

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

25.06.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.31 Методы и средства криптографической защиты информации

(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	18	часов
Лабораторные работы	36	часов
Практические занятия	-	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	54	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	54	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	7	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:

профессор с ученой степенью доктора наук	ИБ	СОГЛАСОВАНО	А.Н. Леухин
(должность)	(кафедра)		(И.О. Фамилия)

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

	(наименование кафедры)	
30.04.2021	протокол №	17
(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): Е.В. Зверева, Начальник отдела ПД ИТР ОАО ММЗ

Рабочая программа проверена и зарегистрирована в УМЦ 01.07.2021 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-10 Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ОПК-10.1 Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах	знания: Знает основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах умения: Умеет использовать основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах навыки: владеет навыками применения основных криптографических методов, алгоритмов, протоколов, используемые для защиты информации в автоматизированных системах
	ОПК-10.2 Обоснование необходимости использования криптографических средств защиты информации	знания: Знает криптографические средства защиты информации умения: Умеет обосновать необходимость использования криптографических средств защиты информации навыки: владеет навыком использовать криптографические средства защиты информации
	ОПК-10.3 владеет навыками применения инструментальных средств анализа безопасности программного обеспечения при построении систем защиты информации автоматизированных систем	знания: умения: навыки: владеет навыками применения инструментальных средств анализа безопасности программного обеспечения при построении систем защиты информации автоматизированных систем

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: Безопасность вычислительных сетей (ОПК-10)

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-10)

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
Основные задачи и принципы КЗИ. Общие понятия криптографии	11	ОПК-10
Лекция. КЗИ. основные задачи и принципы КЗИ	2	
Лабораторная работа. Шифрование методом перестановки. расшифрование методом перестановки	4	
Задания для самостоятельной работы, в том числе выполнение самостоятельная работа	5	
Криптография: от древних греков до 21 века	15	ОПК-10
Лекция. Обзор классической и современной криптографии: от древних греков до 21 века	2	
Лабораторная работа. Шифрование, расшифрование методами многоалфавитной замены	4	
Лабораторная работа. Исследование энтропии текстов до и после шифрования в зависимости от длины ключа(периода гаммы)	4	
Задания для самостоятельной работы, в том числе выполнение самостоятельная работа	5	
Современная криптография	20	ОПК-10
Лекция. Симметричные и ассиметричные алгоритмы и схемы шифрования. Основные варианты использования	2	
Лабораторная работа. Криптоанализ классических шифров (вертикальной перестановки, Вижинера или гаммирования с линейным конгруэнтным генератором)	4	
Лабораторная работа. Исследование практической криптостойкости шифра классических шифров в зависимости от длины ключа (период гаммы) и длины шифротекста	4	
Задания для самостоятельной работы, в том числе выполнение самостоятельная работа	10	
Криптоанализ. Основные модели и методы	18	ОПК-10
Лекция. Теоретическая и практическая криптография. Методы шифров	2	
Лекция. Режим шифрования. Модели шифров. Формальные модели шифров. Алгебраическая модель шифра. Модель шифра простой замены	2	

Лабораторная работа. Современные блочные шифры на базе сети Файстеля. Шифрование, расшифрование методом DES.	4	ОПК-10
Задания для самостоятельной работы, в том числе выполнение самостоятельная работа	10	
Криптоанализ современных шифров	32	
Лекция. Симметричные системы шифрования и расшифрования	2	
Лекция. Принципы блочного шифрования. Шифр Файстеля	2	
Лабораторная работа. Современные потоковые шифры. Генерация гаммы с помощью РСЛОС, с помощью DES	4	
Лекция. Реализация КЗИ в сетях общего пользования	2	
Лекция. Протоколы современных криптографических систем. Основные классы протоколов	2	
Лабораторная работа. Электронная цифровая подпись	4	
Лабораторная работа. Криптография в мессенджерах	4	
Задания для самостоятельной работы, в том числе выполнение самостоятельная работа	12	
Иная контактная работа:	0	
Подготовка к экзамену	30	
Проведение экзамена	6	

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 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 лабораторных работ. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе.

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.	Смарт, Н. Криптография [Текст] : переводное издание / Н. Смарт ; пер. с англ. С. А. Кулешова под ред. С. К. Ландо. М.: Техносфера, 2005. - 525 с. ISBN 5-94936-043-10077099877. Экземпляры: всего 16.	16
2.	Гашков, Сергей Борисович. Криптографические методы защиты информации [Текст] : [учеб. пособие для студентов вузов по направлению "Прикладная математика и информатика", специальности "Информ. безопасность"] / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. М.: Академия, 2010. - 297, [1] с. ISBN 978-5-7695-4962-5. Экземпляры: всего 20.	20
3.	Черемушкин, Александр Васильевич. Криптографические протоколы [Текст] : основные свойства и уязвимости : [учеб. пособие для вузов по специальности "Компьютер. безопасность"] / А. В. Черемушкин. М.: Академия, 2009. - 271, [1] с. ISBN 978-5-7695-5748-4. Экземпляры: всего 20.	20
4.	Баричев, Сергей Геннадьевич. Основы современной криптографии [Текст] : учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. 3-е изд., стер. Москва: Горячая линия - Телеком, 2020. - 175 с. ISBN 978-5-9912-0182-7. Экземпляры: всего 24.	24
5.	Басалова, Г. В. Основы криптографии [Электронный ресурс] / Басалова Г. В. 2-е изд. Москва: ИНТУИТ, 2016. - 282 с.	https://e.lanbook.com/book/100302
6.	Лидовский, В. В. Основы теории информации и криптографии [Электронный ресурс] / Лидовский В. В. 2-е изд. Москва: ИНТУИТ, 2016. - 141 с.	https://e.lanbook.com/book/100349
7.	Панкратова, И. А. Булевы функции в криптографии [Электронный ресурс] : учебное пособие / Панкратова И. А. Санкт-Петербург: Лань, 2022. - 92 с. ISBN 978-5-8114-3465-7.	https://e.lanbook.com/book/206174
8.	Никифоров, С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учебное пособие / Никифоров С. Н. 2-е изд., стер. Санкт-Петербург: Лань, 2022. - 160 с. ISBN 978-5-8114-4042-9.	https://e.lanbook.com/book/206285
9.	Глухов, М. М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] / Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Санкт-Петербург: Лань, 2022. - 400 с. ISBN 978-5-8114-1116-0.	https://e.lanbook.com/book/210746
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		

1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
3.	Издательство Springer (SpringerOpen)	https://www.springeropen.com
4.	Издательство Elsevier	https://www.sciencedirect.com/
5.	Издательство SpringerNature	https://www.nature.com/
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.	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, 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
2.	107 (III)	Доска маркерная 100*200см (1), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала (1), Экран настенный 200*200см Braun Roll Vision (1), 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

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.

1. Шифрование, расшифрование методами перестановки
2. Шифрование, расшифрование методами многоалфавитной замены
3. Исследование энтропии текстов до и после шифрование в зависимости от длины ключа (периода гаммы)
4. Криптоанализ классических шифров (вертикальной перестановки, Вижинера или гаммирования с линейным конгруэнтным генератором)
5. Исследование практической криптостойкости шифра классических шифров в зависимости от длины ключа (периода гаммы) и длины шифротекста
6. Современные блочные шифры на базе сети Файстеля
7. Шифрование, расшифрование методом DES. Схемы шифрования
8. Статическое исследование криптостойкости шифра DES
9. Современные потоковые шифры
10. Генерация гаммы с помощью РСЛОС, с помощью DES
11. Статистическое исследование гаммы шифра
12. Электронная цифровая подпись

билет № 0

- 1- основные определения криптографии
- 2 Рассчитать длину кода
- 3 Определить тип кода

Перечень вопросов для проведения промежуточной аттестации

1. Дайте определение понятию "криптография"
2. Назовите принципы криптографической защиты информации
3. Перечислите Общие понятия криптографии: открытый и шифрованный тексты, ключи шифрования, криптосистема, атака, стойкость
4. Какие бывают способы криптографической защиты информации
5. Основные средства решения главных задач криптографии
6. Протоколы современных криптографических систем
7. Аутентификация и цифровая подпись
8. Управление секретными ключами
9. Симметричные и асимметричные алгоритмы и схемы шифрования. Основные варианты их использования
10. Теоретическая и практическая криптография
11. Модели шифров. Алгоритмы шифрования
12. Режимы шифрования
13. Формальные модели шифров. Алгебраическая модель шифра
14. Модель шифра простой замены. Модель перестановочного шифра. Шифрвеличины и шифробозначения
15. Математическая модель кодирования-раскодирования шифром простой замены
16. Классификация шифров. Примеры различных классов шифров
17. Протоколы современных криптографических систем. Основные классы протоколов
18. Доказательства с нулевым разглашением. Протокол с подбрасыванием монеты. Протоколы голосования. Протоколы совместного рукопожатия
19. Цифровые подписи и протоколы аутентификации

- 20. Управление секретными ключами. Схема генерации ключей
- 21. Хранение ключей. Иерархия ключей
- 22. Схема аутентификации мастер-ключа. Симметричные и асимметричные схемы распределения ключей с и без ЦРК
- 23. Постановка задачи криптографической защиты информации в сетях
- 24. Основные виды шифрования в сетях
- 25. Канальное и сквозное шифрование. внешняя и внутренняя схемы