МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
декан факультета прикладной математики, информатики и механики

_____А.И. Шашкин
подпись, расшифровка подписи
23.05.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.43 Криптографические протоколы

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист по защите информации

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Воронков Борис Николаевич, к. т. н., доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики 23.05.2020 г., протокол № 9

_____
отметки о продлении вносятся вручную)

8. Учебный год: 2023/2024 **Семестр(ы):** 7

9. **Цели и задачи учебной дисциплины:** Цель дисциплины – теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом и синтезом криптографических протоколов. Задачи освоения дисциплины: изучение основных свойств, характеризующих защищённость криптографических протоколов, и основных механизмов, применяемых для обеспечения выполнения того или иного свойства безопасности протокола; приобретение навыков поиска уязвимостей протоколов.

10. Место учебной дисциплины в структуре ООП: Дисциплина «Криптографические протоколы» входит в базовую часть учебного плана и изучается в 7 семестре.

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы
1.	Б1.Б.44 Криптографические методы защиты информации
2.	Б1.Б.51.04 Криптографические стандарты

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-3.	способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знание протоколов: распределения ключей, идентификации, разделения секрета. Умение проводить анализ безопасности криптографических протоколов. Владение навыками программной реализации криптографических протоколов.
ПК-4.	способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знание методов разработки криптографических протоколов. Умение разрабатывать математические модели безопасности криптографических протоколов. Владение навыками моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* – 3/108.

Форма промежуточной аттестации*(зачет/экзамен)* зачёт с оценкой.

13. Виды учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	68		68			
в том числе: лекции	34		34			
Практические	0		0			
Лабораторные	34		34			
Самостоятельная работа	40		40			
Контроль						
Итого:	108		108			
Форма промежуточной аттестации			ЗаО			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Протоколы распределения ключей	Протоколы и их классификация. Обмен ключами средствами симметричной криптографии. Протоколы открытого распределения ключей. Протоколы передачи секретного ключа по открытому каналу.
2	Аутентификация	Аутентификация при входе в систему. Вручение битов на хранение. Бросание монеты по телефону. Доказательство с нулевым разглашением. Схемы аутентификации.
3	Дополнительные промежуточные протоколы	Разделение секрета. Скрытый канал связи. Мысленный покер. Мысленный покер с тремя игроками.
2. Практические занятия не предусмотрены		
3. Лабораторные работы		
3.1	Лабораторная работа №1 Тема: разработка модулярного калькулятора.	*Теоретические сведения* 1. Основные понятия и свойства модулярной арифметики. 2. Операции сравнения по модулю. 3. Обратные по модулю величины. 4. Возведение в степень по модулю. *Практическая часть* Реализация модулярного калькулятора на одном из языков прогаммирования.
3.2	Лабораторная работа №2 Тема: Протоколы с нулевым разглашением.	*Теоретические сведения* 1. Определение и свойства протоколов с нулевым разглашением. 2. Протокол Гиллу – Кискатра. 3. Протокол Фиата – Шамира. 4. Протокол Шнорра. *Практическая часть* 1. Реализация и исследование протоколов. 2. Подготовка и защита отчёта по лабораторной работе.
3.3	Лабораторная работа №3 Тема: Протоколы удалённой аутентификации.	*Теоретические сведения* 1. Понятие аутентификации. 2. Механизмы аутентификации. 3. Механизмы предоставления прав. 4. Удалённая аутентификация. 5. Протоколы PAP, CHAP, S/KEY. *Практическая часть* 1. Реализация протоколов PAP, CHAP, S/KEY в виде приложения 2. Подготовка и защита отчёта по лабораторной работе.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Всего
1	Распределение ключей.	12		12	16	40
2	Аутентификация.	12		12	14	38
3	Дополнительные промежуточные протоколы.	10		10	10	30
	Итого:	34		34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой библиографии, итоговое повторение теоретического материала. Подготовка отчётов по лабораторным работам и подготовка к зачёту с оценкой.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	*Смарт Н. Криптография / Н. Смарт; пер. с англ. С.А. Кулешова; под ред. С. К. Ландо. – М.: Техносфера, 2006. – 525 с.*
2	*Салий В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. – 2010. – (URL: http://www.sgu.ru/files/nodes/11017/V.N. Saliy. Kriptograficheskie metody i sredstva zashchity informacii.doc) (дата обращения: 12.05.2019)*

б) дополнительная литература:

№ п/п	Источник
3	*Воронков Б. Н. Криптографические методы защиты информации / Б. Н. Воронков, Ю. А. Крыжановская. – Воронеж: Издательский дом ВГУ, 2018. – 114 с.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
4	https://e.lanbook.com/ - ЭБС «Лань»
5	*www.lib.vsu.ru — Зональная научная библиотека ВГУ*

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Windows7. Мультимедийные лекционные демонстрации. Презентации на базе конспекта лекций.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-3.	Знать протоколы: распределения ключей,	Раздел 1. Распределение ключей Раздел 2. Протоколы	Устный опрос.

Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	идентификации, разделения секрета.	идентификации. Раздел 3. Протоколы разделения секрета.	
	Уметь проводить анализ безопасности криптографических протоколов.	Разделы 1 – 3.	Устный опрос. Лабораторные работы.
	Владеть навыками программной реализации криптографических протоколов.	Разделы 1 – 3.	Устный опрос, защита отчётов по лабораторным работам.
ПК-4. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать методы разработки криптографических протоколов.	Раздел 1. Распределение ключей Раздел 2. Протоколы идентификации. Раздел 3. Протоколы разделения секрета.	Устный опрос. Лабораторные работы. защита отчётов по лабораторным работам.
	Уметь разрабатывать математические модели безопасности криптографических протоколов.		
	Владеть навыками моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.		
Промежуточная аттестация			Комплект КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на зачёте с оценкой используется – шкала и критерии оценивания в соответствии с таблицей.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ПК-3.. Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности	Знать протоколы: распределения ключей, идентификации, разделения секрета.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Уметь проводить анализ безопасности криптографических протоколов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеть навыками программной реализации криптографических протоколов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
ПК-4. Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать методы разработки криптографических протоколов.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Уметь разрабатывать математические модели безопасности криптографических протоколов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеть навыками моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примеры контрольных вопросов и заданий:

1. Протоколы и их классификация.
2. Обмен ключами средствами симметричной криптографии.
3. Протоколы открытого распределения ключей.
4. Протоколы передачи секретного ключа по открытому каналу.
5. Аутентификация при входе в систему.
6. Вручение битов на хранение.
7. Бросание монеты по телефону.
8. Доказательство с нулевым разглашением.
9. Схемы аутентификации.
10. Методы разделения секрета.
11. Скрытый канал связи.
12. Мысленный покер.
13. Мысленный покер с тремя игроками.

19.3.2. Примеры заданий к лабораторной работе

1. Ознакомиться с двумя протоколами открытого распределения ключей.
2. Изучить и привести описание одного из наиболее эффективных протоколов.
3. Реализовать с помощью ППП Maple или на каком либо языке программирования алгоритм Диффи-Хеллмана.
4. Разработать и реализовать алгоритм бросания монеты по телефону.
5. Ответить на контрольные вопросы.
6. Составить отчёт о проделанной работе.

19.3.3. Пример контрольно-измерительного материала

УТВЕРЖДАЮ

заведующий кафедрой
ERP-систем и бизнес-процессов
_____ Й. Беккер
подпись, расшифровка подписи
_03.06.2019

Направление подготовки / специальность ___10.05.01_Компьютерная безопасность
шифр, наименование
Дисциплина__Криптографические протоколы_____

Вид контроля _____зачёт с оценкой_____
промежуточный контроль - экзамен, зачет; текущий контроль с указанием формы

Контрольно-измерительный материал №_1_

1. Протоколы распределения ключей и их классификация.

2. Разделение секрета. Скрытый канал связи.

Преподаватель _____ .____
подпись расшифровка подписи

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторные работы; тестирования. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по вопросам компьютерной безопасности.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.