Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Клочков Юрий Сергеевич
Должность: Ректор
Дата подписания: 14.10.2026 15:07:07
Уникальный программный ключ:
3beb265d5d589e7ff4c954946f3ad99a1e70ac12

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

УТВЕРЖДАЮ

И.о. заведующего кафедрой
_____В.А. Копырин
«_____» _____20___г.

РАБОЧАЯ ПРОГРАММА

Дисциплины: **Информационная безопасность систем управления технологическими процессами**

направление подготовки: **27.03.04 Управление в технических системах**

направленность (профиль): **Интеллектуальные системы и средства автоматизированного управления**

форма обучения: **очная**

Рабочая программа рассмотрена
на заседании кафедры кибернетических систем

Протокол № _____от «__» _____20__г.

1. Цели и задачи освоения дисциплины

Цель 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.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к Блоку 1 части, формируемой участниками образовательных отношений.

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 вычислительных системах и компьютерных сетях.

Содержание дисциплины является логическим продолжением содержания дисциплин: «Информационные сети и телекоммуникации», «Вычислительные машины, системы и сети», «Правовая культура», и служит основой для выполнения ВКР.

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)
ПКС-2 Способен участвовать в эксплуатации объектов профессиональной деятельности	**ПКС-2.1.** Разбирается в особенностях автоматизированных систем управления производствами, в характере производственных процессов, в месте этих систем в общей структуре управления предприятием и специфике решаемых ими задач по оперативному управлению производством.	Знать: З1 - современные технологии и методы защиты информации в автоматизированных системах управления производством.
		Уметь: У1 - выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.
		Владеть: В1 – способами, средствами и методами применения современных

		технологий защиты информации в инфокоммуникационных системах и компьютерных сетях.
	ПКС-2.5. Решает стандартные задачи профессиональной деятельности на основе требований нормативно-технической документации	Знать: З2 – требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.
		Уметь: У2 - выбирать современные способы, средства и методы обеспечения необходимых показателей качества информационной безопасности автоматизированных производств.
		Владеть: В2 - навыками работы с нормативно-правовой документацией в сфере информационной безопасности.
	ПКС-2.6. Демонстрирует знание теоретических основ оценки надежности автоматизированных систем управления технологическими процессами, методов оценки эффективности и надёжности систем управления	Знать: З3 – теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.
		Уметь: У3 - обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.
		Владеть: В3 – методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.

4. Объем дисциплины/ модуля

Общий объем дисциплины составляет 4 зачетных единиц, 144 часа.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
очная	4/8	22	0	22	64	36	экзамен

5. Структура и содержание дисциплины/модуля

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 [2]
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в курс. Источники, риски и формы атак на информацию.	2	0	0	6	8	ПКС-2.1, ПКС-2.5, ПКС-2.6	Собеседование, тест

2	2	Источники, риски и формы атак на информацию.	4	0	0	10	14		Собеседование, тест
3	3	Криптографические модели, алгоритмы шифрования.	4	0	6	12	22		Тест, отчет по лабораторной работе
4	4	Политика безопасности, стандарты безопасности.	4	0	2	12	18		Тест, отчет по лабораторной работе
5	5	Защита данных в операционных системах	4	0	6	12	22		Тест, отчет по лабораторной работе
6	6	Многоуровневая защита корпоративных сетей; защита информации в сетях.	4	0	8	12	24		Тест, отчет по лабораторной работе
7	Экзамен		0	0	0	36	36		Тест
Итого:			22	0	22	100	144		

заочная форма обучения (ЗФО) не предусмотрена

5.2 Содержание дисциплины.

5.2.1 Содержание разделов дисциплины (дидактические единицы).

Раздел 1. Введение в курс. Источники, риски и формы атак на информацию. Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.

Раздел 2. Источники, риски и формы атак на информацию. Анализ и классификация источников угроз безопасности автоматизированных систем (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 электронной цифровой подписи (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 несанкционированного доступа (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 Гостехкомиссии 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 защита 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	Тема лекции		
		ОФО	ЗФО	
1	1	2	-	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.
2	2	4	-	Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС
3	3	4	-	Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.
4	4	4	-	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 Гостехкомиссии России по защите от НСД к информации.
5	5	4	-	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.
6	6	4	-	Многоуровневая зашита корпоративных сетей. Сетевые протоколы.
Итого:		22	-	

Практические занятия

Не предусмотрены

Лабораторные работы

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Наименование лабораторной работы		
		ОФО	ЗФО	
1	3	6	-	Лабораторная работа № 1. Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей
2	4	2	-	Лабораторная работа №2. Разработка программы разграничения полномочий пользователей на основе парольной аутентификации
3	5	4	-	Лабораторная работа №3.Разработка и программная реализация криптографических алгоритмов
4	5	2	-	Лабораторная работа №4. Использование функций криптографического интерфейса Windows для защиты информации
5	6	4	-	Лабораторная работа №5. Изучение программных средств шифрования, компьютерной стеганографии и защиты от вредоносных программ
6	6	4	-	Лабораторная работа №6. Защита программного обеспечения от несанкционированного использования и копирования
Итого:		22	-	-

Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины	Тема			Вид СРС
		ОФО	ЗФО		

1	1	6	-	Основные понятия и определения. Информация. Защита информации. Автоматизированная система обработки данных (АСОД) как объект защиты.	Изучение теоретического материала. Подготовка к тестированию.
2	2	10	-	Анализ и классификация источников угроз безопасности АС, виды атак на информационные ресурсы. Основные принципы и подходы обеспечения информационной безопасности АС	Изучение теоретического материала. Подготовка к тестированию.
3	3	12	-	Криптографические системы и протоколы: история развития, принципы функционирования, математическая основа, основные алгоритмы. Протоколы ЭЦП.	Изучение теоретического материала. Подготовка к лабораторным работам. Оформление отчета по лабораторным работам. Подготовка к защите лабораторных работ и тестированию.
4	4	12	-	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 Гостехкомиссии России по защите от НСД к информации.	Изучение теоретического материала. Подготовка к лабораторным работам. Оформление отчета по лабораторным работам. Подготовка к защите лабораторных работ и тестированию.
5	5	12	-	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.	Изучение теоретического материала. Подготовка к лабораторным работам. Оформление отчета по лабораторным работам. Подготовка к защите лабораторных работ и тестированию.
6	6	12	-	Многоуровневая зашита корпоративных сетей. Сетевые протоколы защиты информации. Сканирование и мониторинг информационной безопасности.	Изучение теоретического материала. Подготовка к лабораторным работам. Оформление отчета по лабораторным работам. Подготовка к защите лабораторных работ и тестированию.
	1-6	36		Подготовка к экзамену	
Итого:		100	-		

5.2.3 Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

-визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);

- работа на компьютерах(лабораторные занятия);

6 Тематика курсовых работ/проектов

Курсовая работа не предусмотрено.

7 Контрольные работы

В учебном плане не запланированы.

8. Оценка результатов освоения дисциплины/модуля

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	Собеседование	10
2	Выполнение и защита лабораторных работ	20
	ИТОГО за первую текущую аттестацию	30
2 текущая аттестация		
1	Выполнение и защита лабораторных работ	40
2	Тестирование	30
	ИТОГО за вторую текущую аттестацию	70
	ВСЕГО	**100**

9. Учебно-методическое и информационное обеспечение дисциплины/модуля

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»

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

1. Microsoft Office Professional Plus;
2. Windows 8.
3. Маткад.
4. Матлаб и FuzzyTech.

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	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно- наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1	Информационное обеспечение систем управления	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации Оснащенность: Учебная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте, проектор, проекционный экран.	625001, Тюменская область, г. Тюмень, ул. Мельникай те, д. 70 625001, Тюменская область, г. Тюмень, ул. 50 лет Октября, д. 38
		Лабораторные занятия: Производственная мебель: столы, стулья, доска аудиторная. Компьютер в комплекте (16 шт.).	625001, Тюменская область, г. Тюмень, ул. Мельникай те, д. 70 625001, Тюменская область, г. Тюмень, ул. 50 лет Октября, д. 38

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к лабораторным занятиям.

Проведение практических занятий направлено на закрепление полученных теоретических знаний по

дисциплине «Информационная безопасность систем управления технологическими процессами». Каждое лабораторное занятие имеет наименование и цель работы, основные теоретические положения, методику выполнения лабораторной работы, а также контрольные вопросы. После выполнения лабораторной работы, 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: Информационная безопасность систем управления технологическими процессами
Код, направление подготовки: 27.03.04 Управление в технических системах
Направленность (профиль): Интеллектуальные системы и средства автоматизированного управления

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-2	**ПКС-2.1.** Разбирается в особенностях автоматизированных систем управления производствами, в характере производственных процессов, в месте этих систем в общей структуре управления предприятием и специфике решаемых ими задач по оперативному управлению производством.	Знать: З1 - современные технологии и методы защиты информации в автоматизированных системах управления производством.	Не знает современные технологии и методы защиты информации в автоматизированных системах управления производством.	Удовлетворительно знает современные технологии и методы защиты информации в автоматизированных системах управления производством.	Хорошо знает современные технологии и методы защиты информации в автоматизированных системах управления производством.	Отлично знает современные технологии и методы защиты информации в автоматизированных системах управления производством.
		Уметь: У1 - выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Не умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Удовлетворительно умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Хорошо умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Отлично умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.
		Владеть: В1 – способами, средствами и методами применения современных технологий защиты информации в инфокоммуникационных системах и	Не владеет способами, средствами и методами применения современных технологий защиты информации в инфокоммуникацион	Удовлетворительно владеет способами, средствами и методами применения современных технологий защиты	Хорошо владеет способами, средствами и методами применения современных технологий защиты информации в инфокоммуникаци	Отлично владеет способами, средствами и методами применения современных технологий защиты информации в инфокоммуникацио

		компьютерных сетях.	ных системах и компьютерных сетях.	информации в инфокоммуникационных системах и компьютерных сетях.	онных системах и компьютерных сетях.	нных системах и компьютерных сетях.
	ПКС-2.5. Решает стандартные задачи профессиональной деятельности на основе требований нормативно-технической документации	Знать: З2 – требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.	Не знает требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.	Удовлетворительно знает требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.	Хорошо знает требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.	Отлично знает требования отраслевых, национальных и международных стандартов в области обеспечения информационной безопасности.
		Уметь: У2 - выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Не умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Удовлетворительно умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Хорошо умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.	Отлично умеет выбирать современные способы, средства и методы обеспечения информационной безопасности автоматизированных производств.
		Владеть: В2 - навыками работы с нормативно-правовой документацией в сфере информационной безопасности.	Не владеет навыками работы с нормативно-правовой документацией в сфере информационной безопасности.	Удовлетворительно владеет навыками работы с нормативно-правовой документацией в сфере информационной безопасности.	Хорошо владеет навыками работы с нормативно-правовой документацией в сфере информационной безопасности.	Отлично владеет навыками работы с нормативно-правовой документацией в сфере информационной безопасности.

	ПКС-2.6. Демонстрирует знание теоретических основ оценки надежности автоматизированных систем управления технологическими процессами, методов оценки эффективности и надёжности систем управления	Знать: З3 – теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.	Не знает теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.	Удовлетворительно знает теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.	Хорошо знает теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.	Отлично знает теоретические основы обеспечения требуемого качества надежности и защищенности инфокоммуникационного оборудования.
		Уметь: У3 - обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.	Не умеет обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.	Удовлетворительно умеет обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.	Хорошо умеет обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.	Отлично умеет обеспечивать требуемую защиту сетевых устройств, входящих в состав инфокоммуникационной системы, от несанкционированного доступа.
		Владеть: В3 – методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.	Не владеет методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.	Удовлетворительно владеет методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.	Хорошо владеет методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.	Отлично владеет методами обеспечения требуемого уровня надежности и безопасности инфокоммуникационной системы.

Приложение 2

КАРТА

обеспеченности дисциплины (модуля) учебной и учебно-методической литературой

Дисциплина: Информационная безопасность систем управления технологическими процессами
Код, направление подготовки: 27.03.04 Управление в технических системах
Направленность (профиль): Интеллектуальные системы и средства автоматизированного управления

№ п/п	Названиеучебного,учебно-методическогоиздания, автор,издательство, вид издания, год издания	Количествоэкземпляров вБИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного вариантав ЭБС (+/-)
1	**Рябко, Б.Я.** Криптографические методы защиты информации : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2012. — 229 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/5193	ЭР	20	100	ЭБС Лань
2	**Романьков, В. А.** Введение в криптографию [Текст] : курс лекций : студентам вузов / В. А. Романьков. - 2-е изд., испр. и доп. - Москва : ФОРУМ, 2012. - 239 с.	15	20	100	-
3	**Мельников, В.П. Методы и средства хранения и защиты компьютерной информации** [Текст]: учебник для студентов вузов, обучающихся по направлениям: "Автоматизация технологических процессов и производств", "Конструкторско-технологическое обеспечение машиностроительных производств" / В. П. Мельников, А. Г. Схиртладзе ; ред. В. П. Мельников. - Старый Оскол : ТНТ, 2014. - 399 с	15	20	100	-