

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ  
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/  
(Ф.И.О. декана (директора института))

07.02.2023 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

С.1.1.44 Управление информационной безопасностью

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность)	10.05.03 Информационная безопасность автоматизированных систем
Квалификация выпускника	Специалист (бакалавр/магистр/специалист)
Специализация	Безопасность автоматизированных систем критически важных объектов

Курс	5
Семестр	9

Распределение учебного времени

Трудоемкость по учебному плану	180 / 5	часов/зачетных единиц
Лекции	36	часов
Лабораторные работы	36	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	72	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	72	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	9	семестр
Зачет	-	семестр
БРК, ДЗ	-	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

доцент с ученой степенью кандидата наук	ИВС	СОГЛАСОВАНО	Е.С. Кубашева
(должность)	(кафедра)		(И.О. Фамилия)
Заведующая кафедры ИБ	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина  
Кафедра информационной безопасности

(наименование кафедры)			
31.01.2023	протокол №	10/1	
(дата)			
Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина	
		(И.О. Фамилия)	

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)  
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит  
выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 15.02.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /М.Л. Бойкова/

## Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.1 знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации	<b>знания:</b> основных понятий и характеристик основных отраслей права, применяемых в профессиональной деятельности организации <b>умения:</b> <b>навыки:</b>
	ОПК-5.2 умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	<b>знания:</b> <b>умения:</b> формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы <b>навыки:</b>
	ОПК-5.3 Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	<b>знания:</b> Знает как разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов <b>умения:</b> Умеет разрабатывать системы защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов <b>навыки:</b> Разработки систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов

## Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Организационное и правовое обеспечение информационной безопасности (ОПК-5)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-5)

## Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, классическая лекция, мини-проекты

#### Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

##### 9 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
<b>Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.</b>	<b>20</b>	ОПК-5
Лекция. Ключевые вопросы информационной безопасности	1	
Лекция. Информационная безопасность в системе национальной безопасности России.	1	
Лабораторная работа. Анализ бизнес-процессов предприятия	4	
Лабораторная работа. Анализ информационных потоков и ИТ-инфраструктуры предприятия	4	
Задания для самостоятельной работы, в том числе выполнение Работа с литературой. Работа с лекционным материалом	10	
<b>Стандартизация процессов управления информационной безопасностью</b>	<b>16</b>	ОПК-5
Лекция. Стандарты управления информационной безопасностью	2	
Роль стандартов ИБ. "Оранжевая книга" как основополагающий оценочный стандарт. Международный стандарт ISO/IEC 15408.		
Лекция. Стандарты BS 7799 и ISO/IEC 17799. Их основные положения.	2	
Лекция. Сертификация СУИБ на соответствие ISO 27001.	2	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией	10	
<b>Классификация угроз информационной безопасности.</b>	<b>22</b>	ОПК-5
Лекция. Угрозы информационной безопасности.	2	
Классификация угроз информационной безопасности.		
Лекция. Модель нарушителя информационной безопасности.	2	
Лабораторная работа. Анализ внутренних и внешних угроз информационной безопасности	4	
Лабораторная работа. Построение модели нарушителя	4	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией. Работа с лекционным материалом. Подготовка к практическим занятиям	10	
<b>Документальное обеспечение управления информационной безопасностью.</b>	<b>22</b>	ОПК-5
Лекция. Документальное обеспечение управления информационной безопасностью.	2	
Лекция. Корпоративная и частные политики информационной безопасности.	2	

Лабораторная работа. Разработка концепции информационной безопасности предприятия	4	ОПК-5
Лабораторная работа. Разработка политики информационной безопасности предприятия	4	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией. Работа с лекционным материалом. Подготовка к практическим занятиям	10	
<b>Меры обеспечения информационной безопасности.</b>	<b>20</b>	
Лекция. Процессы управления информационной безопасностью.	2	
Лекция. Система управления информационной безопасностью.	2	
Лекция. Организационные вопросы управления информационной безопасностью	2	
Лекция. Технические аспекты управления информационной безопасностью	2	
Лекция. Программные средства управления информационной безопасностью.	2	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией. Работа с лекционным материалом. Подготовка к практическим занятиям	10	ОПК-5
<b>Идентификация и анализ информационных рисков</b>	<b>18</b>	
Лекция. Идентификация и анализ информационных рисков	2	
Лекция. Методы управления информационными рисками.	2	
Лабораторная работа. Анализ информационных рисков предприятия	4	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией. Работа с лекционным материалом. Подготовка к практическим занятиям	10	ОПК-5
<b>Измерение информационной безопасности. Оценка процессов управления информационной безопасностью.</b>	<b>26</b>	
Лекция. Измерение информационной безопасности. Оценка процессов управления информационной безопасностью.	2	
Лекция. Оценка экономической эффективности деятельности по управлению	2	
Лекция. Аудит информационной безопасности.	2	
Лабораторная работа. Разработка технического задания на создание системы обеспечения информационной	4	
Лабораторная работа. Оценка экономической эффективности системы обеспечения информационной	4	
Задания для самостоятельной работы, в том числе выполнение Работа с нормативной документацией. Работа с лекционным материалом. Подготовка к практическим занятиям	12	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

## Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины **Управление ИБ** рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

**Занятия лекционного типа** дают систематизированные знания по дисциплине **Управление ИБ**, концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. Подготовка к **занятиям семинарского типа** включает ознакомление с планом **лабораторного** занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины **Управление ИБ**, оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине **Управление ИБ** является **экзамен**;

## Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
<b>УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ</b>		
1.	Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс] / В. Ф. Шаньгин. Москва: ДМК Пресс, 2014. - 702 с. ISBN 978-5-94074-768-0.	<a href="http://e.lanbook.com/books/element.php?pl1_id=50578">http://e.lanbook.com/books/element.php?pl1_id=50578</a>
2.	Чекулаева, Елена Николаевна. Управление информационной безопасностью [Текст] : учебное пособие : для студентов и магистрантов направлений подготовки 10.05.03 "Информационная безопасность автоматизированных систем", 10.04.01 "Информационная безопасность" / Е. Н. Чекулаева, Е. С. Кубашева; Министерство науки и высшего образования Российской Федерации, ФГБОУ ВО "Поволжский государственный технологический университет". Йошкар-Ола: ПГТУ, 2020. - 153 с. ISBN 978-5-8158-2165-1. Экземпляры: всего	15 / <a href="https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf">https://portal.volgatech.net/books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf</a>
3.	Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет- университет информ. технологий. М., 2003. - 277 с. ISBN 5-9556-0003-5. Экземпляры: всего 18.	18
4.	Конеев, Искандер Рустамович. Информационная безопасность предприятия [Текст] : [понятия и	9

	принципы. Методики и модели защиты. Классификация атак. Типовая модель нападения. Немного о хакерах и анонимайзерах. Методика упр. рисками. Критерии оценки. Криптогр. средства и механизмы. Истории криптогр. Классификация шифров] / И. Конеев, А. Беляев. Санкт-Петербург: БХВ-Петербург, 2003. - 733 с. ISBN 5-94157-280-8. Экземпляры: всего 9.	
5.	Галатенко, В. А. Основы информационной безопасности [Текст] : курс лекций / В. А. Галатенко ; под ред. В. Б. Бетелина ; Интернет-университет информ. технологий. 2-е изд., испр. М., 2004. - 261 с. ISBN 5-9556-0015-9. Экземпляры: всего 23.	23
6.	Корт, Семен Станиславович. Теоретические основы защиты информации [Текст] : [учеб. пособие для студентов вузов по группе специальностей в обл. информ. безопасности] / С. С. Корт. М.: Гелиос АРВ, 2004. - 233 с. ISBN 5-85438-010-2. Экземпляры: всего 28.	28
7.	Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] : учеб. пособие по специальностям в обл. информ. безопасности / С. Н. Семкин, Э. В. Беляков, С. В. Гребенев, В. И. Козачок. М.: Гелиос АРВ, 2005. - 185 с. ISBN 5-85438-042-0. Экземпляры: всего 30.	30
8.	Садердинов, Али Абдулович. Информационная безопасность предприятия [Текст] : учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов ; Междунар. акад. наук информации, информ. процессов и технологий (МАН ИПТ). 2-е изд. М.: Дашков и К, 2005. - 335 с. ISBN 5-94798-558-6. Экземпляры: всего 10.	10
9.	Основы информационной безопасности [Текст] : [учеб. пособие по специальностям в обл. информ. безопасности] / Е. Б. Белов [и др.]. М.: Горячая линия - Телеком, 2006. - 544 с. ISBN 5-93517-292-5. Экземпляры: всего 16.	16

## 6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	535 (III)	Мультимедийный комплект 4 (1), Ноутбук Acer (1), Персональный компьютер в сборе PowerCool(Core i3-8100/H310/16GbDDR4/HDD 0.5Tb/23"6 АОС/кл.мышь/пач-корд 3м) (20), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft

		Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
--	--	---

## Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

### 7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»



## 7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

Билет 1

1. Назвать основные компоненты системы обеспечения информационной безопасности. 2. В чем заключается концептуальная разница между концепцией и политикой информационной безопасности? 3. С какой целью разрабатывается концепция информационной безопасности? 4. Какими документами определяется содержание концепции информационной безопасности? 5. Что такое объекты защиты? Приведите их классификацию.

Билет 2

В чем различие между политиками, стандартами, процедурами, руководствами информационной безопасности? 2. Опишите этапы жизненного цикла политики информационной безопасности. 3. Какие виды частных политик информационной безопасности бывают? 4. Какими российскими и международными стандартами регулируются процессы создания политики информационной безопасности? 5. В каких случаях политики информационной безопасности аннулируются?

Билет 3

1. Опишите основные работы по созданию системы защиты информации согласно ГОСТ Р 51583-2014. 2. Приведите классификацию информационных систем по требованиям защиты информации. 3. Перечислите функции заказчика и оператора по обеспечению защиты информации в информационной системе. 4. Охарактеризуйте типы субъектов и объектов доступа. 5. Перечислите основные меры защиты информации согласно методическому документу Гостехкомиссии "Специальные требования и рекомендации по технической защите конфиденциальной информации".

Билет 4

1. Какие подходы можно использовать для экономической оценки обеспечения информационной безопасности предприятия? 2. Перечислите основные возможности методики совокупной стоимости владения компании Gartner Group. 3. Приведите основные статьи прямых расходов на обеспечение информационной безопасности предприятия. 4. Приведите основные статьи косвенных расходов на обеспечение информационной безопасности предприятия. 5. Как рассчитывается эффективность подразделения по защите информации?

## Перечень вопросов для проведения промежуточной аттестации

опросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к экзамену) 1. Понятие и задачи информационной безопасности. 2. Уровни обеспечения информационной безопасности. 3. Правовая защита информации. 4. Место информационной безопасности в системе национальной безопасности. 5. Политика обеспечения информационной безопасности Российской Федерации. 6. Современные проблемы информационной безопасности. 7. Модель информационной безопасности организации. 8. Стандартизация процессов управления информационной безопасностью. 9. Состав организационно-распорядительных документов по обеспечению информационной безопасности. 10. Концепция информационной безопасности. 11. Корпоративная политика информационной безопасности. 12.

Частные политики информационной безопасности. 13. Система управления информационной безопасностью. 14. Стратегии построения системы управления информационной безопасностью. 15. Процессный подход к управлению информационной безопасностью. 16. Ресурсы, результаты, владельцы процесса управления информационной безопасностью. 17. Программные средства управления информационной безопасностью. 18. Содержание технического задания на создание системы обеспечения информационной безопасности предприятия. 19. Организационные вопросы управления информационной безопасностью. 20. Состав и основные функции службы безопасности организации. 21. Технические аспекты управления информационной безопасностью. 22. Классификация угроз информационной безопасности. 23. Классификация уязвимостей. 24. Классификация информационных рисков. 25. Идентификация и анализ информационных рисков. 26. Методы оценивания информационных рисков. 27. Обеспечение безопасности персональных данных. 28. Аудит информационной безопасности. 29. Экономическая оценка обеспечения информационной безопасности.