

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Клочков Юрий Сергеевич
Должность: и.о. ректора
Дата подписания: 03.09.2024 11:38:39
Уникальный программный ключ:
4e7c4ea90328ec8e65c5d8058549a2538d7400d1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:

Председатель КСН



М.Л. Белоножко

« 31 » мая 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины: Управление информационной безопасностью и защита информации

направление подготовки: 27.04.03 Системный анализ и управление

направленность: Управление социально-экономическими системами

форма обучения: заочная

Рабочая программа разработана в соответствии с утвержденным учебным планом от 27.05.2021 г. и требованиями ОПОП ВО по направлению подготовки 27.04.03 Системный анализ и управление, направленность: Управление социально-экономическими системами к результатам освоения дисциплины «Управление информационной безопасностью и защита информации».

Рабочая программа рассмотрена на заседании кафедры бизнес-информатики и математики

Протокол № 12 от « 27 » мая 2021 г.

Заведующий кафедрой БИМ



О.М. Барбаков

СОГЛАСОВАНО:



Заведующий выпускающей кафедрой _____ М. Л. Белоножко
«31» мая 2021 г.

Рабочую программу разработал:



А.Н. Величко, старший преподаватель кафедры БИМ

1. Цели и задачи освоения дисциплины

Цель дисциплины заключается в овладении теоретическими знаниями и умениями, развитии навыков практических действий по планированию, организации и проведению работ по обеспечению информационной безопасности в условиях существования угроз безопасности информации.

Задачи дисциплины:

- изучение нормативных правовых и организационных основ обеспечения информационной безопасности;
- формирование умений выявления и формулирования требований к обеспечению информационной безопасности;
- формирование умений планирования, реализации, и контроля процесса управления информационной безопасностью;
- формирование навыков проведения работ по обеспечению информационной безопасности;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части Блока 1, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины «Системное и критическое мышление» является логическим продолжением содержания дисциплин: «Информационно-коммуникативные технологии», «Защита интеллектуальной собственности».

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1. Применяет методы управления командной работой с учетом требований информационной безопасности	Знать: 3.3.1 методы и средства управления информационной безопасностью Уметь: У.3.1 осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью Владеть: В.3.1 практическими навыками оценки и совершенствование процесса управления информационной безопасностью
ПКС -3. Способен управлять аналитическими ресурсами и компетенциями	ПКС-3.1. Применяет знания теории управления ресурсами	Знать: 3.3.1 методы и средства управления информационной безопасностью Уметь: У.3.1 осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью

		Владеть: В.3.1 практическими навыками оценки и совершенствование процесса управления информационной безопасностью
	ПКС-3.5. Организует процесс разработки и развития профилей компетенций в области информационной безопасности	Уметь: У.3.5 организовать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности Владеть: В.3.5 технологиями разработки и развития профилей компетенций в области информационной безопасности

4. Объем дисциплины

Общий объем дисциплины составляет 5 зачетных единиц, 180 часов.

Таблица 4.1.

Форма обучения	Курс/ семестр	Аудиторные занятия/контактная работа, час.			Самостоятельная работа, час.	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия		
заочная	2/4	6	6	8	151+9	экзамен

5. Структура и содержание дисциплины

9.3. Структура дисциплины.

Очная форма обучения (ОФО)

Не реализуется

Заочная форма обучения (ЗФО) – 4 семестр

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	Общие положения информационной безопасности	1	1	1	21	24	УК-3.1 ПКС-3.1 ПКС-3.5	Задание к лабораторной работе № 1, вопросы для защиты
2	2	Разработка системы управления информационной безопасностью	1	1	2	40	44		Задание к лабораторной работе № 2, вопросы для защиты
3	3	Внедрение и обеспечение функционирования системы управления информационной безопасностью	1	1	2	30	34		Задание к лабораторной работе № 3, вопросы для защиты
4	4	Проведение мониторинга и анализа системы управления информационной безопасностью	1	1	1	20	23		Задание к лабораторной работе № 4, вопросы для защиты
5	5	Поддержка и улучшение системы управления	1	1	1	20	23		Задание к лабораторной работе №

		информационной безопасностью							5, вопросы для защиты
6	6	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	1	1	1	20	23		Задание к лабораторной работе № 6, вопросы для защиты
7	Экзамен						9	УК-3.1 ПКС-3.1 ПКС-3.5	Вопросы для экзамена
Итого:			6	6	8	151	180		

5.2. Содержание дисциплины.

5.2.1. Содержание разделов дисциплины (дидактические единицы).

Раздел 1. «Общие положения информационной безопасности».

Основные понятия в области информационной безопасности. Нормативно-правовые акты, специальные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.

Раздел 2. «Разработка системы управления информационной безопасностью».

Область и границы действия системы управления информационной безопасностью. Методика оценки угроз безопасности информации. Уязвимости. Оценка и варианты обработки рисков информационной безопасности. Выбор целей и мер управления для обработки рисков информационной безопасности, утверждение остаточных рисков информационной безопасности.

Раздел 3. «Внедрение и обеспечение функционирования системы управления информационной безопасностью».

Разработка и реализация плана обработки рисков информационной безопасности. Внедрение мер управления информационной безопасностью. Организационно-технические аспекты обеспечения безопасности информации. Принципы обеспечения информационной безопасности в социальных сетях. Принципы обеспечения безопасных вычислений в распределенных вычислительных средах. Принципы обеспечения безопасности данных в облачных хранилищах данных. Принципы обеспечения безопасности при обработке потоковых данных в реальном времени. Принципы обеспечения защиты конфиденциальности при крупномасштабном поиске и анализе информации. Принципы обеспечения информационной безопасности при передаче информации. Управление работой и ресурсами системы управления информационной безопасностью. Обнаружение событий информационной безопасности и реагирование на инциденты.

Раздел 4. «Проведение мониторинга и анализа системы управления информационной безопасностью».

Процедуры мониторинга и анализа результативности системы управления информационной безопасностью. Внутренний аудит системы управления информационной безопасностью. Регистрация действий и событий информационной безопасности.

Раздел 5. «Поддержка и улучшение системы управления информационной безопасностью».

Выявление возможности улучшения системы управления информационной безопасностью. Корректирующие и предупреждающие действия. Внедрение улучшений.

Раздел 6. «Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий».

Охраняемые результаты интеллектуальной деятельности и средства индивидуализации. Споры, связанные с защитой интеллектуальных прав. Защита интеллектуальных прав. Защита личных неимущественных прав. Защита исключительных прав. Особенности защиты прав лицензиата. Технические средства защиты авторских прав и интеллектуальной собственности.

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	ОЗФО	
1	1	-	1	-	Общие положения информационной безопасности
2	2	-	1	-	Разработка системы управления информационной безопасностью
3	3	-	1	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	-	1	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	-	1	-	Поддержка и улучшение системы управления информационной безопасностью
6	6	-	1	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		-	6	-	-

Практические занятия

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	-	1	-	Общие положения информационной безопасности
2	2	-	1	-	Разработка системы управления информационной безопасностью
3	3	-	1	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	-	1	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	-	1	-	Поддержка и улучшение системы управления информационной безопасностью
6	6	-	1	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		-	6	-	-

Лабораторные работы

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	-	1	-	Общие положения информационной безопасности
2	2	-	2	-	Разработка системы управления информационной безопасностью
3	3	-	2	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью
4	4	-	1	-	Проведение мониторинга и анализа системы управления информационной безопасностью
5	5	-	1	-	Поддержка и улучшение системы управления информационной безопасностью
6	6	-	1	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий
Итого:		-	8	-	-

Самостоятельная работа студента

Таблица 5.2.4

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	-	21	-	Общие положения информационной безопасности	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
2	2	-	40	-	Разработка системы управления информационной безопасностью	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
3	3	-	30	-	Внедрение и обеспечение функционирования системы управления информационной безопасностью	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
4	4	-	20	-	Проведение мониторинга и анализа системы управления информационной безопасностью	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
5	5	-	20	-	Поддержка и улучшение системы управления информационной безопасностью	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
6	6	-	20	-	Основы охраны авторских прав и интеллектуальной собственности в сфере информационных технологий	Подготовка к практическим занятиям, оформление отчетов по практическим занятиям
Итого:		-	151	-		

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

- информационно-телекоммуникационная (лекционные занятия, практические, лабораторные занятия)
- групповая (практические, лабораторные занятия)
- индивидуальная (практические, лабораторные занятия)
- рейтинговая (практические, лабораторные занятия)

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

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

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

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1	2	3
1.1	Выполнение и защита лабораторной работы № 1	15
1.2	Выполнение и защита лабораторной работы № 2	20

1.3	Выполнение и защита лабораторной работы № 3	20
1.4	Выполнение и защита лабораторной работы № 4	15
1.5	Выполнение и защита лабораторной работы № 5	15
1.6	Выполнение и защита лабораторной работы № 6	15
	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:

- ЭБС «Издательства Лань»;
- ЭБС «Электронного издательства ЮРАЙТ»;
- Собственная полнотекстовая база (ПБД) БИК ТИУ;
- Научная электронная библиотека «eLIBRARY.RU»;
- ЭБС «IPRbooks»;
- Научно-техническая библиотека ФГБОУ ВО РГУ нефти и газа имени И.М. Губкина;
- Научно-техническая библиотека ФГБОУ ВО УГНТУ (г. Уфа);
- Научно-техническая библиотека ФГБОУ ВО УГТУ (г. Ухта);
- ЭБС «Проспект»;
- ЭБС «Консультант студент».

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

- Microsoft Windows;
- Microsoft Office Professional Plus;
- Oracle VirtualBox;
- Nessus;
- Nmap;
- Wireshark;
- John the Ripper;
- Snort;
- SecretNet;
- VipNet;
- OpenVPN;
- КриптоПро;

10. Материально-техническое обеспечение дисциплины

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

Таблица 10.1

№ п/п	Перечень оборудования, необходимого для освоения дисциплины/модуля	Перечень технических средств обучения, необходимых для освоения дисциплины/модуля (демонстрационное оборудование)
1	Персональные компьютеры	Комплект мультимедийного оборудования: проектор, экран, колонки, интерактивная доска, персональные компьютеры. Локальная и корпоративная сеть.

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим, лабораторным занятиям.

Практические, лабораторные занятия способствуют углублённому изучению дисциплины и служат основной формой подведения итогов самостоятельной работы студентов. Цель практических занятий заключается в углублении и закреплении теоретических знаний, а также в формировании практических компетенций, необходимых будущим специалистам.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику будущих функциональных обязанностей обучающихся, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Студенту рекомендуется следующая схема подготовки к занятию:

- проработать конспект лекций;
- изучить рекомендованную литературу;
- при затруднениях сформулировать вопросы к преподавателю;
- после выполнения практического задания оформить отчет и подготовиться к защите.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

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. 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, решение вариативных задач, 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.

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Управление информационной безопасностью и защита информации

Код, направление подготовки: 27.04.03 Системный анализ и управление

Направленность: Управление социально-экономическими системами

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
УК-3	Знать: УК-3.1 3.3.1 методы и средства управления информационной безопасностью	Не знает основные методы и средства управления информационной безопасностью	Демонстрирует знание некоторых методов и средств управления информационной безопасностью	Демонстрирует достаточные знания методов и средств управления информационной безопасностью	Демонстрирует исчерпывающие знания о методах и средствах управления информационной безопасностью
	Уметь: УК-3.1 У.3.1 - осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью	Не умеет осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью	Демонстрирует отдельные умения осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью	Демонстрирует достаточные умения осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью	Демонстрирует исчерпывающие умения осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью
	Владеть: УК-3.1 В 3.3.1 - практическими навыками оценки и совершенствования процесса управления информационной безопасностью	Не владеет практическими навыками оценки и совершенствования процесса управления информационной безопасностью	Демонстрирует отдельные практические навыки оценки и совершенствования процесса управления информационной безопасностью	Демонстрирует достаточные практические навыки оценки и совершенствования процесса управления информационной безопасностью	Демонстрирует исчерпывающие практические навыки оценки и совершенствования процесса управления информационной безопасностью
ПКС -3	Знать: ПКС-3.1 3.3.1 - методы и средства управления информационной безопасностью	Не знает методы и средства управления информационной безопасностью	Демонстрирует отдельные знания методов и средств управления информационной безопасностью	Демонстрирует достаточные знания методов и средств управления информационной безопасностью	Демонстрирует исчерпывающие знания методов и средств управления информационной безопасностью

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Уметь: ПКС-3.1 У.3.1 - осуществлять управление процессами, оценку и контроль качества процесса управления информационно й безопасностью	Не умеет осуществлять управление процессами, оценку и контроль качества процесса управления информационно й безопасностью	Демонстрирует отдельные умения осуществлять управление процессами, оценку и контроль качества процесса управления информационно й безопасностью	Демонстрирует достаточные умения осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью	Демонстрирует исчерпывающие умения осуществлять управление процессами, оценку и контроль качества процесса управления информационной безопасностью
	Владеть: ПКС-3.1 В.3.1 - практическими навыками оценки и совершенствование процесса управления информационно й безопасностью	Не владеет практическими навыками оценки и совершенствование процесса управления информационно й безопасностью	Частично владеет практическими навыками оценки и совершенствование процесса управления информационно й безопасностью	Хорошо владеет практическими навыками оценки и совершенствование процесса управления информационной безопасностью	В совершенстве владеет практическими навыками оценки и совершенствование процесса управления информационной безопасностью
	Владеть: ПКС-3.5 В 3.5 технологиями разработки и развития профилей компетенций в области информационной безопасности	Не владеет технологиями разработки и развития профилей компетенций в области информационной безопасности	Демонстрирует отдельные практические навыки разработки и развития профилей компетенций в области информационной безопасности	Демонстрирует достаточные практические навыки разработки и развития профилей компетенций в области информационной безопасности	Демонстрирует исчерпывающие практические навыки разработки и развития профилей компетенций в области информационной безопасности
	Уметь: ПКС-3.5 У.3.5 - организовать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности	Не умеет организовывать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности	Демонстрирует отдельные умения организовывать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности	Демонстрирует достаточные умения организовывать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности	Демонстрирует исчерпывающие умения организовывать процесс разработки различных компетенций для социально-экономических систем с учетом требований в области информационной безопасности

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1-2	3	4	5
	Владеть: ПКС-3.5 В.3.5 - технологиями разработки и развития профилей компетенций в области информационной безопасности	Не владеет технологиями разработки и развития профилей компетенций в области информационной безопасности	Владеет технологиями разработки и развития профилей компетенций в области информационной безопасности	Хорошо владеет технологиями разработки и развития профилей компетенций в области информационной безопасности	В совершенстве владеет технологиями разработки и развития профилей компетенций в области информационной безопасности

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Управление информационной безопасностью и защита информации

Код, направление подготовки: 27.04.03 Системный анализ и управление

Направленность: Управление социально-экономическими системами

№ 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	Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. - Москва: Издательство Юрайт, 2020. - 309 с. - (Бакалавр и магистр. Академический курс). - ЭБС "Юрайт". - ISBN 978-5-534-04732-5 https://urait.ru/bcode/449285	ЭР	15	100	+
2	Защита информации: учебное пособие для вузов / А. А. Внуков. - 3-е изд., пер. и доп. - Москва: Издательство Юрайт, 2021. - 161 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-534-07248-8 https://urait.ru/bcode/470131	ЭР	15	100	+
3	Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020. - 312 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-9916-9043-0 https://urait.ru/bcode/452368	ЭР	15	100	+
4	Основы информационной безопасности: учебное пособие / С. А. Нестеров. - 4-е изд., стер. - Санкт-Петербург: Лань, 2018. - 324 с. - ЭБС Лань. - ISBN 978-5-8114-2290-6 https://e.lanbook.com/book/103908	ЭР	15	100	+
5	Информационная безопасность и защита информации: практикум / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. - Дубна: Государственный университет «Дубна», 2020. - 85 с. - ЭБС "Лань". - ISBN 978-5-89847-608-3 https://e.lanbook.com/book/154490	ЭР	15	100	+
6	Бабенко, Л.К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. - Москва: Юрайт, 2020. - 220 с. - (Высшее образование). - ЭБС "Юрайт". - ISBN 978-5-9916-9244-1 https://urait.ru/bcode/452871	ЭР	15	100	+

7	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 http://www.iprbookshop.ru/87643.html	ЭР	15	100	+
8	Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2019. - 344 с. - ЭБС Лань. - ISBN 978-5-8114-3940-9 https://e.lanbook.com/book/125739	ЭР	15	100	+
9	Информационная безопасность и защита информации / В. Ф. Шаньгин. - Саратов: Профобразование, 2019. - 702 с. - ЭБС "IPR BOOKS". - ISBN 978-5-4488-0070-2 http://www.iprbookshop.ru/87995.html	ЭР	15	100	+
10	Основы информационной безопасности: учебное пособие / В. А. Галатенко. - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Эр Медиа, 2020. - 266 с. - URL: http://www.iprbookshop.ru/97562.html	ЭР	15	100	+

Заведующий кафедрой БИМ



О.М. Барбаков

Директор БИК _____



Д.Х. Каюкова

**Дополнения и изменения
к рабочей программе дисциплины**

Управление информационной безопасностью и защита информации
на 2023 - 2024 учебный год

С учётом развития науки, практики, технологий и социальной сферы, а также результатов мониторинга потребностей работодателей, в рабочую программу вносятся следующие дополнения (изменения):

№	Вид дополнений/изменений	Содержание дополнений/изменений, вносимых в рабочую программу
1	Актуализация современных профессиональных баз данных и информационных справочных систем	<p>Изложить п.9.2 в следующей редакции:</p> <p>9.2. Современные профессиональные базы данных и информационные справочные системы:</p> <ul style="list-style-type: none"> – Электронно-библиотечная система (обеспечивающая доступ, в том числе к профессиональным базам данных) ООО «ЭБС ЛАНЬ» https://e.lanbook.com – «Образовательная платформа ЮРАЙТ» (обеспечивающая доступ, в том числе к профессиональным базам данных) «Электронного издательства ЮРАЙТ» www.urait.ru – Электронная библиотека/Электронный каталог Тюменского индустриального университета http://webirbis.tsogu.ru/ – Научная электронная библиотека «eLIBRARY.RU» (обеспечивающая доступ к профессиональным базам данных, информационным справочным и поисковым системам) http://www.elibrary.ru – Электронно-библиотечная система (обеспечивающая доступ, в том числе к профессиональным базам данных) «IPRbooks» http://www.iprbookshop.ru – Научно-техническая библиотека ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина» http://elib.gubkin.ru/ – Научно-техническая библиотека ФГБОУ ВО «Уфимский государственный нефтяной технический университет» http://bibl.rusoil.net/ – Научно-техническая библиотека ФГБОУ ВО «Ухтинский государственный технический университет» http://lib.ugtu.net/books – Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru – Электронно-библиотечная система «PROОбразование» www.profspo.ru – <u>Национальная электронная библиотека (НЭБ)</u> https://rusneb.ru/

Дополнения и изменения внес:



Старший преподаватель кафедры БИМ

А.Н. Величко

Дополнения (изменения) в рабочую программу рассмотрены и одобрены на заседании кафедры бизнес-информатики и математики

Заведующий кафедрой БИМ



О.М. Барбаков

СОГЛАСОВАНО:

Заведующий выпускающей кафедрой



М.Л. Белоножко

«15» мая 2023 г.