

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

02.02.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.33 Организационное и правовое обеспечение ИБ

(код и наименование дисциплины по учебному плану)

Направление подготовки (специальность) 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника Специалист
(бакалавр/магистр/специалист)

Специализация Анализ безопасности информационных систем

Курс 4
Семестр 7

Распределение учебного времени

Трудоемкость по учебному плану	144 / 4	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	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	72	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	7	семестр

(год)

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

Программу составили:

доцент	ИБ	СОГЛАСОВАНО	А.П. Александров
(должность)	(кафедра)		(И.О. Фамилия)

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

(наименование кафедры)		
31.01.2022	протокол №	23
(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 07.02.2022 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

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-5.2 умеет формулировать основные требования информационной безопасности при эксплуатации автоматизированной системы	знания: умения: Формировать перечень мероприятий по предотвращению угроз безопасности информации автоматизированной системы навыки:
	ОПК-5.3 Разработка систем защиты информации автоматизированных систем с учетом действующих нормативно-правовых документов	знания: Основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации умения: Определять комплекс мер для обеспечения безопасности информации в автоматизированных системах навыки: Разработка проектной документации на системы защиты автоматизированных систем
	ОПК-5.1 знает основные понятия и характеристику основных отраслей права, применяемых в профессиональной деятельности организации	знания: Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации умения: навыки:
2. ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированной	ОПК-6.1 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации	знания: Способы реализации угроз безопасности в автоматизированных системах умения: навыки:
	ОПК-6.2 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации	знания: умения: Классифицировать и оценивать угрозы безопасности информации для автоматизированной системы навыки:

нных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.3 Определение комплекса мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации автоматизированных систем	знания: Организационные меры по защите информации умения: Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации в автоматизированных системах навыки: Разработка 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: Основы информационной безопасности (ОПК-6)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Управление информационной безопасностью (ОПК-5); государственной итоговой аттестации в форме: Подготовка к процедуре защиты и защита выпускной квалификационной работы (ОПК-6)

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: классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Аудиторная и самостоятельная работа	144	ОПК-5, ОПК-6
Лекция. Темы лекций:	36	

<ol style="list-style-type: none"> 1. Правовая система информационной безопасности Российской Федерации. 2. Компетенция органов государственной власти по обеспечению информационной безопасности. 3. Федеральные и ведомственные нормативные акты в области информационной безопасности. 4. Международные и отечественные стандарты в сфере информационной безопасности. 5. Лицензирование, сертификация и аттестация в сфере информационной безопасности. 6. Защита интеллектуальной собственности. 7. Правовое регулирование охранной деятельности, проведения оперативно-розыскных мероприятий 8. Юридическая ответственность за преступления и правонарушения в сфере информационной безопасности. 9. Обеспечение безопасности критической информационной инфраструктуры. 		
<p>Лабораторная работа. Лабораторные (практические) занятия:</p> <ol style="list-style-type: none"> 1. Информация как объект правового регулирования. 2. Конституционные гарантии прав на информацию и механизм их реализации. 3. Концептуальные основы информационной безопасности в Российской Федерации. 4. Законодательство Российской Федерации в области информационной безопасности. 5. Правовой режим защиты государственной тайны 6. Правовой режим защиты конфиденциальной информации 7. Персональные данные, правовой режим защиты персональных данных. 8. Сведения служебного характера, правовой режим их защиты. 9. Сведения, связанные с профессиональной деятельностью (профессиональная тайна). 10. Лицензирование и сертификация в информационной сфере 11. Защита интеллектуальной собственности. 12. Международное законодательство в области защиты информации 13. Юридическая ответственность (уголовная, административная, гражданско-правовая, дисциплинарная) за нарушения правового режима конфиденциальной информации. 14. Обеспечение безопасности критической информационной инфраструктуры. 	36	

Задания для самостоятельной работы, в том числе выполнение РГР

Темы РГР:

1. Правовые основы и процедура лицензирования деятельности в области информационной безопасности.
2. Международное законодательство в области защиты персональных данных.
3. Права и свободы гражданина и человека на информацию.
4. Ответственность за преступления и правонарушения в области информационной безопасности.
5. Система государственной и отраслевой стандартизации защиты информации Российской Федерации .
6. Организационно-правовая регламентация охранной деятельности в Российской Федерации.
7. Правовые основы и процедура сертификации в области защиты информации.
8. Ответственность за нарушение прав на интеллектуальную собственность.
9. Справочно-правовые системы Российской Федерации.
10. Зарубежный опыт нормативно-правового обеспечения защиты информации.
11. Государственная тайна, особенности защиты государственной тайны.
12. Конфиденциальная информация, ее состав и особенности организации защиты.
13. Роль Межведомственной Комиссии в защите государственной тайны.
14. Понятие интеллектуальной собственности.
- Законодательство Российской Федерации об интеллектуальной собственности.
15. Правовые основы патентования в Российской Федерации. Механизм патентования.
16. Роль органов ФСБ Российской Федерации в обеспечении информационной безопасности.
17. Роль Федеральной службы по техническому и экспортному контролю Российской Федерации в обеспечении информационной безопасности.
18. Органы лицензирования и их полномочия.
19. Органы сертификации и их полномочия.
20. Правовые основы охраны программ для ЭВМ, баз данных и топологии интегральных микросхем.
21. Особенности правовой охраны секретных изобретений.
22. Правовой режим защиты коммерческой тайны.
23. Правовой режим защиты персональных данных.
24. Правовые режимы защиты профессиональной тайны.
25. Требования и принципы защиты объектов критической информационной инфраструктуры Российской Федерации.
26. Правовое регулирование отношений, связанных с обеспечением доступа к информации о деятельности государственных органов.
27. Доктрина информационной безопасности Российской Федерации.

28. Объекты и субъекты правоотношений в области информационной безопасности.		
29. Организационная система обеспечения информационной безопасности Российской Федерации.		
30. Государственные информационные системы, основания для их создания и функционирования.	72	
Иная контактная работа: выполнение реферата, дифференцированный зачет (БРК)	0	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины 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, 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 практического (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, 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.

Изучение дисциплины включает выполнение **расчётно-графической работы**.

Подготовка расчётно-графических работ осуществляется в течение семестра в соответствии с перечнем рекомендуемых тем РГР. Успешное выполнение РГР достигается путем анализа теоретических и практических материалов по выбранной теме тщательной подготовке к защите РГР.

Подготовка к выполнению РГР

Подготовка заключается в:

- внимательном изучении выбранной темы, уяснении цели и задачи работы;
- изучении и анализе относящихся к данной теме организационно-правовых документов и материалов их практического применения.

Выполнение РГР

Используя лекционный материал, действующие в Российской Федерации нормативно-правовые документы, регламентирующие деятельность в сфере информационной безопасности, учебную и специальную литературу, информацию из современных периодических изданий подобрать материалы, необходимые для выполнения РГР. В

работе могут приводиться примеры применения организационно-правовых мер защиты информации по выбранной теме на российских предприятиях и в учреждениях, зарубежный опыт работы в данной области информационной безопасности, мнения о дальнейшем совершенствовании защиты информации в рассматриваемой области.

Целью выполнения РГР является формирование и развитие профессиональных компетенций, приобретение практических навыков реализации требований по организации защиты информации, изучение современного опыта построения систем информационной безопасности, подготовка к БКР по результатам изучения дисциплины.

Оформление РГР

Составление отчета о проведенных исследованиях является заключительным этапом выполнения РГР. Отчет выполняется в электронном (машинописном) виде, руководствуясь следующими положениями:

- титульный лист оформляется в соответствии с требованиями по оформлению практических заданий и курсовых работ с указанием дисциплины и темы РГР;
- РГР должна содержать оглавление, введение с постановкой задачи, аналитическую часть, практическое использование/применение рассматриваемой темы, заключение, перечень используемой литературы. Допускается введение в РГР других разделов и приложений по усмотрению студента. Объем РГР как правило должен составлять 15-30 листов формата А-4;
- к защите РГР готовится презентация, состоящая из 10-15 слайдов.

Защита РГР проводится индивидуально.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине является балльно-рейтинговый контроль.

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
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Галатенко, В. А. Стандарты информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 307 с. ISBN 5-9556-0053-1.	https://e.lanbook.com/book/100511
2.	Галатенко, В. А. Основы информационной безопасности [Электронный ресурс] / Галатенко В. А. 2-е изд. Москва: ИНТУИТ, 2016. - 266 с. ISBN 978-5-94774-821-5.	https://e.lanbook.com/book/100295
3.	Смирнов, Владимир Иванович. Защита информации [Текст] : лабораторный практикум : [по направлению 09.03.01] / В. И. Смирнов; М-во образования и науки Рос. Федерации, ФГБОУ ВО "Поволж. гос. технол. ун-т". Йошкар-Ола: ПГТУ, 2017. - 65 с. ISBN 978-5-8158-1866-8. Экземпляры: всего 25.	25 / https://portal.volgatech.net/books/Smirnov_zashita_informacii_2017.pdf
4.	Основы информационной безопасности [Текст] : учебное пособие : [по направлению подготовки 09.03.01]	10

	системы и технологии"] / [Ю. Ю. Громов и др.]. Старый Оскол: ТНТ, 2017. - 381 с. ISBN 978-5-94178-216-1. Экземпляры: всего 10.	
5.	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
6.	Петренко, В. И. Защита персональных данных в информационных системах. Практикум [Текст] : Учебное пособие для вузов / Петренко В. И., Мандрица И. В.; Мандрица И. В. 4-е изд., стер. Санкт-Петербург: Лань, 2022. - 108 с. ISBN 978-5-507-45301-6.	https://e.lanbook.com/book/264242
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru
2.	Информационно-правовой портал Гарант	http://www.garant.ru

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)	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, Microsoft Office Standard, Агент Dr.Web, 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.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

БИЛЕТ БКР № 1

По дисциплине: «Организационное и правовое обеспечение информационной безопасности»

1. Информация как объект правового регулирования.

2. Органы лицензирования и их полномочия.

Зав. кафедрой ИБ _____ И.Г. Сидоркина

« ____ » _____ 20__ г.

Перечень вопросов для проведения промежуточной аттестации

Перечень

вопросов к БРК

1. Информация как объект правового регулирования. Субъекты и объекты правоотношений в области информационной безопасности.
2. Конституционные гарантии прав на информацию и механизм их реализации.
3. Национальные интересы Российской Федерации в информационной сфере. Угрозы информационной безопасности Российской Федерации и их источники.
4. Система обеспечения информационной безопасности Российской Федерации и ее функции.
5. Законодательство Российской Федерации в области информационной безопасности.
6. Доктрина информационной безопасности Российской Федерации.
7. Понятие и виды защищаемой информации по законодательству РФ.
8. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
9. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, засекречивания и рассекречивания сведений, относимых к государственной тайне.
10. Органы защиты государственной тайны и их компетенция.
11. Понятие и порядок допуска и доступа к государственной тайне.
12. Конфиденциальная информация, ее состав и признаки. Правовые режимы конфиденциальной информации их особенности.
13. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
14. Правовой режим защиты коммерческой тайны.
15. Персональные данные. Правовая регламентация обработки персональных данных в информационных системах.

персональных данных.

16. Правовые основы отнесения сведений к профессиональной тайне. Правовые акты, регламентирующие защиту профессиональной тайны.

17. Понятие лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию.

18. Лицензирование деятельности в области защиты государственной тайны. Специальные экспертизы и государственная аттестация руководителей.

19. Органы лицензирования и их полномочия. Участники лицензионных отношений в сфере защиты информации.

20. Понятие сертификации по российскому законодательству. Объекты сертификационной деятельности (сертификации).

21. Органы сертификации и их полномочия.

22. Международное законодательство в области защиты персональных данных.

23. Стандартизация в области защиты информации.

24. Государственные информационные системы, порядок их создания и функционирования.

25. Требования по защите государственных информационных систем.

26. Органы государственной власти, уполномоченные в области обеспечения информационной безопасности.

27. Законодательство РФ об интеллектуальной собственности. Понятие интеллектуальной собственности. Объекты и субъекты авторского права.

28. Правовая охрана программ для ЭВМ, баз данных и топологии интегральных микросхем.

29. Исключительные и смежные авторские права. Защита авторских и смежных прав.

30. Основы патентных правоотношений. Условия патентоспособности.

31. Авторы изобретений и патентообладатели.

32. Механизм патентования.

33. Особенности правовой охраны секретных изобретений.

34. Защита прав патентообладателей и авторов.

35. Понятие критической информационной инфраструктуры Российской Федерации, объекты и субъекты КИИ.

36. Принципы обеспечения безопасности критической информационной инфраструктуры.

37. Правовая регламентация охранно-детективной деятельности и оперативно-розыскной деятельности.

38. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).

39. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).

40. Преступления в сфере компьютерной информации.