МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

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

Рабочая программа дисциплины

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Код УМК 69532

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

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

специализация 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 (специализация : Разработка защищенного программного обеспечения)

ОПК.1 Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Индикаторы

ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук

ОПК.1.2 Осуществляет первичный сбор и анализ материала, интерпретирует различные математические и физические объекты

ОПК.1.3 Использует практический опыт решения стандартных задач математических и (или) естественных наук

ОПК.6 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Индикаторы

ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

ОПК.9 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Индикаторы

ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации

ОПК.9.2 Анализирует возможности криптографических средств защиты информации

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: 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-Гамаля, на основе теории групп
Понятие алгоритма Эль-Гамаля, 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 обмены 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 c. — 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-образовательной 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

ОПК.6

Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.6.1 Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	Знать основные требования безопасности компьютерных систем и сетей. Уметь проводить разработки в области обеспечения безопасности компьютерных систем и сетей. Владеть методами и приемами научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.	**Неудовлетворител** Не знает основные требования безопасности компьютерных систем и сетей. Не умеет проводить разработки в области обеспечения безопасности компьютерных систем и сетей. Не владеет методами и приемами научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. **Удовлетворительн** Знает основные требования безопасности компьютерных систем и сетей. Не умеет проводить разработки в области обеспечения безопасности компьютерных систем и сетей. Не владеет методами и приемами научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. **Хорошо** Знает основные требования безопасности компьютерных систем и сетей. Умеет проводить разработки в области обеспечения безопасности компьютерных систем и сетей. Не владеет в полной мере методами и приемами научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей. **Отлично** Знает основные требования безопасности компьютерных систем и сетей. Умеет проводить разработки в области обеспечения безопасности компьютерных

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично систем и сетей. Владеет в полной мере методами и приемами научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

ОПК.1

Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.1.1 Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук	Знать базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Уметь применять на практике базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Владеть навыками применения базовых понятий, основной терминологии и знаний основных положений и концепций в области математических и естественных наук при решении профессиональных задач.	**Неудовлетворител** Не знает базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Не умеет применять на практике базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Не владеет навыками применения базовых понятий, основной терминологии и знаний основных положений и концепций в области математических и естественных наук при решении профессиональных задач. **Удовлетворительн** Знает базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Умеет с ошибками применять на практике базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Не владеет навыками применения базовых понятий, основной терминологии и знаний основных положений и концепций в области математических и естественных наук при решении профессиональных задач. **Хорошо** Знает базовые понятия, основную терминологию и знания основных положений и концепций в области

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо математических и естественных наук. Умеет без ошибок применять на практике базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Не владеет в полной мере навыками применения базовых понятий, основной терминологии и знаний основных положений и концепций в области математических и естественных наук при решении профессиональных задач. **Отлично** Знает базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Умеет без ошибок применять на практике базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук. Владеет в полной мере навыками применения базовых понятий, основной терминологии и знаний основных положений и концепций в области математических и естественных наук при решении профессиональных задач.
ОПК.1.2 Осуществляет первичный сбор и анализ материала, интерпретирует различные математические и физические объекты	Знать методы сбора и анализа материала, интерпретации различных математических и физических объектов. Уметь осуществлять первичный сбор и анализ материала, обобщать полученную информацию. Владеть навыками интерпретации различных математических и физических объектов.	**Неудовлетворител** Не знает методы сбора и анализа материала, интерпретации различных математических и физических объектов. Не умеет осуществлять первичный сбор и анализ материала, обобщать полученную информацию. Не владеет навыками интерпретации различных математических и физических объектов. **Удовлетворительн** Знает методы сбора и анализа материала, интерпретации различных математических и физических объектов. Умеет осуществлять первичный сбор и анализ материала, но не умеет обобщать

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн полученную информацию. Не владеет навыками интерпретации различных математических и физических объектов. **Хорошо** Знает методы сбора и анализа материала, интерпретации различных математических и физических объектов. Умеет осуществлять первичный сбор и анализ материала, обобщать полученную информацию. Не владеет в полной мере навыками интерпретации различных математических и физических объектов. **Отлично** Знает методы сбора и анализа материала, интерпретации различных математических и физических объектов. Умеет осуществлять первичный сбор и анализ материала, обобщать полученную информацию. Владеет в полной мере навыками интерпретации различных математических и физических объектов.
ОПК.1.3 Использует практический опыт решения стандартных задач математических и (или) естественных наук	Знать стандартные задачи математических и (или) естественных наук. Уметь решать стандартные задачи математических и (или) естественных наук. Владеть практическим опытом решения стандартных задач математических и (или) естественных наук.	**Неудовлетворител** Не знает стандартные задачи математических и (или) естественных наук. Не умеет решать стандартные задачи математических и (или) естественных наук. Не владеет практическим опытом решения стандартных задач математических и (или) естественных наук. **Удовлетворительн** Знает стандартные задачи математических и (или) естественных наук. Умеет решать с ошибками стандартные задачи математических и (или) естественных наук. Не владеет практическим опытом решения стандартных задач математических и (или) естественных наук. **Хорошо** Знает стандартные задачи математических и (или) естественных наук.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Умеет решать без ошибок стандартные задачи математических и (или) естественных наук. Не владеет практическим опытом решения стандартных задач математических и (или) естественных наук. **Отлично** Знает стандартные задачи математических и (или) естественных наук. Умеет решать без ошибок стандартные задачи математических и (или) естественных наук. Владеет практическим опытом решения стандартных задач математических и (или) естественных наук.

ОПК.9

Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.9.1 Ориентируется в методах и средствах криптографической защиты информации	Знать основные методы и средства криптографической защиты информации. Уметь находить информацию о существующих методах и средствах криптографической защиты информации. Владеть навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации.	**Неудовлетворител** Не знает основные методы и средства криптографической защиты информации. Не умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Удовлетворительн** Знает основные методы и средства криптографической защиты информации. Умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Хорошо** Знает основные методы и средства

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо криптографической защиты информации. Умеет находить информацию о существующих методах и средствах криптографической защиты информации. Не владеет в полной мере навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации. **Отлично** Знает основные методы и средства криптографической защиты информации. Умеет находить информацию о существующих методах и средствах криптографической защиты информации. Владеет в полной мере навыками поиска, анализа и обобщения информации о существующих методах и средствах криптографической защиты информации.
ОПК.9.2 Анализирует возможности криптографических средств защиты информации	Знать существующие криптографические средства защиты информации. Уметь анализировать возможности криптографических средств защиты информации. Владеть навыками анализа при выборе криптографических средств защиты информации при решении практических заданий.	**Неудовлетворител** Не знает существующие криптографические средства защиты информации. Не умеет анализировать возможности криптографических средств защиты информации. Не владеет навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Удовлетворительн** Знает существующие криптографические средства защиты информации. Не умеет анализировать возможности криптографических средств защиты информации. Не владеет навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Хорошо** Знает существующие криптографические средства защиты информации. Умеет анализировать возможности криптографических средств защиты информации.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Не владеет в полной мере навыками анализа при выборе криптографических средств защиты информации при решении практических заданий. **Отлично** Знает существующие криптографические средства защиты информации. Умеет анализировать возможности криптографических средств защиты информации. Владеет в полной мере навыками анализа при выборе криптографических средств защиты информации при решении практических заданий.

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
ОПК.1.2 Осуществляет первичный сбор и анализ материала, интерпретирует различные математические и физические объекты **ОПК.1.1** Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук **ОПК.1.3** Использует практический опыт решения стандартных задач математических и (или) естественных наук **ОПК.9.1** Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Алгоритмы RSA и Эль-Гамаля, на основе теории групп **Письменное контрольное мероприятие**	контрольное мероприятие - тест

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.1.2 Осуществляет первичный сбор и анализ материала, интерпретирует различные математические и физические объекты **ОПК.1.1** Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук **ОПК.1.3** Использует практический опыт решения стандартных задач математических и (или) естественных наук **ОПК.9.1** Ориентируется в методах и средствах криптографической защиты информации **ОПК.9.2** Анализирует возможности криптографических средств защиты информации	Алгоритмы обмены ключами, шифрования и аутентикации на основе Эллиптических кривых **Письменное контрольное мероприятие**	контрольное мероприятие - тест

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.1.2 Осуществляет первичный сбор и анализ материала, интерпретирует различные математические и физические объекты **ОПК.1.1** Применяет базовые понятия, основную терминологию и знания основных положений и концепций в области математических и естественных наук **ОПК.1.3** Использует практический опыт решения стандартных задач математических и (или) естественных наук **ОПК.6.1** Ориентируется в методах и приемах научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей **ОПК.9.2** Анализирует возможности криптографических средств защиты информации **ОПК.9.1** Ориентируется в методах и средствах криптографической защиты информации	Зачет **Итоговое контрольное мероприятие**	контрольное мероприятие - тест

Спецификация мероприятий текущего контроля

Алгоритмы RSA и Эль-Гамаля, 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-Гамаля	

	10

Алгоритмы обмены ключами, шифрования и аутентикации 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 аутентикации 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