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

УТВЕРЖДАЮ
и.о. заведующего кафедрой
ERP-систем и бизнес-процессов
С.Л. Кенин
25.04.2022

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.45 Методы и средства криптографической защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Анализ безопасности компьютерных систем

Математические методы защиты информации

Математические методы защиты информации (УВЦ)

3. Квалификация (степень) выпускника: Специалист

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 15.04.2022 протокол № 8

_____

отметки о продлении вносятся вручную)

8. Учебный год: 2025/2026 **Семестр(ы):** 7

9. **Цели и задачи учебной дисциплины**

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике.

Задачи дисциплины - дать основы: системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.

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 выпускников):

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-10.1	Знает основные задачи, решаемые криптографическими методами.	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости
		ОПК-10.2	Знает математические модели шифров, подходы к оценке их стойкости.	
		ОПК-10.3	Знает зарубежные и российские криптографические стандарты.	
		ОПК-10.4	Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.	
		ОПК-10.5	Умеет применять математические методы при исследовании криптографических алгоритмов.	
		ОПК-10.6	Владеет навыками использования типовых криптографических алгоритмов.	

				информации в компьютерных системах.

12. Объем дисциплины в зачетных единицах/час— 3/108.

Форма промежуточной аттестации - зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	64		64			
в том числе: лекции	34		34			
Практические						
Лабораторные	34		34			
Самостоятельная работа	40		40			
Итого:	108		108			
Форма промежуточной аттестации	Зачет с оценкой		Зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные понятия. Терминология.	Информация, сообщения, сигналы, криптосистемы.	Криптографические методы защиты информации (10.05.01)
1.2	Математические основы криптографии	Теоремы о простых числах. Алгоритм Евклида. Функция Эйлера. Свойства модулярной арифметики. Теорема Эйлера. Вычисление обратных величин. Расширенный алгоритм Евклида	
1.3	Общие вопросы информационной безопасности	Основы классической криптографии. Классификация криптографических методов. Угрозы информации. Атаки на криптосистемы.	
1.4	Особенные системы криптографии.	Классы стойкости. Идеальные криптосистемы.	
1.5	Системы шифрования	Шифр RSA. Шифр Эль Гамаля. Цифровая подпись	
2. Лабораторные работы			
2.1	Работа с криптографическими средствами защиты	ГОСТ Р 34.12-2015, «Магма». ГОСТ Р 34.12-2015, «Кузнечик». Криптосистема Эль Гамаля.	Криптографические методы защиты информации (10.05.01)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоя-тельная работа	Всего
1.1	Основные понятия. Терминология.	6	0	4	10
1.2	Математические основы криптографии	8	0	12	20
1.3	Общие вопросы информационной безопасности	8	10	8	26
1.4	Особенные системы криптографии	8		4	12
1.5	Системы шифрования	4	4	4	12
2.1	Работа с криптографическими средствами защиты	0	20	8	28
	Итого:	34	34	40	108

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	Рябко, Б. Я. Криптографические методы защиты информации : учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097 (дата обращения: 5.04.2019). — Режим доступа: для авториз. пользователей.
2	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: 5.02.2022). — Режим доступа: для авториз. пользователей.
3	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: 5.02.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
4	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.
5	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
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
8	Криптографические методы защиты информации (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.

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 проекта. 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 методы защиты информации», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение: ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

Список аудиторий ФКН:
394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 479
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, ауд. 505п
Учебная аудитория: специализированная мебель, компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 292
Учебная аудитория: специализированная мебель, компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6’’ FHD Lenovo V155-15API

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, ауд. 380
Учебная аудитория: специализированная мебель, компьютер преподавателя i3-3240-3,4ГГц, монитор с ЖК 17’’, мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 291
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 293
Учебная аудитория: специализированная мебель, персональные компьютеры на базе Core i7-11700K-3.6 ГГц, мониторы ЖК 24’’ (16 шт.), мультимедийный проектор, экран. Лабораторное оборудование компьютерной графики видеоадаптеры GeForce RTX 3070.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 297
Учебная аудитория: специализированная мебель, ноутбуки HP EliteBook на базе Intel Core i5-8250U-3.4 ГГц, мониторы ЖК 24’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 382
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24’’ (16 шт.), ТВ панель-флипчарт.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 385
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1а, аудитория 387
Учебная аудитория: специализированная мебель, компьютер преподавателя Core2Duo-E7600-3ГГц, монитор с ЖК 22’’, мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 314п
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i3-7100-3,6ГГц, мониторы ЖК 19’’ (16 шт.), мультимедийный проектор, экран.

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 316п
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19’’ (30 шт.), мультимедийный проектор, экран

394018, г. Воронеж, площадь Университетская, д. 1, корпус 1б, аудитория 303п
Учебная аудитория: специализированная мебель, персональные компьютеры на базе i3-8100-3,9ГГц, мониторы ЖК 24'' (13 шт.), мультимедийный проектор, экран.
Лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности: персональные компьютеры на базе Intel i3-8100 3.60ГГц, мониторы ЖК 19'' (10 шт.), стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС".

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
1.1	Основные понятия. Терминология.	ОПК-10	ОПК-10.1-3	Контрольная работа
1.2	Математические основы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.3	Общие вопросы информационной безопасности	ОПК-10	ОПК-10.1-3	Контрольная работа
1.4	Особенные системы криптографии	ОПК-10	ОПК-10.1-3	Контрольная работа
1.5	Системы шифрования	ОПК-10	ОПК-10.2, 5	Контрольная работа
2.1	Работа с криптографическими средствами защиты	ОПК-10	ОПК-10.4-6	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:

- контрольная работа,
- 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. Студент выполняет предложенное преподавателем задание, представляет его в письменном виде, при необходимости, комментирует выполненные действия, анализирует и интерпретирует результаты. В курсе предусмотрена одна контрольная работа (одна тема 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

Лабораторная работа №1 Тема: ГОСТ Р 34.12-2015, «Магма»

Теоретические сведения
1. Схема Фейстеля.
2. Операции по модулю.
3. Нелинейное преобразование.
4. Преобразование ключа.
Практическая часть
Обучение на основе компьютерной программы

Лабораторная работа №2 Тема: ГОСТ Р 34.12-2015, «Кузнечик».
Теоретические сведения
1. Простые и расширенные поля Галуа.
2. Преобразование ключа..
3. SP-сети.
Практическая часть
1. Реализация и исследование стандарта.
2. Подготовка и защита отчёта по лабораторной работе.

Лабораторная работа №3 Тема: Криптосистема Эль Гамаля.
Теоретические сведения

1. Понятие дискретного алгоритма.
2. Криптостойкость.
3. Сравнение с RSA.

Практическая часть

1. Обучение на основе компьютерной программы.
2. Подготовка и защита отчёта по лабораторной работе.

Технология проведения

Все лабораторные работы обязательны для выполнения. 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 зачету.

Перечень вопросов к зачету (КИМ №1)

1. Что такое информационная безопасность?
2. В чем заключаются постулаты информационной безопасности?
3. Чем достигается обеспечение безопасности?
4. Что такое способы защиты информации?
5. В чем проявляются угрозы информации?
6. Что такое инженерно-техническая защита информации?
7. Что такое цена и ценность информации?
8. В чем состоят цели защиты информации?
9. Что подразумевается под эффективностью защиты информации?
10. Что такое система безопасности?
11. Охарактеризуйте физические системы защиты информации.
12. На какие классы разделяются инженерно-технические средства защиты информации?
13. Что такое криптология, криптограмма, криптография, криптоанализ?
14. Дайте определение криптосистемы (шифра).
15. В чем состоит основная идея шифрования данных?
16. В чем различие и в чем сходство шифрования и кодирования?
17. В чем различие терминов "дешифрование" и "расшифрование"?
18. Для решения каких задач используется кодирование информации?
19. Охарактеризуйте методы симметричного шифрования данных.
20. Опишите схему симметричного шифрования информации.
21. Приведите упрощённую схему алгоритма шифрования/расшифрования DES?
22. Что такое криптостойкость?
23. Каковы количественные характеристики криптостойкости?
24. Каким образом классифицируется инженерно-техническая защита информации?
25. Перечислите возможные виды утечек информации.

26. Сформулируйте основные законы модулярной арифметики.
27. Что представляет собой функция Эйлера?
28. В чем состоит теорема Эйлера?
29. Охарактеризуйте основные способы нахождения обратных по модулю величин.
30. Что такое криптосистема Эль Гамаля?

Критерии оценки ответов на вопросы зачета

Для оценивания результатов обучения на зачете 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:

$$Q_{пром\_ат} = 0{,}4Q_{КР} + 0{,}6Q_{зач}$$

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.