ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Кафедра Цифровых систем и инженерных технологий

Принято Ученым советом
Университета Вернадского
«26» сентября 2024 г. протокол №2

«УТВЕРЖДЕНО»
Проректор по образовательной деятельности
_____Кудрявцев М.Г.
«26» сентября 2024 г.

Рабочая программа дисциплины

Теоретико-числовые основы защиты информации

Направление подготовки 44.04.01 Педагогическое образование

Направленность (профиль) программы Прикладная математика и информатика

Квалификация Магистр

Форма обучения **очная**

Балашиха 2024

Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки 44.04.01 Педагогическое образование

Рабочая программа дисциплины разработана *доцентом кафедры цифровых систем и инженерных технологий, к.т.н. Рамазановой Г.Г.*

Рецензент: *доцент кафедры цифровых систем и инженерных технологий, к.ф.н. Хисматуллина Ю.Р.*

1. Планируемые результаты обучения по дисциплине, соотнесенные с установленными в ОПОП ВО индикаторами достижения компетенций

1.1 Перечень компетенций, формируемых учебной дисциплиной

Код и наименование компетенции	Индикаторы достижения компетенций Планируемые результаты обучения
Профессиональные компетенции	
ПК-1 Способен применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов	Знать: теоретическую информатику, фундаментальную и прикладную математику для анализа и синтеза информационных систем и процессов Уметь: Самостоятельно определяет тематику, цели, содержание, формы, методы и средства, ожидаемые результаты деятельности обучающихся, в том числе с особыми образовательными потребностями Владеть: способностью оценивать результаты анализа и синтеза информационных систем и процессов на всех этапах

2. Цели и задачи освоения учебной дисциплины, место дисциплины в структуре ОПОП ВО

Дисциплина «Теоретико-числовые основы защиты информации» относится к обязательной части основной профессиональной образовательной программы высшего образования 44.04.01 Педагогическое образование, профиль «Прикладная математика и информатика».

Целями изучения дисциплины «Теоретико-числовые основы защиты информации» является систематизация и расширение знаний студентов в области целых чисел и многочленов над конечными полями, овладение методами теории чисел, имеющими криптографические приложения для защиты информации.

3. Объем учебной дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий, текущий и промежуточный контроль по дисциплине) и на самостоятельную работу обучающихся

Вид учебной работы	3 семестр
Общая трудоемкость дисциплины, зачетных единиц	3
часов	**108**
Аудиторная (контактная) работа, часов	**28,25**
в т.ч. занятия лекционного типа	14
занятия семинарского типа	14
промежуточная аттестация	0,25
Самостоятельная работа обучающихся, часов	**75,75**
Вид промежуточной аттестации	зачёт

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Перечень разделов дисциплины с указанием трудоемкости аудиторной (контактной) и самостоятельной работы, видов контролей и перечня компетенций

Наименование разделов и тем	Трудоемкость, часов			Код компетенции
	всего	в том числе		
		аудиторной (контактной) работы	самостоятельной работы	
Раздел 1. Повторение. Теория делимости в Z. Простые и составные числа. Арифметические функции. Сравнения и их свойства. Сравнения с одной переменной. Системы сравнений.	**49**	14	35	ПК-1
Раздел 2. Первообразные корни и индексы. Многочлены над (конечными) полями. Основы компьютерной алгебры.	**55**	14,25	40,75	
Итого за семестр	**104**	28,25	75,75	
Промежуточная аттестация	4	0,25	-	
ИТОГО по дисциплине	**108**	**28,25**	**75,75**	

2. Содержание дисциплины по разделам

Раздел 1. Повторение. Теория делимости в Z. Простые и составные числа. Арифметические функции. Сравнения и их свойства. Сравнения с одной переменной. Системы сравнений.

Перечень учебных элементов раздела:

Свойства делимости целых чисел; простые числа; решето Эратосфена; теорема Евклида о бесконечности множества простых чисел. Основная теорема арифметики о разложении целых чисел на простые сомножители; наибольший общий делитель и наименьшее общее кратное. Оценки Чебышева для функции числа простых чисел, не превосходящих x. Арифметические функции: целая и дробная часть числа. Разложение числа n! на простые множители. Мультипликативные функции. Функция Эйлера и ее свойства; сумма делителей и число делителей. Оценки среднего значения арифметических функций. Повторение: Числовые сравнения, их основные свойства. Вычеты и классы вычетов по модулю m; кольца классов вычетов; полная система вычетов; приведенная система вычетов. Теоремы Эйлера и Ферма. Сравнения первой степени с одним неизвестным, простейшие приемы решений. Квадратичные вычеты и невычеты; число решений сравнения: критерий Эйлера для квадратичных вычетов и невычетов. Степенные вычеты и невычеты n-ой степени; число степенных вычетов; критерий для отыскания степенных вычетов; решение двучленных сравнений с помощью вычетов. Системы сравнений; их решения. Сравнения n-ой степени по составному модулю; сведение сравнения по составному модулю к системе сравнений по простому модулю; сравнения второй степени: сведение сравнения второй степени к двучленному сравнению. Символ Лежандра и его свойства; закон взаимности квадратичных вычетов; сравнения второй степени по составному модулю.

Раздел 2. Первообразные корни и индексы. Многочлены над (конечными) полями. Ос-новы компьютерной алгебры.

Перечень учебных элементов раздела:

Первообразные корни и индексы: показатель числа по модулю m; свойства показателей; теорема о существовании первообразного корня по простому модулю; первообразные корни по модулям p и 2p; теорема об отыскании первообразных корней; индексы по модулям p и 2p; таблицы индексов; двучленные сравнения n-ой степени; существование решений. Повторение: основные понятия и теоремы теории многочленов над полем. Неприводимые многочлены над конечным полем. Строение конечных полей.

Порядок многочлена. Нахождение НОД. Разложение полинома на простые множители по модулю p. Разложение полинома над Z. Компьютерная алгебра (КА) как наука, ее отличительные особенности. Системы компьютерной алгебры (обзор).Представление данных в системах КА: представление целых чисел, дробей, вещественных чисел, представление полиномов. Возможности оптимизации вычислительных операций. Целые числа произвольной точности, алгоритмы для сложения, вычитания, умножения и деления. Восстановление целого числа по остаткам. Деление в модулярной арифметике. Кольцо многочленов над кольцом с единицей. Сложность умножения двух многочленов. Интерполяция многочленов.

5. Оценочные материалы по дисциплине

Оценочные материалы по дисциплине представлены в виде фонда оценочных средств.

6. Материально-техническое и учебно-методическое обеспечение дисциплины

6.1 Перечень учебно-методического обеспечения по дисциплине

№ п/п	Автор, название, место издания, издательство, год издания, количество страниц, режим доступа
1	Методические указания по изучению дисциплины

6.2 Перечень учебных изданий, необходимых для освоения дисциплины

Основная литература:

1. Практикум по информатике / Н. М. Андреева, Н. Н. Василюк, Н. И. Пак, Е. К. Хеннер. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 248 с. — ISBN 978-5-507-47299-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/359810

2. Кудинов, Ю. И. Основы современной информатики : учебное пособие для вузов / Ю. И. Кудинов, Ф. Ф. Пащенко. — 6-е изд., стер. — Санкт-Петербург : Лань, 2024. — 256 с. — ISBN 978-5-507-47572-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/392393

3. Ганичева, А. В. Дискретная математика : учебное пособие для вузов / А. В. Ганичева, А. В. Ганичев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 160 с. — ISBN 978-5-507-49204-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/382370

Дополнительная литература:

1. Перельман, Я. И. Занимательная математика : научно-популярное издание / Я. И. Перельман. — Санкт-Петербург : Лань, 2024. — 96 с. — ISBN 978-5-507-51673-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427199

2. Белова, О. О. Дискретная математика. Практикум / О. О. Белова. — Санкт-Петербург : Лань, 2024. — 384 с. — ISBN 978-5-507-48259-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/367442

6.3 Современные профессиональные базы данных, информационные справочные системы и лицензионное программное обеспечение

Современные профессиональные базы данных, информационные справочные системы, цифровые электронные библиотеки и другие электронные образовательные ресурсы

1. Договор о подключении к Национальной электронной библиотеке и предостав-

лении доступа к объектам Национальной электронной библиотеки №101/НЭБ/0502-п от 26.02.2020 5 лет с пролонгацией

2. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 27.04.2016 бессрочно

3. Соглашение о бесплатном тестовом доступе к Polpred.com. Обзор СМИ 02.03.2020 бессрочно

4. Информационно-справочная система «Гарант» – URL: https://www.garant.ru/ Информационно-справочная система Лицензионный договор № 261709/ОП-2 от 25.06.2021

5. «Консультант Плюс». – URL: http://www.consultant.ru/ свободный доступ

6. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014).

Доступ к электронной информационно-образовательной среде, информационно-телекоммуникационной сети «Интернет»

1. Система дистанционного обучения Moodle www.portfolio.rgunh.ru (свободно распространяемое)

2. Право использования программ для ЭВМ Mirapolis HCM в составе функциональных блоков и модулей: Виртуальная комната.

3. Инновационная система тестирования – программное обеспечение на платформе 1С (Договор № К/06/03 от 13.06.2017). Бессрочный.

4. Образовательный интернет – портал Университета Вернадского (свидетельство о регистрации средства массовых информации Эл № ФС77-51402 от 19.10.2012).

Лицензионное и свободно распространяемое программное обеспечение

1. OpenOffice – свободный пакет офисных приложений (свободно распространяемое)

2. linuxmint.com https://linuxmint.com/ (свободно распространяемое)

3. Электронно-библиотечная система AgriLib http://ebs.rgunh.ru/ (свидетельство о государственной регистрации базы данных №2014620472 от 21.03.2014) собственность университета.

4. Официальная страница ФГБОУ ВО МСХ РФ «Российский государственный университет народного хозяйства имени В.И. Вернадского» https://vk.com/rgunh.ru (свободно распространяемое)

5. Портал ФГБОУ ВО МСХ РФ «Российский государственный университет народного хозяйства имени В.И. Вернадского» (свободно распространяемое) https://zen.yandex.ru/id/5fd0b44cc8ed19418871dc31

6. Антивирусное программное обеспечение Dr. WEB Desktop Security Suite (Сублицензионный договор №13740 на передачу неисключительных прав на программы для ЭВМ от 01.07.2021).

6.4 Перечень учебных аудиторий, оборудования и технических средств обучения

Учебная аудитория для проведения лекционных занятий (поточная). Специализированная мебель, доска меловая, мультимедийное оборудование, проектор, экран настенный	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д.50, каб. 129 Площадь помещения 118,1 кв.м № по технической инвентаризации 140, этаж 1
Учебная аудитория для занятий лекционного типа, семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы), для проведения групповых консультаций и индивидуальной работы обучавшихся с педагогическими работниками, для проведения текущего контроля и промежуточной аттестации.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 125 Площадь помещения 51,6 кв.м № по технической инвентаризации 136, этаж 1

Специализированная мебель, доска меловая. Мультимедийное оборудование, проектор, экран настенный	
Помещение для самостоятельной работы. Персональные компьютеры в сборке с выходом в интернет.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, читальный зал Площадь помещения 497,4 кв. м. № по технической инвентаризации 177, этаж 1
Помещение для самостоятельной работы. Специализированная мебель, персональные компьютеры в сборке с выходом в интернет.	143900, Московская область, г. Балашиха, ул. Юлиуса Фучика д.1, каб. 320 Площадь помещения 49,7 кв. м. № по технической инвентаризации 313, этаж 3
Учебная аудитория для учебных занятий обучающихся из числа инвалидов и лиц с ОВЗ. Специализированная мебель. Автоматизированное рабочее место для инвалидов-колясочников с коррекционной техникой и индукционной системой ЭлСис 290; Автоматизированное рабочее место для слабовидящих и незрячих пользователей со стационарным видеоувеличителем ЭлСис 29 ON; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с портативным видеоувеличителем ЭлСис 207 CF; Автоматизированное рабочее место для слабовидящих и незрячих пользователей с читающей машиной ЭлСис 207 CN; Аппаратный комплекс с функцией видеоувеличения и чтения для слабовидящих и незрячих пользователей ЭлСис 207 OS.	143907, Московская область, г. Балашиха, ул. шоссе Энтузиастов, д. 50, каб. 105 Площадь помещения 52,8 кв. м. № по технической инвентаризации 116, этаж 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НАРОДНОГО ХОЗЯЙСТВА ИМЕНИ В.И. ВЕРНАДСКОГО»
(Университет Вернадского)

Кафедра Цифровых систем и инженерных технологий

Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Теоретико-числовые основы защиты информации

Направление подготовки 44.04.01 Педагогическое образование

Направленность (профиль) программы Прикладная математика и информатика

Квалификация Магистр

Форма обучения **очная**

Балашиха 2024 г.

1.Описание показателей и критериев оценивания планируемых результатов обучения по учебной дисциплине

Компетенций	Индикатор сформированности компетенций	Уровень освоения	Планируемые результаты обучения
ПК-1 Способен применять знания теоретической информатики, фундаментальной и прикладной математики для анализа и синтеза информационных систем и процессов	**Знать (З):** теоретическую информатику, фундаментальную и прикладную математику для анализа и синтеза информационных систем и процессов **Уметь (У):** Самостоятельно определяет тематику, цели, содержание, формы, методы и средства, ожидаемые результаты деятельности обучающихся, в том числе с особыми образовательными потребностями **Владеть (В):** способностью оценивать результаты анализа и синтеза информационных систем и процессов на всех этапах	**Пороговый (удовлетворительно)**	**Знать:** теоретическую информатику, фундаментальную и прикладную математику для анализа и синтеза информационных систем и процессов **Уметь:** Самостоятельно определяет тематику, цели, содержание, формы, методы и средства, ожидаемые результаты деятельности обучающихся, в том числе с особыми образовательными потребностями **Владеть:** способностью оценивать результаты анализа и синтеза информационных систем и процессов на всех этапах
		Продвинутый (хорошо)	**Знать:** теоретическую информатику, фундаментальную и прикладную математику для анализа и синтеза информационных систем и процессов **Уметь:** Самостоятельно определяет тематику, цели, содержание, формы, методы и средства, ожидаемые результаты деятельности обучающихся, в том числе с особыми образовательными потребностями **Владеть:** способностью оценивать результаты анализа и синтеза информационных систем и процессов на всех этапах
		Высокий (отлично)	**Знать:** теоретическую информатику, фундаментальную и прикладную математику для анализа и синтеза информационных систем и процессов **Уметь:** Самостоятельно определяет тематику, цели, содержание, формы, методы и средства, ожидаемые результаты деятельности обучающихся, в том числе с особыми образовательными потребностями **Владеть:** способностью оценивать результаты анализа и синтеза информационных систем и процессов на всех этапах

2. Описание шкал оценивания

2.1 Шкала оценивания на этапе текущего контроля

Форма текущего контроля	Отсутствие усвоения (ниже порогового)*	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Доклад	не выполнена или все задания решены неправильно	Цель и задачи доклада достигнуты частично. Актуальность темы определена неубедительно.	Цель и задачи выполнения доклада достигнуты. Актуальность темы подтверждена. Доклад	Цель написания доклада достигнута, задачи решены. Актуальность темы исследования

		В докладе выявлены значительные отклонения от требований методических указаний.	выполнен с незначительными отклонениями от требований методических указаний.	корректно и полно обоснована. Доклад выполнен согласно требованиям.

2.2 Шкала оценивания на этапе промежуточной аттестации (зачет и экзамен, курсовая работа)

Форма промежуточной аттестации	Отсутствие усвоения (ниже порогового)	Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
Ответы на вопросы к зачёту	не выполнена или все задания решены неправильно	Цель и задачи вопроса достигнуты частично. Актуальность темы определена неубедительно.	Цель и задачи выполнения вопроса достигнуты. Актуальность темы подтверждена.	Цель написания ответа на вопрос достигнута, задачи решены.

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ

ВОПРОСЫ ДЛЯ ПОДГОТОВКИ ДОКЛАДОВ

1. Понятие математической защиты информации и информационной безопасности
2. Способы защиты информации.
3. Некоторые исторические алгоритмы (алгоритмы Цезаря, Виженера).
4. Криптоанализ исторических алгоритмов (алгоритмы Цезаря, Виженера).
5. Влияние длины блока на криптографическую стойкость алгоритма (алгоритмы Хилла и Плейфейра).
6. Ассиметричная криптосистема: рюкзачная криптосистема и ее криптоанализ.
7. Ассиметричная криптосистема: плотный рюкзак.
8. Крптосистема RSA и ее криптоанализ.
9. Криптосистемы основанные на дискретных логарифмах.
10. Криптосистемы Рабина, Эль-Гамеля.
11. Криптосистема Вильемса, Уильямса
12.Обзор потоковых кодов.
13. Симметричные криптосистемы (алгоритмы DES, Blowfish, Гост28147-89, AES, RC6, Serpent, Mars).

ПРИМЕРНАЯ ТЕМАТИКА ВОПРОСОВ К ЗАЧЕТУ

1. ЭЦП RSA, ЭЦП Эль-Гамаля.
2. Схема ЭЦП DSA и ее модификация.
3. Схема ГОСТ Р34.10-94 и ее модификация.
4. Подделка ЭЦП. Неотрицаемые цифровые подписи
5. Криптосистемы основанные на эллептических кривых.
6. Свойства криптографических хэш-функций. Их использование в протоколах аутентификации и для контроля изменения чувствительной информации. Однонаправленные хэш-функции, использующие симметричные блочные алгоритмы.
7. Хэш-функция MD5
8. Хэш-функция SHA-1
9. Распределение ключей. Трехпроходный протокол Шамира.
10. Открытое распределение ключей
11.Обмен зашифрованными ключами: базовый протокол EKE (реализация EKE с помощью RSA, Эль-Гамаля, Diffie-Hellman.)
12. Разделение секрета. Схема интерполяционных многочленов Лагранжа.
13. Подсознательный канал (Ong-Schnorr-Shamir, Эль-Гамаль, DSA).
14. Доказательство с нулевым знанием.