

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.В.05 Математические методы в криптографии

1. Код и наименование направления подготовки / специальности:

01.04.02 Прикладная математика и информатика

2. Профиль подготовки / специализация/магистерская программа:

Математическое и программное обеспечение информационных систем

3. Квалификация (степень) выпускника: магистр

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: НМС факультета Прикладной математики, информатики и механики № 8 от 15.04.2022

8. Учебный год: 2023/2024

Семестр(ы): 4

9. Цели и задачи учебной дисциплины

Цели изучения дисциплины: получение теоретических и практических знаний, необходимых для проектирования и реализации адаптивных криптографических систем; получение опыта организации и руководства проведения работ по обработке и анализу научно-технической информации.

Задачи изучения дисциплины: получение знаний об основных тенденциях развития информационных технологий в области защиты БД, способов и технологий обновления защищённых БД, механизмов контроля обновления БД; получение навыков проведения анализа возможностей внедрения новых информационных технологий, планирования и осуществления мероприятий по переходу на новые версии защищённых БД; приобретение опыта разработки и описания типовых процессов миграции защищённых БД на новые платформы и новые версии ПО.

10. Место учебной дисциплины в структуре ОПОП:

дисциплина относится к части, формируемой участниками образовательных отношений, 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
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации, результатов исследований	ПК-1.3	Выбирает методы решения поставленной задачи с учетом имеющихся ресурсов, а также теоретического обобщения научных данных, результатов экспериментов и наблюдений.	Знать: основные тенденции развития информационных технологий в области защиты БД, способы и технологии обновления защищённых БД, механизмы контроля обновления БД. Умеет анализировать возможности внедрения новых информационных технологий, планировать, организовывать и осуществлять мероприятия по переходу на новые версии защищённых БД. Владеет навыками разработки и описания типовых процессов миграции защищённых БД на новые платформы и новые версии
ПК-2	Способен осуществлять научное руководство проведением исследований по отдельным задачам	ПК-2.2	Организует сбор и изучение научно-технической информации по теме проводимых исследований и разработок.	

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом —2/72.

Форма промежуточной аттестации зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)			
	Всего	В том числе в интерактивной форме	По семестрам	
			№ сем. 4	№ сем.

Аудиторные занятия					
в том числе:	лекции	24		24	
	практические	-		-	
	лабораторные	12		12	
Самостоятельная работа		36		36	
Форма промежуточной аттестации		Зачет с оценкой		Зачет с оценкой	
Итого:		72		72	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Стойкость криптографических систем	Информационно-теоретический подход, подход на основе теории сложности	Математические методы в криптографии (01.04.02)
1.2	Математические модели шифрования с использованием конечных полей	Первообразные корни, дискретные логарифмы, поля Гауа	
1.3	Линейные рекуррентные последовательности над конечными полями	Элементы теории конечного поля. Последовательности максимального периода	
1.4	Применение конечных полей в поточных шифрах	Адаптивные криптографические системы	
2. Лабораторные работы			
2.1	Линейные рекуррентные последовательности над конечными полями	Простые поля Гауа в криптографии.	
2.2	Применение конечных полей в поточных шифрах	Расширенные поля Гауа в криптографии	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Стойкость криптографических систем	4			6	10
2	Математические модели шифрования с использованием конечных полей	10			18	34
3	Линейные рекуррентные последовательности над конечными полями	6		6	12	24

4	Применение конечных полей в поточных шифрах	4		6	-	4
	Итого:	24		12	36	72

14. Методические указания для обучающихся по освоению дисциплины

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

Лекционные занятия посвящены рассмотрению теоретических основ базовых понятий, стандартов. Лабораторные работы предназначены для формирования умений и навыков, закрепленных компетенций по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, подготовку к лабораторным работам и к зачету.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, перед лабораторными работами просматривать конспекты лекций.

При использовании дистанционных образовательных технологий и электронного обучения следует выполнять все указания преподавателя 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 . — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
2	Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157578 . — Режим доступа: для авториз. пользователей.
3	Бутакова, Н. Г. Криптографические методы и средства защиты информации : учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург : Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161347 . — Режим доступа: для авториз. пользователей.
4	Криптографические методы защиты информации : учебное пособие / составители И. А. Калмыков [и др.]. — Ставрополь : СКФУ, 2015. — 109 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155280 . — Режим доступа: для авториз. пользователей.

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	Математические методы в криптографии (01.04.02)/ Ю.А. Степанец — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/

16. Перечень учебно-методического обеспечения для самостоятельной работы

Самостоятельная работа обучающегося должна включать подготовку к лабораторным работам и подготовку к промежуточной аттестации.

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.

Указанные в учебно-методическом комплексе учебные пособия и справочные материалы, приведены в таблице ниже:

№ 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 . — Режим доступа: для авториз. пользователей.
2	Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157578 . — Режим доступа: для авториз. пользователей.
3	Электронно-библиотечная система «Лань». - Режим доступа: https://e.lanbook.com .
4	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http://www.lib.vsu.ru .
5	Математические методы в криптографии (01.04.02)/ Ю.А. Степанец — Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/

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 самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в.

18. Материально-техническое обеспечение дисциплины:

Лекции: лекционная аудитория, учебная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Лабораторные работы: специализированная аудитория, оснащенная учебной мебелью и персональными компьютерами для индивидуальной работы с возможностью подключения к сети «Интернет» (компьютерные классы, студии), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).

Самостоятельная работа: учебная мебель, компьютерный класс, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение:

- ОС Windows 10,
- интернет-браузер (Mozilla Firefox);
- ПО Adobe Reader;
- пакет стандартных офисных приложений для работы с документами, таблицами (МойОфис, LibreOffice).

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	Стойкость криптографических систем	ПК-1, ПК-2	ПК-1.3, ПК-2.2	Лабораторная работа
2	Математические модели шифрования с использованием конечных полей	ПК-1, ПК-2	ПК-1.3, ПК-2.2	Лабораторная работа
3	Линейные рекуррентные последовательности над конечными полями	ПК-1, ПК-2	ПК-1.3, ПК-2.2	Лабораторная работа
4	Применение конечных полей в поточных шифрах	ПК-1, ПК-2	ПК-1.3, ПК-2.2	Лабораторная работа
Промежуточная аттестация, форма контроля – зачет с оценкой				

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: лабораторные работы.

Перечень лабораторных работ

Лабораторная работа №1 Простые поля Галуа в криптографии.

Содержание

Теоретические сведения 1. Формула и теорема Эйлера. 2. Обратные по модулю величины. 3. Шифрование и расшифрование в БД. Практическая часть 1. Освоение законов модулярной арифметики. 2. Подготовка и защита отчёта по лабораторной работе.

Лабораторная работа №2 Расширенные поля Галуа в криптографии.

Содержание

Теоретические сведения 1. Современные стандарты криптопреобразований. 2. Защита информации в БД. 3. Имитозащита. 4. Режимы работы криптосистем. Практическая часть 1. Освоение стандартов криптозащиты в БД. 2. Подготовка и защита отчёта по лабораторной работе.

Технология проведения

Студент выполняет предложенные преподавателем задания, результаты представляет на дисплее, комментирует выполненные действия, анализирует и интерпретирует результаты.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (выполнены все задания, 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

1. Классификация криптографических методов защиты информации.
2. Основная теорема арифметики. Некоторые проблемы теории чисел.
3. Атаки на криптосистемы с симметричными ключами. Ограничения на использование идеальных криптосистем.
4. Стойкость криптосистем и алгоритмов.
5. Информационно-теоретический подход к оценке стойкости криптосистем.
6. Вычислительная сложность криптоалгоритмов.
7. Первообразные корни и их свойства.
8. Индексы (дискретные логарифмы) и их свойства.
9. Поля Галуа. Многочлены над простыми полями.
10. Китайская теорема об остатках для многочленов.
11. Линейные рекуррентные последовательности над конечными полями. Последовательности максимального периода.
12. Методы защиты информации в БД.
13. Криптоанализ алгоритмов защиты информации.
14. Применение конечных полей в поточных шифрах.

Критерии оценки ответов на вопросы зачета

Для оценивания результатов обучения на зачете используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, все лабораторные работы выполнены.	Повышенный уровень	Отлично
Обучающийся владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, но допускает ошибки при ответе, все лабораторные работы выполнены.	Базовый уровень	Хорошо

Обучающийся частично владеет частично теоретическими основами дисциплины, фрагментарно способен иллюстрировать ответ примера, все лабораторные работы выполнены.	Пороговый уровень	Удовлетворительно
Обучающийся демонстрирует отрывочные, фрагментарные знания, лабораторные работы не выполнены	–	Неудовлетворительно