

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ЭФ

УТВЕРЖДАЮ /Н.М. Стрельникова/
(Ф.И.О. декана (директора института))

01.03.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.1.25 Информационная безопасность

(код и наименование дисциплины по учебному плану)

Направление подготовки
(специальность)

09.03.03 Прикладная информатика

Квалификация выпускника

Бакалавр

(бакалавр/магистр/специалист)

Направленность

Прикладная информатика в экономике

Курс 4
Семестр 7

Распределение учебного времени

Трудоемкость по учебному плану	108 / 3	часов/зачетных единиц
Лекции	14	часов
Лабораторные работы	28	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	42	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	66	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	7	семестр
БРК, ДЗ	-	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.03.03 Прикладная информатика

Программу составили:

доцент с ученой степенью кандидата наук	ИБ	СОГЛАСОВАНО	Е.Н. Чекулаева
(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	Т.А. Уразаева
		(И.О. Фамилия)

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

	СОГЛАСОВАНО	О.Е. Иванов
		(И.О. Фамилия)

Эксперт(ы): Жубрин Алексей Анатольевич, помощник генерального директора ОАО
«ММЗ» по информатизации – начальник управления информационных технологий
Рабочая программа проверена и зарегистрирована в УМЦ 06.03.2023 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-3 Способен решать стандартные задачи профессиональной деятельности на основе информационн ой и библиографиче ской культуры с применением информационн о-коммуникацион ных технологий и с учетом основных требований информационн ой безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности умения: навыки:
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: умения: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности навыки:
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	знания: умения: навыки: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

2. ОПК-4 Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1. Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	знания: Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы умения: навыки:
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	знания: умения: Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы навыки:
	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы	знания: умения: навыки: Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы

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: Информационные технологии (ОПК-3), Вычислительные системы, сети и телекоммуникации (ОПК-3), Вычислительные системы, сети и телекоммуникации (ОПК-4)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих дисциплинах: Проектирование информационных систем (ОПК-4); государственной итоговой аттестации в форме: Выполнение и защита выпускной квалификационной работы (ОПК-3), Выполнение и защита выпускной квалификационной работы (ОПК-4)

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, процедуры самообучения

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
Раздел 1 Основы ИБ	64	ОПК-3, ОПК-4
Лекция. Основы информационной безопасности	2	
Лабораторная работа. Найти Гости и ответить на вопросы	2	
Лекция. Перечень защищаемой информации. Защита информации	2	
Лабораторная работа. Провести классификацию защищаемой информации	4	
Лекция. Угрозы и модель угроз ИБ	2	
Лабораторная работа. Ответить на вопросы из Гостов	2	
Лекция. Нарушители ИБ. Модель нарушителя	1	
Лабораторная работа. Разработка требований к ИС	2	
Лекция. Методы и средства защиты информации	1	
Лабораторная работа. Оценка состояния безопасности ИС	4	
Лекция. Риски в управлении ИБ	2	
Лабораторная работа. Разработка и анализ объекта защищаемой информации	4	
Задания для самостоятельной работы, в том числе выполнение КР "Финансовая безопасность на примере организации"	36	
Методы и средства защиты ИБ	44	ОПК-3, ОПК-4
Лекция. Модель КСИБ предприятия и методы ее оценки	2	
Лабораторная работа. Проведение анализа целостности информации и ее оценка уязвимости	6	
Лекция. Мониторинг, контроль и аудит ИБ	2	
Лабораторная работа. Повышение уровня ИБ в ИС	4	
Задания для самостоятельной работы, в том числе выполнение РГР Проведение анализа КСЗИ	30	
Иная контактная работа:	0	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины семестра 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 семестра, 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 семестра.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины семестра, 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 семестра, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины семестра включает выполнение контрольной работы, расчетно-графической работы.

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине семестра является зачет.

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.	Малюк, Анатолий Александрович. Введение в защиту информации в автоматизированных системах [Текст] : учеб. пособие для студентов по специальностям, не входящим в группу специальностей в обл. информ. безопасности / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. М.: Горячая линия - Телеком, 2001. - 144 с. ISBN 5-93517-062-0. Экземпляры: всего 8.	8
2.	Малюк, Анатолий Александрович. Информационная безопасность [Текст] : концептуальные и методологические основы защиты информации : [учеб. пособие для студентов вузов по специальности 075400 "Комплексная защита объектов информ."] / А. А. Малюк. М.: Горячая линия - Телеком, 2004. - 280 с. ISBN 5-93517-197-X. Экземпляры: всего 10.	10
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.	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
5.	Чекулаева, Елена Николаевна. Управление информационной безопасностью [Текст] : учебное	15 / https://portal.volgatech.net/b

	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	books/Chekulayeva_Upravleniye_informatsionnoy_bezopasnostyu_2020.pdf
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
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
3.	Профессиональные справочные системы Техэксперт	http://www.cntd.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.	107 (III)	Анализатор линейных коммуникаций УЛАН-2 (1), Генератор шума Соната -P2 (1), Доска маркерная 100*200см (1), ИБП UPS 1100VA (7), Коммутатор D-Link DES-3200-28 (8), Коммутатор D-Link DES-3810-28 (2), Комплекс защиты информации Secret Disk 4.0 (1), Комплекс защиты информации Secret Net 5.0 (2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/М "Катран" (1), Ноутбук Acer Aspire 3 A315-42 (1), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, Монитор BenQ G2450HM,клав,мышь (3), ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, Монитор 24" BenQ G2450HM,клав,мышь (2), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Система виброакустической защиты "Соната-AB" (1), Система	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

	виброакустической.защиты "Соната-РС2" (1), Средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е" (2), Экран настенный 200*200см Braun Roll Vision (1), Комплект учебной мебели (1)	
--	--	--

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	Зачтено

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.

1. Виды политик по управлению информационной безопасности
2. Работа оператора для безопасности информации
3. Термин "документированная процедура"
4. Основные способы защиты информации

5. Классы риска информационной безопасности
6. Система управления паролями
7. Политика информационной безопасности
8. Средства защиты информации
9. Анализ последовательности информации
10. Примеры несанкционированного доступа
11. Процедура организации для защиты данных
12. Система менеджмента информационной безопасности
13. Современные способы защиты информации
14. "Стратегии" обеспечения достоверности информации
15. Назначение политики менеджмента инцидентов ИБ

Перечень вопросов для проведения промежуточной аттестации

Пороговый уровень

1. Основные составляющие информационной безопасности.
2. Основные принципы национальной безопасности.
3. Виды информации
4. Угрозы информационной безопасности
5. Виды политик по управлению информационной безопасности
6. Работа оператора для безопасности информации
7. Термин "документированная процедура"
8. Основные способы защиты информации
9. Классы риска информационной безопасности
10. Этапы менеджмента инцидентов ИБ

Продвинутый уровень

12. Показатели, влияющие на информационную безопасность.
13. Основные акты в области информационной безопасности.
14. Правовой режим доступа информации
15. Характер происхождения угроз
16. Функции управляющего совета по вопросам информационной безопасности
17. Система управления паролями

18. Политика информационной безопасности

19. Средства защиты информации

20. Анализ последовательности информации

21. Примеры несанкционированного доступа

Высокий уровень

22. Информационная безопасность и информационные технологии

23. Органы, обеспечивающие информационную безопасность

24. Конфиденциальная информация

25. Классификация и модели угроз безопасности

26. Факторы успешного внедрения информационной безопасности

27. Процедура организации для защиты данных

28. Система менеджмента информационной безопасности

29. Современные способы защиты информации

30. "Стратегии" обеспечения достоверности информации

31. Назначение политики менеджмента инцидентов ИБ