контрольных работ.

1. *Задача.* Исходные данные:
Сообщение: ПОНЕДЕЛЬНИК НАЧИНАЕТСЯ В СУББОТУ.
Ключ: ЗОНТ
Необходимо:
-зашифровать сообщение, используя алгоритм перестановки по столбцам.
2. *Задача.* Исходные данные:
Сообщение: ПРИЛЕТАЮ В ЧЕТВЕРГ
Алфавит: русский.
Ключ: ВОЛНА
Необходимо:
-зашифровать сообщение, используя алгоритм сложной замены.
3. Задача. Исходные данные:
Пусть некоторое сообщение M=5.
Определены следующие параметры для алгоритма шифрования RSA:
P=7 Q=11 K_o=13
Необходимо:
-найти секретный ключ K_c;
-зашифровать сообщение M;
-расшифровать сообщение M.
4. Задача. Исходные данные:
Для некоторого сообщения M известно, что
M= 7.
Определены следующие параметры для алгоритма El Gamal
P=31 G=2 X=3 K=11
Необходимо:
-найти открытый ключ Y;
-зашифровать сообщение M;
-расшифровать криптограмму и получить исходное сообщение M.
5. *Задача.* Исходные данные:
Пусть пользователям A и B необходимо обменяться общим секретным ключом с использованием алгоритма Диффи-Хеллмана.
Определены следующие параметры:
модуль P=97 G=2
Необходимо:
-самостоятельно определить значения ключей K_A и $K_{|B}$;
-рассчитать общий секретный ключ.

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	Работа на практических занятиях	30
2	Проверка результатов самостоятельной работы	10
3	Аттестация	10
	ИТОГО за первую текущую аттестацию	50

2 текущая аттестация		
1	Работа на практических занятиях	30
2	Проверка результатов самостоятельной работы	10
3	Аттестация	10
	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	Работа на практических занятиях	30
2	Проверка результатов самостоятельной работы (выполнение контрольной работы)	30
3	Тесты	30
4	Устный опрос	10
	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/модуля

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	Перечень технических средств обучения, необходимых для освоения

	дисциплины/модуля	дисциплины/модуля (демонстрационное оборудование)
-	-	Проектор, акустическая система (колонки), интерактивная доска Комплект учебно-наглядных пособий.

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим занятиям.

Проведение практических занятий направлено на закрепление полученных теоретических знаний о защите информации в автоматизированных системах управления.

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

дисциплины: Защита информации в автоматизированных системах управления
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	Критерии оценивания результатов обучения			
			1-2	3	4	5
УК-1	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.	Знать: З1 - системный подход при решении проблемных ситуаций; методы анализа своих проблемных ситуаций	Не знает системный подход при решении проблемных ситуаций; методы анализа своих проблемных ситуаций	Частично знает системный подход при решении проблемных ситуаций; методы анализа своих проблемных ситуаций	Знает системный подход при решении проблемных ситуаций; методы анализа своих проблемных ситуаций, но допускает незначительные ошибки	В полном объеме знает системный подход при решении проблемных ситуаций; методы анализа своих проблемных ситуаций
		Уметь: У1- принимать решения при проблемных ситуациях	Не умеет принимать решения при проблемных ситуациях	Частично умеет принимать решения при проблемных ситуациях	Умеет принимать решения при проблемных ситуациях, но допускает незначительные ошибки	В полном объеме умеет принимать решения при проблемных ситуациях
		Владеть: В1 - методами решения проблемных ситуаций	Не владеет методами решения проблемных ситуаций	Частично владеет методами решения проблемных ситуаций	Владеет методами решения проблемных ситуаций, но допускает незначительные ошибки	В полном объеме владеет методами решения проблемных ситуаций
	УК-1.2 Осуществляет поиск вариантов решения поставленной проблемной ситуации на	Знать: З2 актуальность и важность проблем защиты информации	Не знает актуальность и важность проблем защиты информации	Частично знает актуальность и важность проблем защиты информации	Знает актуальность и важность проблем защиты информации, но допускает незначительные ошибки	В полном объеме знает актуальность и важность проблем защиты информации

	основе доступных источников информации, определяет в рамках выбранного алгоритма вопросы (задачи), подлежащие дальнейшей разработке, предлагает способы их решения.	Уметь: У2 - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	Не умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	Частично умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	Умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам, но допускает незначительные ошибки	В полном объеме умеет пользоваться современной научно-технической информацией по исследуемым проблемам и задачам
		Владеть: В2 - терминологией в области защиты информации	Не владеет терминологией в области защиты информации	Частично владеет терминологией в области защиты информации	Владеет терминологией в области защиты информации, но допускает незначительные ошибки	В полном объеме владеет терминологией в области защиты информации
УК-2	УК-2.1 Разрабатывает концепцию проекта в рамках обозначенной проблемы, формулируя цель, задачи, актуальность, значимость (научную, практическую, методическую и иную в зависимости от типа проекта), ожидаемые результаты и возможные сферы их применения, разрабатывает план реализации про-	Знать: З3 - основные правила обеспечения информационной безопасности при разработке методик и инструкций	Не знает основные правила обеспечения информационной безопасности при разработке методик и инструкций	Частично знает основные правила обеспечения информационной безопасности при разработке методик и инструкций	Знает основные правила обеспечения информационной безопасности при разработке методик и инструкций, но допускает незначительные ошибки	В полном объеме знает основные правила обеспечения информационной безопасности при разработке методик и инструкций
		Уметь: У3 - разрабатывать рекомендации и методики, позволяющие обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения	Не умеет разрабатывать рекомендации и методики, позволяющие обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения	Частично умеет разрабатывать рекомендации и методики, позволяющие обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения	Умеет разрабатывать рекомендации и методики, позволяющие обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения, но допускает незначительные ошибки	В полном объеме умеет разрабатывать рекомендации и методики, позволяющие обеспечить сохранность данных при попытке несанкционированного доступа, утечки и разглашения

	екта и осуществляет мониторинг хода его реализации	Владеть: В3 - навыками применения рекомендаций и методик по совершенствованию информационной безопасности	Не владеет навыками применения рекомендаций и методик по совершенствованию информационной безопасности	Частично владеет навыками применения рекомендаций и методик по совершенствованию информационной безопасности	Владеет навыками применения рекомендаций и методик по совершенствованию информационной безопасности, но допускает незначительные ошибки	В полном объеме владеет навыками применения рекомендаций и методик по совершенствованию информационной безопасности
ПКС-2	ПКС-2.1 Применяет действующую нормативную базу в области обеспечения информационной безопасности	Знать: З4 - нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Не знает нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Частично знает нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Знает нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации, но допускает незначительные ошибки	В полном объеме знает нормативные правовые акты в области защиты информации; принципы формирования политики информационной безопасности в автоматизированных системах; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
		Уметь: У4 - применять действующую нормативную базу в области обеспечения безопасности информации	Не умеет применять действующую нормативную базу в области обеспечения безопасности информации	Частично умеет применять действующую нормативную базу в области обеспечения безопасности информации	Умеет применять действующую нормативную базу в области обеспечения безопасности информации, но допускает незначительные ошибки	В полном объеме умеет применять действующую нормативную базу в области обеспечения безопасности информации

		Владеть: В4 - навыками применения действующей нормативной базы в области обеспечения информационной безопасности	Не владеет навыками применения действующей нормативной базы в области обеспечения информационной безопасности	Частично владеет навыками применения действующей нормативной базы в области обеспечения информационной безопасности	Владеет навыками применения действующей нормативной базы в области обеспечения информационной безопасности, но допускает незначительные ошибки	В полном объеме владеет навыками применения действующей нормативной базы в области обеспечения информационной безопасности
	ПКС-2.2 Рассматривает виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Знать: З5 - принципы организации и структуру систем защиты информации автоматизированных систем	Не знает принципы организации и структуру систем защиты информации автоматизированных систем	Частично знает принципы организации и структуру систем защиты информации автоматизированных систем	Знает принципы организации и структуру систем защиты информации автоматизированных систем, но допускает незначительные ошибки	В полном объеме знает принципы организации и структуру систем защиты информации автоматизированных систем
		Уметь: У5 - определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Не умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Частично умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации, но допускает незначительные ошибки	В полном объеме умеет определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации
		Владеть: В5 - методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Не владеет методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Частично владеет методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации	Владеет методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации, но допускает незначительные ошибки	В полном объеме владеет методикой выбора средств защиты информации, обеспечивающих реализацию технических мер защиты информации

	ПКС-2.3 Анализирует структурные и функциональные схемы защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знать: З6 - принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Не знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Частично знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности, но допускает незначительные ошибки	В полном объеме знает принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей и их компонентов; методики проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
		Уметь: У6 - анализировать основные узлы и устройства современных автоматизированных систем	Не умеет анализировать основные узлы и устройства современных автоматизированных систем	Частично умеет анализировать основные узлы и устройства современных автоматизированных систем	Умеет анализировать основные узлы и устройства современных автоматизированных систем, но допускает незначительные ошибки	В полном объеме умеет анализировать основные узлы и устройства современных автоматизированных систем

		Владеть: В6 - навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Не владеет навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Частично владеет навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности	Владеет навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности, но допускает незначительные ошибки	В полном объеме владеет навыками проведения анализа структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности
	ПКС-2.4 Анализирует и выявляет основные угрозы информационной безопасности в автоматизированных системах	Знать: З7 - основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Не знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Частично умеет основные угрозы безопасности информации и модели нарушителя в автоматизированных системах	Умеет основные угрозы безопасности информации и модели нарушителя в автоматизированных системах, но допускает незначительные ошибки	В полном объеме умеет основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
		Уметь: У7 - анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	Не умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	Частично умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации	Умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, но допускает незначительные ошибки	В полно объеме умеет анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации
		Владеть: В7 - навыком выявлять основные угрозы информационной безопасности в автоматизированных системах	Не владеет навыком выявлять основные угрозы информационной безопасности в автоматизированных системах	Частично владеет навыком выявлять основные угрозы информационной безопасности в автоматизированных системах	Владеет навыком выявлять основные угрозы информационной безопасности в автоматизированных системах, но допускает незначительные ошибки	В полном объеме владеет навыком выявлять основные угрозы информационной безопасности в автоматизированных системах

	ПКС-2.5 Разрабатывает предложения по совершенствованию системы управления информационной безопасностью в автоматизированных системах	Знать: З8 - принципы подбора инструментальных средств тестирования систем защиты информации в АСУ	Не знает принципы подбора инструментальных средств тестирования систем защиты информации в АСУ	Частично знает принципы подбора инструментальных средств тестирования систем защиты информации в АСУ	Знает принципы подбора инструментальных средств тестирования систем защиты информации в АСУ, но допускает незначительные ошибки	В полном объеме знает принципы подбора инструментальных средств тестирования систем защиты информации в АСУ
		Уметь: У8 - определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Не умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Частично умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем	Умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем, но допускает незначительные ошибки	В полном объеме умеет определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем
		Владеть: В8 - составлением методик тестирования систем защиты информации автоматизированных систем	Не владеет составлением методик тестирования систем защиты информации автоматизированных систем	Частично владеет составлением методик тестирования систем защиты информации автоматизированных систем	Владеет составлением методик тестирования систем защиты информации автоматизированных систем, но допускает незначительные ошибки	В полном объеме владеет составлением методик тестирования систем защиты информации автоматизированных систем

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина Защита информации в автоматизированных системах управления
Код, 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	Малюк, А. А. Защита информации в информационном обществе: учебное пособие / А. А. Малюк. — Москва : Горячая линия-Телеком, 2015. — 230 с. — Режим доступа: https://e.lanbook.com/book/94632	ЭР	30	100	+
2	Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — Режим доступа: https://e.lanbook.com/book/111075	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.