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
24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.О.46 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:

Степанец Юлия Александровна , к.т.н., доцент кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

научно-методическим советом факультета ПММ от 15.06.2021 протокол № 10

_____

отметки о продлении вносятся вручную)

8. Учебный год: 2021/2022 **Семестр(ы):** 8

9. **Цели и задачи учебной дисциплины**

Целью является теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом и синтезом криптографических протоколов.

Задачи освоения дисциплины: изучение основных свойств, характеризующих защищенность 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 ОПОП: дисциплина относится к обязательной части блока Б1 дисциплин учебного плана.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.7	Знает типовые криптопротоколы, используемые в сетях связи.	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
		ОПК-10.8	Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем.	
		ОПК-10.9	Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	
		ОПК-10.10	Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.	
		ОПК-10.11	Владеет подходами к разработке и анализу безопасности криптографических протоколов.	
		ОПК-10.20	Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	

12. Объем дисциплины в зачетных единицах/час – 4/144.
Форма промежуточной аттестации - экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			8			
Аудиторные занятия	56		56			
в том числе: лекции	28		28			
Практические	0		0			
Лабораторные	28		28			
Самостоятельная работа	52		52			
Контроль	36		36			
Итого:	144		144			
Форма промежуточной аттестации	Экзамен		Экзамен			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Протоколы распределения ключей	Протоколы и их классификация. Обмен ключами средствами симметричной криптографии. Протоколы открытого распределения ключей. Протоколы передачи секретного ключа по открытому каналу.	Криптографические протоколы (10.05.01)
1.2	Аутентификация	Аутентификация при входе в систему. Вручение битов на хранение. Бросание монеты по телефону. Доказательство с нулевым разглашением. Схемы аутентификации.	
1.3	Дополнительные промежуточные протоколы	Разделение секрета. Скрытый канал связи. Мысленный покер. Мысленный покер с тремя игроками.	
2. Лабораторные работы			
2.1	Работа с протоколами	Разработка модулярного калькулятора. Протоколы с нулевым разглашением. Протоколы удалённой аутентификации.	Криптографические протоколы (10.05.01)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Распределение ключей.	10		0	16	8	34
1.2	Аутентификация.	10		0	14	8	32
1.3	Дополнительные промежуточные протоколы.	8		0	10	8	26
2.1	Работа с протоколами	0		28	12	12	52
	Итого:	28		28	52	36	144

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, [б. г.]. — Часть 1 — 2017. — 64 с. — ISBN 978-5-7641-1053-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111765 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.
2	Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2018 — Часть 2 — 2018. — 63 с. — ISBN 978-5-7641-1215-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/138103 (дата обращения: 10.02.2020). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Пугин, В. В. Криптографические протоколы : учебное пособие / В. В. Пугин. — Самара : ПГУТИ, 2019. — 68 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223319 (дата обращения: 20.01.2020). — Режим доступа: для авториз. пользователей.
4	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)

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

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

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, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Криптографические протоколы (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном. Аудитория для практических занятий должна быть оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном.

Программное обеспечение:
- ОС Windows 8 (10),
- интернет-браузер (Goolge Chrome, Mozilla Firefox).
- ПО Adobe Reader;
- пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, МойОфис, LibreOffice);
- ПО Maple или аналогичная среда визуального программирования.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Распределение ключей.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
2	Аутентификация.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
3	Дополнительные промежуточные протоколы.	ОПК-10	ОПК-10.7-10, 20	Контрольная работа
4	Работа с протоколами	ОПК-10	ОПК-10.9-11, 20	Лабораторные работы
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- контрольные работы,
- лабораторные работы.

Перечень контрольных работ

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.

Технология проведения

Студент выбирает вариант задания, ориентируясь на номер зачетки (последняя цифра). Студент выполняет предложенное преподавателем задание, представляет его в письменном виде, при необходимости, комментирует выполненные действия, анализирует и интерпретирует результаты. В курсе предусмотрено две контрольные работы (две темы из списка).

Критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Все задания контрольной работы выполнены, арифметических и логических ошибок нет, показано владение терминологией.	Повышенный уровень	Отлично
Все задания контрольной работы выполнены, но имеют место быть незначительные ошибки (арифметические, логические, в терминологии).	Базовый уровень	Хорошо
Не все задания контрольной работы выполнены и имеют место быть несущественные ошибки (арифметические, логические, в терминологии).	Пороговый уровень	Удовлетвори-тельно
Задания контрольной работы не выполнены или имеют место быть существенные ошибки (арифметические, логические, в терминологии).	–	Неудовлетво-рительно

Перечень лабораторных работ

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 программирования.
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	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.

Пример формирования задания 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.

Технология проведения
Все лабораторные работы обязательны для выполнение. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания
- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания и они правильные, даны пояснения);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к экзамену.

Перечень вопросов к экзамену (КИМ №1)

1. Перечислите режимы работы обучающей программы DES Tutorial.
2. Какова длина ключа алгоритма DES?
3. Что означает выражение "конкатенация битовых строк ассоциативна"?
4. Что представляет собой операция по модулю два?
5. Что такое криптология, криптограмма, криптография, криптоанализ?
6. В чем состоит основная идея шифрования данных?
7. В чем различие и в чем сходство шифрования и кодирования?
8. В чем различие терминов "дешифрование" и "расшифрование"?
9. Для решения каких задач используется кодирование информации?
10. Приведите алгоритм перехода от двоичной системы счисления к десятичной и наоборот.
11. Приведите алгоритм перехода от шестнадцатеричной системы счисления к десятичной и наоборот.
12. Опишите схему симметричного шифрования информации.
13. Что является аргументом функции шифрования F?
14. Приведите упрощённую схему алгоритма шифрования DES?
15. Приведите упрощённую схему алгоритма расшифрования DES?
16. Приведите схему реализации функции шифрования F.
17. Опишите алгоритм реализации "функций преобразования S(i).
18. Что означает фраза "процесс расшифрования данных является инверсным по отношению к процессу шифрования"?
19. Какие преобразования используются при реализации функции шифрования F(R,K)?
20. Какие биты ключа не влияют на шифрование? Для каких целей могут использоваться эти биты?
21. Расшифруйте сокращение "DES".
22. Почему (и какие?) программа добавляет символы к строкам, размеры которых не кратны восьми?
23. Для какой цели была разработана программа "DES Tutorial"?
24. Что такое криптостойкость? Каковы количественные характеристики криптостойкости?
25. Опишите алгоритм получения 48-битовых ключей K(i).
26. Докажите, что таблица 2 ("конечная перестановка") является обратной по отношению к таблице 1 ("начальная перестановка").
27. Опишите упрощённую схему асимметричного шифрования.
28. Какова максимальная длина открытого текста в программе DES? Подтвердите экспериментально.
29. В чем разница между закрытой, секретной и конфиденциальной информацией?
30. Что такое цена и ценность информации?
31. Что подразумевается под эффективностью защиты информации?
32. Что такое система безопасности?
33. В чем заключаются постулаты безопасности?
34. Чем достигается обеспечение безопасности?
35. Что такое способы защиты информации?
36. Что такое пространственное, временное, структурное и энергетическое скрытие информации?

37. В чем состоят цели защиты информации?
38. Охарактеризуйте физические системы защиты информации.
39. На какие классы разделяются инженерно-технические средства защиты информации?
40. В чем проявляются угрозы информации?
41. Что такое инженерно-техническая защита информации?
42. Каким образом классифицируется инженерно-техническая защита информации?
43. Что такое информационная безопасность?
44. Что такое защита информации?
45. Перечислите возможные виды утечек информации.
46. Охарактеризуйте методы симметричного шифрования данных.
47. Что такое отношение сравнимости?
48. Что называется полным набором вычетов по модулю n (n – целое число)?
49. Сформулируйте основные законы модулярной арифметики.
50. Что представляет собой функция Эйлера?
51. В чем состоит теорема Эйлера?
52. Сформулируйте малую теорему Ферма.
53. Как найти функцию Эйлера $\varphi(\prod_{i=1}^{n} p_i^{r_i})$, где p_i – простые числа, n и r_i - натуральные числа?
54. Дайте определение величины, обратной целому числу a по модулю n.
55. Охарактеризуйте основные способы нахождения обратных по модулю величин.
56. Что такое дискретный логарифм? В чем заключается проблема дискретного логарифмирования?
57. Дайте определение криптосистемы (шифра).
58. Что такое криптосистема Эль Гамаля?

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле:

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.