Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

Факультет физико-математических и естественных наук

Рекомендовано МССН
02.00.00 «Компьютерные и информационные науки»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины

Математические основы защиты информации и информационной безопасности

Рекомендуется для направления подготовки

02.04.02 – Фундаментальная информатика и информационные технологии

Направленность программы
Управление инфокоммуникациями и интеллектуальные системы

1. Цели и задачи дисциплины

Целью дисциплины является овладение современным математическим аппаратом реализации вычислительных методов в виде программ и навыками применения их в математическом моделировании.

2. Место дисциплины в структуре ОП ВО

Цикл, к которому относится дисциплина «Математические основы защиты информации и информационной безопасности»: Б1 «Дисциплины (модули)», обязательная часть.

В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП ВО.

Таблица № 1. Предшествующие и последующие дисциплины, направленные на формирование компетенций

Универсальные компетенции

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
УК-1, УК-2, УК-7	-	• Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) • Научно-исследовательская работа • Преддипломная практика • ВКР

Общепрофессиональные компетенции

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
ОПК-1, ОПК-2, ОПК-4	-	• Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) • Научно-исследовательская работа • Преддипломная практика • ВКР

Профессиональные компетенции

Тип задач профессиональной деятельности: научно-исследовательский

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
ПК-1.3	-	• Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) • Научно-исследовательская работа • Преддипломная практика • ВКР

Тип задач профессиональной деятельности: производственно-технологический

Шифр и наименование компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
ПК-2.5	-	Преддипломная практика, ВКР

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: УК-1, УК-2, УК-7, ОПК-1, ОПК-2, ОПК-4, ПК-1 (в части ПК-1.3), ПК-2 (в части ПК-2.5)

Расшифровка компетенций

- **УК-1** Способен осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
  - **УК-1.1** Знает принципы сбора, отбора и обобщения информации.
  - **УК-1.2** Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.
  - **УК-1.3** Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов.
- **УК-2** Способен управлять проектом на всех этапах его жизненного цикла.
  - **УК-2.1** Знает необходимые для осуществления профессиональной деятельности правовые нормы.
  - **УК-2.2** Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности.
  - **УК-2.2** Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.
- **УК-7** Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных
  - **УК-7.1** Знает принципы применения цифровых технологий для сбора, отбора и обобщения информации
  - **УК-7.2** Умеет применять цифровые технологии для поиска, обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий
  - **УК-7.3** Владеет навыками применения цифровых технологий и методов поиска, обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий
- **ОПК-1** Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.
  - **ОПК-1.1** Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций
  - **ОПК-1.2** Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты
  - **ОПК-1.3** Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности

- **ОПК-2** Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.
  - **ОПК-2.1** Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включённого в Единый Реестр Российских программ.
  - **ОПК-2.2** Умеет анализировать типовые языки программирования, составлять программы.
  - **ОПК-2.3** Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов коммуникации.
- **ОПК-4** Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.
  - **ОПК-4.1** Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла.
  - **ОПК-4.2** Умеет осуществлять управление проектами информационных систем.
  - **ОПК-4.3** Имеет практический опыт анализа и интерпретации информационных систем.
- **ПК-1** Проведение работ по обработке и анализу научно-технической информации и результатов исследований.
  - **ПК-1.3** Умеет применять полученные знания в области фундаментальных научных основ математики и информатики, а также решать стандартные задачи собственной научно-исследовательской деятельности; умеет решать научные задачи с пониманием существующих подходов к верификации моделей по тематике исследований в соответствии с выбранной методикой. научных семинаров, научно-технических конференций.
- **ПК-2** Организационное и технологическое обеспечение проектирования и дизайна ИС.
  - **ПК-2.5** Знает основы программирования; современные методики тестирования разрабатываемых информационных систем; современные инструменты и методы верификации программного кода.

В результате изучения дисциплины студент должен:

Знать:
- основные криптографические алгоритмы;
- основные криптографические протоколы;
- области применения криптографических методов при защите информационных систем.

Уметь:
- решать криптографические задачи прикладного характера;
- применять разные криптографические алгоритмы к прикладным задачам;
- использовать разные средства поддержания процесса разработки программного обеспечения.

Владеть:
- навыками использования криптографических программ;
- навыками написания криптографических программ;
- навыками поддержки процесса разработки программного обеспечения.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетных единиц.

Вид учебной работы	Всего часов	Семестр 1, модуль 2
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия (ПЗ)		
Семинары (С)		
Лабораторные работы (ЛР)	36	36
Самостоятельная работа (всего)	135	162
Общая трудоемкость	216	216
Зачётных единиц	6	6

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

№	Наименование раздела дисциплины	Содержание раздела
1	Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем	• Основы безопасности сетевых информационных технологий.
2	Шифрование	• Симметричная криптография. • Асимметричная криптография.
3	Алгоритмы обмена ключей и протоколы аутентификации	• Хэш-функции и аутентификация сообщений. Цифровая подпись • Алгоритм обмена ключами Диффи–Хеллмана

5.2. Разделы дисциплин и виды занятий

№	Наименование раздела дисциплины	Лекц	Практ. зан.	Лаб. зан.	Сем.	СРС	Всего час.
1	Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем	6		12		54	72
2	Шифрование	6		12		54	72
3	Алгоритмы обмена ключей и протоколы аутентификации	6		12		54	72
	Всего часов	18		36		162	216

6. Лабораторный практикум

№ раздела дисциплины	Наименование лабораторных работ	Трудоём-кость (час.)
1	Простые шифры	8
2	Основы блочного шифрования	8
2	Асимметричная криптография и цифровая подпись	6
3	Алгоритма обмена ключами Диффи-Хеллмана	8
3	Алгоритмы электронной цифровой подписи	6
	Всего часов	36

7. Практические занятия (семинары)

Не предусмотрены.

8. Материально-техническое обеспечение дисциплины

Мультимедийная учебная аудитория для проведения учебных занятий (в том числе для лекционного типа занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации).

Компьютерные (дисплейные) классы с доступом к сети Интернет и электронно-образовательной среде Университета для выполнения обучающимися лабораторных работ по дисциплине, для проведения обучающимися самостоятельной работы и компьютерного тестирования обучающихся (при необходимости).

9. Информационное обеспечение дисциплины

Программное обеспечение:

- ОС Linux.
- Офисный пакет LibreOffice (лицензия MPL-2.0).
- ПО для просмотра формата pdf (например, `evince` (лицензия GPL-2+ CC-BY-SA-3.0)).
- GNU Midnight Commander (лицензия GNU GPL 3).
- Julia (лицензия MIT).
- Jupyter (лицензия BSD).
- gcc (лицензия GNU GPL 3).

Базы данных, информационно-справочные и поисковые системы:

- Сайт библиотеки РУДН http://lib.rudn.ru/.
- Сайт ТУИС http://esystem.rudn.ru/.

10. Учебно-методическое обеспечение дисциплины

а) Основная литература

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2020. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450277.
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469567.

б) Дополнительная литература

1. Информационная безопасность компьютерных сетей: учебно-методический комплекс / Д.С. Кулябов, А. В. Королькова, М. Н. Геворкян. — Москва: РУДН, 2015. — 64 с.
2. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. — Издательство: Горячая линия — Телеком , 2011 г.
3. Лапонина О.Р. «Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие», 3-е изд. испр., М. ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», БИНОМ. Лаборатория знаний, 2012г., 531с. — URL: http://www.intuit.ru/department/security/networksec/.
4. В. Столлингс «Криптография и защита сетей. Принципы и практика», 2-е изд. 2001г., Издательский дом «Вильямс», 672 с.
5. Б. Шнайер «Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С», 2-е изд. 2003г.
6. М. А. Иванов «Криптографические методы защиты информации в компьютерных системах и сетях», 2001г., «Кудиц-образ», 386с.

11. Методические указания для обучающихся по освоению дисциплины

Учебным планом на изучение дисциплины отводится один модуль. В дисциплине предусмотрены контактные часы в виде лекций, лабораторного практикума. В течение модуля выполняются лабораторные работы, подготовка и презентация доклада, подготовка и презентация группового проекта, подготовка и презентация индивидуального проекта, контрольные мероприятия.

11.1 Методические указания по самостоятельному освоению теоретического материала по дисциплине

Лекционный материал дисциплины охватывает темы, указанные в разделе 5.1 программы дисциплины. В ТУИС (http://esystem.rudn.ru) по темам лекций размещены презентации. Рекомендуется по указанным темам в дополнение к презентациям изучить литературу, указанную в п. 10 программы дисциплины и учебно-методические материалы в ТУИС (http://esystem.pfur.ru).

11.2 Методические указания по выполнению лабораторных работ

- Задания по лабораторным работам выполняются индивидуально каждым студентом в соответствии с календарным планом и методическими указаниями по выполнению лабораторных работ по дисциплине.
- Часть лабораторных работ предусматривает задания для индивидуальной самостоятельной работы студента, обязательные для выполнения.
- Выполнение заданий для самостоятельной работы позволяет студенту приобрести дополнительные навыки и закрепить знания по изучаемой теме.
- По результатам выполнения каждой лабораторной работы студентом готовится отчёт. Отчёты в электронном виде сдаются студентом на проверку через соответствующие разделы ТУИС (http://esystem.pfur.ru).
- Срок сдачи указан для каждой лабораторной работы. В случае сдачи лабораторной не в срок, то ставится не более 51% от максимального балла.

11.3. Рекомендации по подготовке доклада

Доклад – это публичное развёрнутое изложение по заданной теме.

Целями подготовки доклада являются: - внесение знаний из дополнительной литературы; - систематизация материла по теме; - развитие навыков самостоятельной работы с литературой; - пробуждение познавательного интереса к научному познанию.

Основными задачами подготовки доклада являются: - выработка умений излагать содержание материала в короткое время; - выработка умений ориентироваться в материа-

ле и отвечать на вопросы; - выработка умений самостоятельно обобщать и представлять материал, делать выводы.

Доклад должен состоять из трех частей: вступление, основная часть и заключение.

Вступление должно содержать: название доклада, сообщение основной идеи, современную оценку предмета изложения, краткое перечисление рассматриваемых вопросов, форму изложения.

Основная часть должна раскрывать суть затронутой темы. Задача основной части - представить достаточно данных для того, чтобы слушатели заинтересовались темой и захотели ознакомиться с материалами. При этом логическая структура основного блока должна содержать наглядные материалы, аудио-визуальные или визуальные материалы (представление рисунков, таблиц графиков в формате `pdf`).

Заключение должно содержать ясное чёткое обобщение и краткие выводы.

Время доклада – 5–7 мин. Чтение доклада при выступлении запрещено.

11.4. Рекомендации по подготовке презентации доклада

Презентация представляет собой последовательность сменяющих друг друга слайдов. Количество слайдов пропорционально содержанию и продолжительности выступления. На первом слайде обязательно представляется тема выступления и сведения об авторе. На слайды помещается фактический и иллюстративный материал (таблицы, графики, фотографии и пр.), который является уместным и достаточным средством наглядности, помогает в раскрытии стержневой идеи доклада.

В этом случае к слайдам предъявляются следующие требования: - выбранные средства визуализации информации (таблицы, схемы, графики и т.д.) соответствуют содержанию; - использованы иллюстрации хорошего качества (высокого разрешения), с четким изображением, максимальное количество графической информации на одном слайде – 2 рисунка (графики, схемы и т.д.) с текстовыми комментариями (не более 2 строк к каждому).

Наиболее важная информация должна располагаться в центре экрана. Обычный слайд, без эффектов анимации, должен демонстрироваться на экране не менее 10–15 секунд. Слайд с анимациями в среднем должен находиться на экране не меньше 40–60 секунд (без учета времени на случайно возникшее обсуждение). Для всех слайдов презентации необходимо использовать один и тот же шаблон оформления, кегль – для заголовков – не меньше 24 пунктов, для информации – для информации не менее 18. Наилучшей цветовой гаммой для презентации являются контрастные цвета фона и текста (белый фон – чёрный текст; темно-синий фон – светло-желтый текст и т.д.). Рекомендуется не злоупотреблять прописными буквами и не смешивать разные типы шрифтов в одной презентации.

12. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ФОС по дисциплине представлен в приложении к данной программе.

Программа составлена в соответствии с требованиями ОС ВО РУДН.

Разработчик:

профессор кафедры
прикладной информатики
и теории вероятностей, д.ф.-м.н., доцент Д.С. Кулябов

Руководитель программы
заведующий кафедрой
прикладной информатики
и теории вероятностей, д.т.н., проф. К.Е. Самуйлов

Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

Факультет физико-математических и естественных наук

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Наименование дисциплины

Математические основы защиты информации и информационной безопасности

Рекомендуется для направления подготовки

02.04.02 – Фундаментальная информатика и информационные технологии

Направленность программы
Управление инфокоммуникациями и интеллектуальные системы

Паспорт фонда оценочных средств по дисциплине

Дисциплина: Математические основы защиты информации и информационной безопасности

Направление: 02.04.02 – Фундаментальная информатика и информационные технологии

профиль: Управление инфокоммуникациями и интеллектуальные системы

Код контролируемой компетенции или её части	Контролируемый раздел дисциплины	Контролируемая тема дисциплины	А1.1	А1.2	А2	А3	Баллы темы	Баллы раздела
УК-1, УК-2, УК-7, ОПК-1, ОПК-4, ПК-1 (в части ПК-1.3), ПК-2 (в части ПК-2.5)	Р1	Основные понятия информационной безопасности	6	2	2	2	12	24
УК-1, УК-2, УК-7, ОПК-1, ОПК-4, ПК-1 (в части ПК-1.3), ПК-2 (в части ПК-2.5)	Р1	Элементы теории информации и кодирования	6	2	2	2	12	
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р2	Математические основы криптографии	6	2	2	2	12	40
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р2	Симметричная криптография	6	2	2	4	14	
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р2	Асимметричная криптография	6	2	2	4	14	
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р3	Хэш-функции и аутентификация сообщений. Цифровая подпись	6	2	2	2	12	36
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р3	Алгоритм обмена ключами Диффи–Хеллмана	6	2	2	2	12	
УК-2, УК-7, ОПК-1, ОПК-2, ПК-1 (в части ПК-1.3)	Р3	Основные принципы построения защищённых систем	6	2	2	2	12	
		Итого:	48	16	16	20	100	100

Разделы:

- Р1: Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем.
- Р2: Шифрование.
- Р3: Алгоритмы обмена ключей и протоколы аутентификации.

Формы контроля уровня освоения ООП:

- А1.1: Лабораторные работы. Выполнение.
- А1.2: Лабораторные работы. Самопроверка и взаимопроверка.
- А2: Доклады по темам.
- А3: Итоговое тестирование.

Процесс изучения дисциплины направлен на формирование следующих компетенций: УК-1, УК-2, УК-7, ОПК-1, ОПК-2, ОПК-4, ПК-1 (в части ПК-1.3), ПК-2 (в части ПК-2.5)

Расшифровка компетенций

- **УК-1** Способен осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
  - **УК-1.1** Знает принципы сбора, отбора и обобщения информации.
  - **УК-1.2** Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности.
  - **УК-1.3** Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов.
- **УК-2** Способен управлять проектом на всех этапах его жизненного цикла.
  - **УК-2.1** Знает необходимые для осуществления профессиональной деятельности правовые нормы.
  - **УК-2.2** Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности.
  - **УК-2.2** Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.
- **УК-7** Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных
  - **УК-7.1** Знает принципы применения цифровых технологий для сбора, отбора и обобщения информации
  - **УК-7.2** Умеет применять цифровые технологии для поиска, обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий
  - **УК-7.3** Владеет навыками применения цифровых технологий и методов поиска, обработки, анализа, хранения и представления информации в области фундаментальной информатики и информационных технологий
- **ОПК-1** Способен находить, формулировать и решать актуальные проблемы прикладной математики, фундаментальной информатики и информационных технологий.
  - **ОПК-1.1** Обладает фундаментальными знаниями в области математических и естественных наук, теории коммуникаций
  - **ОПК-1.2** Умеет осуществлять первичный сбор и анализ материала, интерпретировать различные математические объекты

  - **ОПК-1.3** Имеет практический опыт работы с решением математических задач и применяет его в профессиональной деятельности
- **ОПК-2** Способен применять компьютерные/суперкомпьютерные методы, современное программное обеспечение (в том числе отечественного производства) для решения задач профессиональной деятельности.
  - **ОПК-2.1** Знает основные положения и концепции в области программирования, архитектуру языков программирования, теории коммуникации, знает основную терминологию, знаком с перечнем ПО, включённого в Единый Реестр Российских программ.
  - **ОПК-2.2** Умеет анализировать типовые языки программирования, составлять программы.
  - **ОПК-2.3** Имеет практический опыт решения задач анализа, интеграции различных типов программного обеспечения, анализа типов коммуникации.
- **ОПК-4** Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.
  - **ОПК-4.1** Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла.
  - **ОПК-4.2** Умеет осуществлять управление проектами информационных систем.
  - **ОПК-4.3** Имеет практический опыт анализа и интерпретации информационных систем.
- **ПК-1** Проведение работ по обработке и анализу научно-технической информации и результатов исследований.
  - **ПК-1.3** Умеет применять полученные знания в области фундаментальных научных основ математики и информатики, а также решать стандартные задачи собственной научно-исследовательской деятельности; умеет решать научные задачи с пониманием существующих подходов к верификации моделей по тематике исследований в соответствии с выбранной методикой. научных семинаров, научно-технических конференций.
- **ПК-2** Организационное и технологическое обеспечение проектирования и дизайна ИС.
  - **ПК-2.5** Знает основы программирования; современные методики тестирования разрабатываемых информационных систем; современные инструменты и методы верификации программного кода.

Балльно-рейтинговая система оценки уровня знаний

Сводная оценочная таблица дисциплины

Раздел	Тема	A1.1	A1.2	A2	A3	Баллы темы	Баллы раздела
P1	Основные понятия информационной безопасности	6	2	2	2	12	24
P1	Элементы теории информации и кодирования	6	2	2	2	12	
P2	Математические основы криптографии	6	2	2	2	12	40
P2	Симметричная криптография	6	2	2	4	14	
P2	Асимметричная криптография	6	2	2	4	14	
P3	Хэш-функции и аутентификация сообщений. Цифровая подпись	6	2	2	2	12	36
P3	Алгоритм обмена ключами Диффи–Хеллмана	6	2	2	2	12	
P3	Основные принципы построения защищённых систем	6	2	2	2	12	
	Итого:	48	16	16	20	100	100

Разделы:

- P1: Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем.
- P2: Основы криптографии.
- P3: Алгоритмы обмена ключей и протоколы аутентификации.

Активности:

- A1.1: Лабораторные работы. Выполнение.
- A1.2: Лабораторные работы. Самопроверка и взаимопроверка.
- A2: Доклады по темам.
- A3: Итоговое тестирование.

Таблица соответствия баллов и оценок

Баллы БРС	Традиционные оценки в РФ	Баллы для перевода оценок	Оценки	Оценки ECTS
86–100	5	95–100	5+	A
		86–94	5	B

69–85	4	69–85	4	C
51–68	3	61–68	3+	D
		51–60	3	E
0–50	2	31–50	2+	FX
		0–30	2	F

Правила применения БРС

1. Раздел (тема) учебной дисциплины считаются освоенными, если студент набрал более 50% от возможного числа баллов по этому разделу (теме).
2. Студент не может быть аттестован по дисциплине, если он не освоил все темы и разделы дисциплины, указанные в сводной оценочной таблице дисциплины.
3. По решению преподавателя и с согласия студентов, не освоивших отдельные разделы (темы) изучаемой дисциплины, в течение учебного семестра могут быть повторно проведены мероприятия текущего контроля успеваемости или выданы дополнительные учебные задания по этим темам или разделам. При этом студентам за данную работу засчитывается минимально возможный положительный балл (51% от максимального балла).
4. При выполнении студентом дополнительных учебных заданий или повторного прохождения мероприятий текущего контроля полученные им баллы засчитываются за конкретные темы. Итоговая сумма баллов не может превышать максимального количества баллов, установленного по данным темам.
5. График проведения мероприятий текущего контроля успеваемости формируется в соответствии с календарным планом курса. Студенты обязаны сдавать все задания в сроки, установленные преподавателем.
6. Время, которое отводится студенту на выполнение мероприятий текущего контроля успеваемости, устанавливается преподавателем. По завершении отведённого времени студент обязан сдать работу преподавателю, вне зависимости от того, завершена она или нет.
7. Использование источников (в том числе конспектов лекций и лабораторных работ) во время выполнения контрольных мероприятий возможно только с разрешения преподавателя.
8. Отсрочка в прохождении мероприятий текущего контроля успеваемости считается уважительной только в случае болезни студента, что подтверждается наличием у него медицинской справки, заверенной круглой печатью КДЦ РУДН, предоставляемой преподавателю не позднее двух недель после выздоровления. В этом случае выполнение контрольных мероприятий осуществляется после выздоровления студента в срок, назначенный преподавателем. В противном случае отсутствие студента на контрольном мероприятии признается неуважительным.
9. Если в итоге за семестр студент получил 0–50 баллов, то студенту разрешается добор необходимого (до 51) количества баллов путём повторного одноразового выполнения предусмотренных контрольных мероприятий, при этом по усмотрению преподавателя аннулируются соответствующие предыдущие результаты. Ликвидация задолженностей проводится в сроки, согласованные с деканатом.
10. Баллы за доклады по темам фиксируются только после доклада во время контактных часов.

Примерный перечень оценочных средств

по дисциплине Математические основы защиты информации и информационной безопасности

Аудиторная работа

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Лабораторная работа	Система практических заданий, направленных на формирование практических навыков у обучающихся	Фонд практических заданий
Презентация (защита) доклада	Средство контроля способностей обучающихся представить перед аудиторией результаты проделанной работы	Темы докладов

Самостоятельная работа

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Подготовка отчетов по результатам выполнения лабораторных работ	Форма проверки качества выполнения студентами лабораторных работ в соответствии с утвержденной программой	Фонд практических заданий
Доклад	Продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы	Темы докладов

Учебным планом на изучение дисциплины отводится один модуль. В дисциплине предусмотрен контактные часы в форме лабораторного практикума, контрольные мероприятия по проверке отчётов по лабораторным работам, подготовка и презентация доклада, подготовка и презентация группового проекта, подготовка и презентация индивидуального проекта. Оценка ставится по результатам работы в семестре.

Оценивание результатов освоения дисциплины производится в соответствии с больно-рейтинговой системой.

Критерии оценки по дисциплине

95–100 баллов:

- полное и своевременное выполнение на высоком уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы, умение делать обоснованные выводы;
- безупречное владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- выраженная способность самостоятельно и творчески решать поставленные задачи;
- полная самостоятельность и творческий подход при изложении материала по программе дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной программой дисциплины и преподавателем.

86–94 балла:

- полное и своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- хорошее владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать поставленные задачи в нестандартных производственных ситуациях;
- усвоение основной и дополнительной литературы, нормативных и законодательных актов, рекомендованных программой дисциплины и преподавателем.

69–85 баллов:

- своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- хороший уровень культуры исполнения лабораторных работ;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать проблемы в рамках программы дисциплины;
- усвоение основной литературы;

51–68 баллов:

- выполнение на удовлетворительном уровне лабораторных работ с оформлением отчетов, прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;

- удовлетворительное владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

31–50 баллов – НЕ ЗАЧТЕНО:

- не выполнение, несвоевременное выполнение или выполнение на неудовлетворительном уровне лабораторных работ, не прохождение контрольных мероприятий, предусмотренных программой курса;
- недостаточно полный объем навыков и компетенции в рамках программы дисциплины;
- неумение использовать в практической деятельности научной терминологии, изложение ответа на вопросы с существенными стилистическими и логическими ошибками;
- слабое владение программным обеспечением по разделам программы дисциплины, некомпетентность в решении стандартных (типовых) производственных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

0–30 баллов – НЕ ЗАЧТЕНО:

- отсутствие умений, навыков, знаний и компетенции в рамках программы дисциплины;
- невыполнение лабораторных заданий, не прохождение контрольных мероприятий, предусмотренных программой курса; отказ от ответов по программе дисциплины;
- игнорирование занятий по дисциплине по неуважительной причине.

Темы докладов

- Системы идентификации по индивидуальным характеристикам человека. (Биометрическая идентификация: по физиологическим параметрам и характеристикам, по особенностям поведения человека).
- Стеганография. Принципы и алгоритмы.
- Электронные деньги.
- Смарт-карты.
- Протоколы SSL (Secure Socket Layer) и TLS (Transport Layer Security).
- Шифропанки.
- Аппаратное шифрование.
- Криптография на эллиптических кривых.
- Защита данных в СУБД.
- Защита телефонных разговоров (PGPfone).
- Устройства Touch-memory.
- Линейный и дифференциальный криптоанализ.
- «Шаг младенца, шаг великана» - метод для вычисления обратной функции (методы взлома, основанные на дискретном логарифмировании).
- Одноключевая криптография. Поточные и блоковые (блочные) шифры.
- Абсолютно надёжные шифры. Схема Фейстеля. Режимы шифрования. Принцип Керкхоффа.
- Односторонние функции. Односторонние функции с секретом (с ловушкой). Цифровая (электронная) подпись, использующая одностороннюю функцию. Примеры (гипотетические) односторонних функций.
- Криптографические хэш-функции. Основные требования к криптографическим хэш-функциям.
- Протокол Диффи-Хеллмана для обмена ключами по открытому каналу связи. Аналог, использующий группу общего вида.
- Криптосистема RSA. Шифрование и цифровая подпись. Обоснование правильности дешифрования. Обоснование подписи.
- Криптосистема Эль-Гамаля. Шифрование и цифровая подпись. Обоснование подписи. Аналог криптосистемы Эль-Гамаля, использующий группу общего вида.
- Цифровая подпись DSA (DSS). Обоснование подписи. Аналог, использующий группу общего вида.

Фонд практических (лабораторных) заданий

по дисциплине Математические основы защиты информации и информационной безопасности

Предлагаются к выполнению 8 лабораторных работ. Отчёты по лабораторным работам выполняются студентом самостоятельно, на лабораторном занятии студент может получить консультацию и методические указания от преподавателя.

Лабораторная работа № 1. Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка стойкости парольной защиты.

Аутентификация и шифрование.

Лабораторная работа № 2. Криптоанализ шифра однобуквенной простой замены. Оценка частотности символов в тексте.

Основные подходы к криптографии.

Лабораторная работа № 3. Криптоанализ шифра «Решетка Кардано».

Основные подходы к криптоанализу.

Лабораторная работа № 4. Симметричные и асимметричные криптосистемы. Электронно-цифровая подпись. Программный комплекс PGP.

Симметричные и ассиметриные криптосистемы. Цифровая подпись.

Лабораторная работа № 5. Симметричные системы шифрования. DES.

Блочные симметричные криптосистемы.

Лабораторная работа № 6. Схема открытого распределения ключей.

Распределение ключей. Инфраструктура ключей.

Лабораторная работа № 7. Аутентификация пользователей веб-систем.

Разработка безопасных web-приложений.

Лабораторная работа № 8. Управление пользователями и их правами доступа в ОС Linux.

Система безопасности ОС Linux.

Методические указания и шкала оценок

Порядок выполнения лабораторной работы заключается в следующем:

- Ознакомиться с разделами методических указаний к данной лабораторной работе.
- Выполнить задания лабораторной работы.
- Составить отчёт.

Отчёт должен содержать следующие разделы:

- титульный лист;
- формулировку цели работы;
- описание результатов выполнения задания: – снимки экрана (скриншоты) с результатами выполнения команд; – результаты выполнения программ (текст или снимок экрана в зависимости от задания);
- выводы, согласованные с целью работы.

Критерии оценки

Оценивается полнота выполнения работы, оформление результатов, полнота ответов на контрольные вопросы, если это предусмотрено заданием.