

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования "Пермский
государственный национальный исследовательский
университет"**

Кафедра информационной безопасности и систем связи

**Авторы-составители: Шкарапута Александр Петрович
Мустакимова Яна Романовна**

Рабочая программа дисциплины

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Код УМК 69532

**Утверждено
Протокол №1
от «31» августа 2020 г.**

Пермь, 2020

1. Наименование дисциплины

Теоретико-числовые методы в криптографии

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность

направленность Разработка защищенного программного обеспечения

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Теоретико-числовые методы в криптографии** у обучающегося должны быть сформированы следующие компетенции:

10.05.01 Компьютерная безопасность (направленность : Разработка защищенного программного обеспечения)

ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности

ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

4. Объем и содержание дисциплины

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	14
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Зачет (10 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Теоретико-числовые методы в криптографии. Первый семестр

Введение в криптографические методы, основной математический аппарат

В этом разделе приводится классификация методов шифрования, их связь с математическим аппаратом, актуальность курса в современных условиях.

Базовые понятия теории групп: группа, поле, образующий элемент, смежный класс

Рассматриваются базовые понятия теории групп: группы, поля, образующего элемента. Применение теории групп в модульной арифметике.

Понятие вычетов как смежный классов. Кольцо вычетов. Рассматривается основная теорема алгебры, китайская теорема об остатках, малая теорема Ферма.

Свойства циклической группы. Свойства мультипликативной группы кольца вычетов.

Алгоритмы RSA и Эль-Гамала, на основе теории групп

Понятие алгоритма Эль-Гамала, шифрование и аутентикация. Первообразный корень.

Понятие алгоритма RSA, шифрование и аутентикация, его уязвимые места.- стандартные атаки.

Алгоритм быстрого возведения в степень по модулю. Использование Cryptools.

Расширения полей, многочлены над полем, характеристика поля

Рассматриваются расширения полей, многочлены над полем, характеристика поля. Применение операций над многочленами в поле определенной характеристики в криптографии (в частности алгоритме AES).

Алгоритмы обмена ключами, шифрования и аутентикации на основе Эллиптических кривых

Геометрия Эллиптических кривых. Подход на основе дискретизации, введение поля элементов (точек).

Понятие суммы точек и их произведения на число.

Основные свойства группы точек эллиптической кривой.

Алгоритмы шифрования и аутентификации на основе эллиптических кривых.

Дискретное преобразование Фурье на основе тригонометрической интерполяции и на основе теории групп, БПФ и его применение.

Рассматривается вывод дискретного преобразование Фурье на основе тригонометрической интерполяции.

Вывод ДПФ на основе теории групп. Быстрое преобразование Фурье и его применение при арифметических операциях с многочленами.

Применение ДПФ в длинной арифметике.

Зачет

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Рожков А. В., Ниссенбаум О. В. Теоретико-числовые методы в криптографии: учебное пособие / А. В. Рожков, О. В. Ниссенбаум. - Тюмень: Издательство Тюменского государственного университета, 2007, ISBN 978-5-88081-873-0. - 160. - Библиогр.: с. 155
2. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. - Москва: Горячая линия - Телеком, 2010, ISBN 978-5-9912-0150-6. - 232. - Библиогр.: с. 225-229

Дополнительная:

1. Алешников, С. И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях : практическое пособие / С. И. Алешников, Е. В. Козьминых. — Калининград : Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. — ISBN 5-88874-689-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/23851>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ

<http://www.mathnet.ru/> Общероссийский математический портал

<http://window.edu.ru/> Единое окно доступа к образовательным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Теоретико-числовые методы в криптографии** предполагает использование следующего программного обеспечения и информационных справочных систем:

- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:

- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice».

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

- система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).
- система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.
- система тестирования Indigo (<https://indigotech.ru/>).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для проведения практических занятий - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине
Теоретико-числовые методы в криптографии**

**Планируемые результаты обучения по дисциплине для формирования компетенции.
Индикаторы и критерии их оценивания**

ПК.3

Способность к анализу и формализации поставленных задач в области информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности	Знает способы оценки защищенности криптографических систем, умеет находить уязвимости криптографических систем и выбирать стратегию их защиты, владеет методами анализа криптографических систем	<p>Неудовлетворител не удовлетворяет требованиям на оценку "Удовлетворительно"</p> <p>Удовлетворительн Знает основные способы оценки защищенности криптографических систем, имеет представление об их основных уязвимостях</p> <p>Хорошо Знает основные способы оценки защищенности криптографических систем, умеет находить уязвимости криптографических систем</p> <p>Отлично Знает способы оценки защищенности криптографических систем, умеет находить уязвимости криптографических систем, способен анализировать криптографические системы выбирать стратегию их защиты</p>

ПК.6

Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	Знает основные принципы построения криптографических систем и связанных с ними математический аппарат; умеет использовать эти знания для задач шифрования, аутентификации, обмена ключами, криптографического анализа; владеет методами построения криптографических систем и их анализа	<p>Неудовлетворител не удовлетворяет требованиям, необходимым для получения оценки "Удовлетворительно"</p> <p>Удовлетворительн Знает каким образом влияют ключевые параметры алгоритмов, влияющие на основные его характеристики (криптостойкость, скорость, емкость занимаемой памяти...)</p> <p>Хорошо</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо</p> <p>Умеет подбирать ключевые параметры алгоритмов, влияющие на основные его характеристики (криптостойкость, скорость, емкость занимаемой памяти...)</p> <p>Отлично</p> <p>Знает о возможностях модификации существующих алгоритмов шифрования и аутентификации на основе математических моделей. Умеет подбирать ключевые параметры алгоритмов, влияющие на основные его характеристики (криптостойкость, скорость, емкость занимаемой памяти...)</p>

ПК.11

способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.11</p> <p>способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>	<p>Знает механизмы защиты криптографических систем, умеет проводить криптоанализ, умеет предлагать безопасные решения для построения криптографических систем</p>	<p>Неудовлетворител</p> <p>не удовлетворяет требованиям на оценку "Удовлетворительно"</p> <p>Удовлетворительн</p> <p>Знает основные механизмы защиты криптографических систем</p> <p>Хорошо</p> <p>Знает основные механизмы защиты криптографических систем, знает основные математические методы криптоанализа</p> <p>Отлично</p> <p>Знает механизмы защиты криптографических систем, умеет проводить криптоанализ, способен предлагать безопасные решения для построения криптографических систем</p>

ПСК.6

Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПСК.6</p> <p>Способность применять</p>	<p>Знает языки, системы и инструментальные средства</p>	<p>Неудовлетворител</p> <p>не удовлетворяет требованиям на оценку</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	программирования на основе которых возможно создавать криптографические системы и их отдельные элементы; умеет создавать программы на основе криптографических систем; владеет методами анализа созданных программ на основе криптографических систем и их отдельных элементов	<p>Неудовлетворител "Удовлетворительно"</p> <p>Удовлетворительн Знает языки, системы и инструментальные средства программирования на основе которых возможно создавать криптографические системы и их отдельные элементы</p> <p>Хорошо Знает языки, системы и инструментальные средства программирования на основе которых возможно создавать криптографические системы и их отдельные элементы; умеет создавать программы на основе криптографических систем</p> <p>Отлично Знает языки, системы и инструментальные средства программирования на основе которых возможно создавать криптографические системы и их отдельные элементы; умеет создавать программы на основе криптографических систем; способен анализировать созданные программы на основе криптографических систем и их отдельных элементов</p>

ПСК.5

способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах	Знает основные программные продукты на основе криптографических систем, умеет оценивать эффективность новых образцов программных продуктов на основе анализа применяемых криптографических систем, владеет навыками выбора наиболее оптимальных конфигураций программных продуктов.	<p>Неудовлетворител не удовлетворяет требованиям на оценку "Удовлетворительно"</p> <p>Удовлетворительн Знает основные программные продукты на основе криптографических систем</p> <p>Хорошо Знает основные программные продукты на основе криптографических систем, умеет оценивать эффективность новых образцов программных продуктов на основе анализа применяемых криптографических систем</p> <p>Отлично Знает основные программные продукты на</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично основе криптографических систем, умеет оценивать эффективность новых образцов программных продуктов на основе анализа применяемых криптографических систем, способен выбирать наиболее оптимальные конфигурации программных продуктов.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

Вид мероприятия промежуточной аттестации : Зачет

Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 43 до 60

«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	Алгоритмы RSA и Эль-Гамала, на основе теории групп Письменное контрольное мероприятие	контрольное мероприятие - тест
ПК.3 Способность к анализу и формализации поставленных задач в области информационной безопасности ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем ПК.11 способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи	Алгоритмы обмена ключами, шифрования и аутентикации на основе Эллиптических кривых Письменное контрольное мероприятие	контрольное мероприятие - тест

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.5 способность оценивать эффективность новых образцов программных средств защиты в компьютерных системах	Зачет Итоговое контрольное мероприятие	контрольное мероприятие - тест

Спецификация мероприятий текущего контроля

Алгоритмы RSA и Эль-Гамала, на основе теории групп

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
знание базовых понятий и вывода основных формул в теории групп	20
применение элементов теории групп в алгоритмах RSA и Эль-Гамала	10

Алгоритмы обмена ключами, шифрования и аутентификации на основе Эллиптических кривых

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **13**

Показатели оценивания	Баллы
Алгоритмы обмена ключами, шифрования и аутентификации на основе Эллиптических кривых	15
Понятия: расширения полей, многочлены над полем, характеристика поля и их применение.	15

Зачет

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Расширения полей, многочлены над полем, характеристика поля. Их применение в криптографии.	10
Эллиптические кривые	10
Основные алгоритмы криптографии и их математическое обоснование	10
Дискретное преобразование Фурье	5
Базовые понятия теории групп и их применение в традиционных алгоритмах шифрования.	5