

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

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

22.04.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

С.1.1.46 Анализ безопасности протоколов

(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 5
Семестр 10

Распределение учебного времени

Трудоемкость по учебному плану	180 / 5	часов/зачетных единиц
Лекции	32	часов
Лабораторные работы	-	часов
Практические занятия	32	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	64	часов
Контактная работа по экзамену	6	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	80	часов
Самостоятельная работа по подготовке к экзамену	30	часов
Экзамен	10	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	ИБ	СОГЛАСОВАНО	А.А. Кречетов
(должность)	(кафедра)		(И.О. Фамилия)

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

		(наименование кафедры)	
19.04.2021	протокол №	4	
(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 18.06.2021 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-17 Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных систем	ОПК-17.1 знает программно-аппаратные средства обеспечения защиты информации автоматизированных систем	знания: - методы анализа и тестирования протоколов; умения: навыки:
	ОПК-17.2 умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы	знания: умения: - создавать формальное описание протоколов с целью их дальнейшего анализа; навыки:
	ОПК-17.3 владеть навыками использования программно-аппаратных средств обеспечения безопасности информации в автоматизированных системах	знания: умения: навыки: - методами и средствами поиска уязвимостей, анализа и верификации протоколов; - типовыми средствами анализа сетевых протоколов;

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

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-17)

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 занятия

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

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

10 семестр

Виды и тематика занятий	Количество часов	Формируемые компетенции
Анализ безопасности протоколов	144	ОПК-17
Лекция. Стандарты безопасности	2	

Лекция. Свойства безопасности	2
Лекция. Модели свойств безопасности	2
Лекция. Криптографические протоколы	2
Лекция. Методы формальной спецификации	6
Лекция. Методы формальной верификации	4
Лекция. Тестирование свойств безопасности	6
Лекция. Мобильность	8
Практическое занятие. Ознакомление с языком описания криптографических протоколов HLSP и инструментом анализа протоколов AVISPA	12
Практическое занятие. Реализация протокола обеспечения конфиденциальности и целостности передачи сообщения между двумя участниками на языке HLPSL и проверка его корректности	10
Практическое занятие. Реализация протокола явного ключевого аутентифицированного обмена с использованием языка спецификации протоколов высокого уровня HLPSL и инструмента анализа протоколов AVISPA	10
Задания для самостоятельной работы, в том числе выполнение Проработка лекций	
Подготовка к практическим заданиям	80
Иная контактная работа:	0
Подготовка к экзамену	30
Проведение экзамена	6

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины (**модуля**) 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 (**модулю**), 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. (**при наличии**) Содержание **самостоятельной работы** определяется рабочей программой дисциплины (**модуля**), 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 (**модуля**), к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Изучение дисциплины (**модуля**) включает выполнение **практические работы**. Периодичность проведения, формы текущего контроля успеваемости, система оценивания

хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине (модулю) 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
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	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
2.	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
3.	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
4.	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
5.	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

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	Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ПО для решения основных пользовательских задач

	(2), Компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь (15), Нелинейный локатор SEL SP-61/M "Катран" (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 виброакустической.защиты "Соната-PC2" (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.	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	отлично

	<p>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</p>	
--	---	--

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. Модели контроля доступа.
2. Noninterference – невливание для детерминированных систем
3. Модель целостности Biba
4. Модель целостности Clark-Wilson
5. Протокол Нидхама-Шредера.
6. Модель Dolev-Yao.
7. Ina Jo.
8. LOTOS.
9. Языки спецификации специального назначения.
10. Протоколы как процессы.
11. Spi-исчисление.
12. Security Process Algebra.
13. Security Process Language.
14. Логика BAN.
15. Логика GNY.
16. Сети Петри.

Перечень вопросов для проведения промежуточной аттестации

1. Модели контроля доступа.
2. Noninterference – невливание для детерминированных систем
3. Модель целостности Biba
4. Модель целостности Clark-Wilson
5. Протокол Нидхама-Шредера.
6. Модель Dolev-Yao.
7. Ina Jo.
8. LOTOS.
9. Языки спецификации специального назначения.
10. Протоколы как процессы.
11. Spi-исчисление.
12. Security Process Algebra.
13. Security Process Language.
14. Логика BAN.
15. Логика GNY.
16. Сети Петри.

Раздел 9. ПЕРЕУТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Программа переутверждена на заседании учебно-методической комиссии _____ (назв. факультета (института)) протокол № _____ от “ _____ ” _____ 20 _____ г. _____ (подпись, Ф.И.О. председателя)	Программа переутверждена на заседании кафедры _____ (название кафедры) протокол № _____ от “ _____ ” _____ 20 _____ г. _____ (подпись, Ф.И.О. зав. кафедрой)
---	--