

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 29.05.2023 12:16:05
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989dae18a

Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»
Факультет физико-математических и естественных наук

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математические основы защиты информации и информационной безопасности

Рекомендована МССН для направления подготовки:

01.04.02 – Прикладная математика и информатика

Освоение дисциплины ведётся в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

Теория вероятностей и математическая статистика

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Математические основы защиты информации и информационной безопасности» является овладение математическим аппаратом современной криптографии и информационной безопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Математические основы защиты информации и информационной безопасности» направлено на формирование у обучающихся следующих компетенций (части компетенций): УК-1, УК-2, УК-7, ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1 (в части ПК-1.3)

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
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 к использованию цифровых технологий и методов поиска, обработки, анализа, хранения и представле-	УК-7.1 Знает принципы применения цифровых технологий для сбора, отбора и обобщения информации. УК-7.2 Умеет применять цифровые технологии для поиска, отработки, анализа,

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	ния информации в области прикладной математики и информатики в условиях цифровой экономики и современной корпоративной информационной культуры.	хранения и представления информации в области прикладной математики и информатики. УК-7.3 Владеет навыками применения цифровых технологий и методов поиска, обработки, анализа, хранения и представления информации в области прикладной математики и информатики.
ОПК-1	Способен решать актуальные задачи фундаментальной и прикладной математики.	ОПК-1.1 Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук. ОПК-1.2 Умеет использовать фундаментальные знания, полученные в области математических и (или) естественных наук, в профессиональной деятельности. ОПК-1.3 Владеет навыками осуществлять выбор методов решения задач профессиональной деятельности на основе теоретических знаний.
ОПК-2	Способен совершенствовать и реализовывать новые математические методы решения прикладных задач.	ОПК-2.1 Способен совершенствовать и (или) разрабатывать новые математические методы для разработки и реализации алгоритмов решения задач (в том числе с использованием программных средств) в области профессиональной деятельности.
ОПК-3	Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности.	ОПК-3.1 Способен модифицировать и (или) разрабатывать, анализировать и реализовывать математические модели в современном естествознании, технике, экономике и управлении.
ОПК-4	Способен комбинировать и адаптировать 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 по проводимым исследованиям. ОПК-4.2 Умеет комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.
ПК-1	Проведение работ по обработке и анализу научно-технической ин-	ПК-1.3 Умеет применять полученные знания в области прикладной математики и информатики, а также решать стан-

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	формации и результатов исследований.	дартные задачи собственной научно-исследовательской деятельности; умеет решать научные задачи с пониманием существующих подходов к верификации моделей по тематике исследований в соответствии с выбранной методикой.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Математические основы защиты информации и информационной безопасности» относится к обязательной части блока Б1 ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Математические основы защиты информации и информационной безопасности».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики	Последующие дисциплины/модули, практики
УК-1	Способен осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	-	Преддипломная практика
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	-	Преддипломная практика
УК-7	Способен к использованию цифровых технологий и методов поиска, обработки, анализа, хранения и представления информации в области прикладной математики и информатики в условиях цифровой экономики и современной корпоративной информационной культуры	-	Преддипломная практика
ОПК-1	Способен решать актуальные задачи фундаментальной и прикладной математики	-	Преддипломная практика

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики	Последующие дисциплины/модули, практики
ОПК-2	Способен совершенствовать и реализовывать новые математические методы решения прикладных задач	-	Преддипломная практика
ОПК-3	Способен разрабатывать математические модели и проводить их анализ при решении задач в области профессиональной деятельности	-	Преддипломная практика
ОПК-4	Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	-	Преддипломная практика
ПК-1	Проведение работ по обработке и анализу научно-технической информации и результатов исследований	-	Преддипломная практика

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины Математические основы защиты информации и информационной безопасности составляет 6 зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы	ВСЕГО, ак.ч.	Семестр(-ы)
		1
<i>Контактная работа, ак.ч.</i>	54	54
в том числе:		
Лекции (ЛК)	18	18
Лабораторные работы (ЛР)	36	36
Практические/семинарские занятия (СЗ)		
<i>Самостоятельная работа обучающихся, ак.ч.</i>	135	135
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	27	27
Общая трудоемкость дисциплины	ак.ч.	216
	зач.ед.	6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы ¹
Раздел 1 Анализ и классификация нормативно-методической базы в области защиты информации. Модели безопасности операционных систем	Тема 1.1 Основные понятия информационной безопасности. Тема 1.2 Модульная арифметика.	ЛК, ЛР
Раздел 2 Основы криптографии.	Тема 2.1. Современные шифры с симметричным ключом. Тема 2.2 Стандарт шифрования данных (DES). Тема 2.3 Криптография с асимметричным ключом.	ЛК, ЛР
Раздел 3 Алгоритмы обмена ключей и протоколы аутентификации.	Тема 3.1 Целостность сообщения и установление подлинности сообщения. Тема 3.2 Установление подлинности объекта. Тема 3.3. Управление ключами.	ЛК, ЛР

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персо-	<ul style="list-style-type: none"> • ОС Linux/ Windows, Python, Julia. • Дополнительное ПО: офисный пакет MS

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
	нальными компьютерами (в количестве 18 шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Office или LibreOffice, OBS Studio
Для самостоятельной работы обучающихся	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	<ul style="list-style-type: none"> • ОС Linux/ Windows, Python, Julia. • Дополнительное ПО: офисный пакет MS Office или LibreOffice, OBS Studio

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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>.

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. ИНТУ-ИТ.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.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

- ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:
 - Электронно-библиотечная система РУДН – ЭБС РУДН <http://lib.rudn.ru/MegaPro/Web>
 - ЭБС «Университетская библиотека онлайн» <http://www.biblioclub.ru>
 - ЭБС Юрайт <http://www.biblio-online.ru>
 - ЭБС «Консультант студента» <http://www.studentlibrary.ru>
 - ЭБС «Лань» <http://e.lanbook.com/>
 - ЭБС «Троицкий мост»
- Базы данных и поисковые системы:
 - электронный фонд правовой и нормативно-технической документации <http://docs.cntd.ru/>
 - поисковая система Яндекс <https://www.yandex.ru/>
 - поисковая система Google <https://www.google.ru/>
 - реферативная база данных SCOPUS <http://www.elsevierscience.ru/products/scopus/>

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:

- Курс видеолекций по дисциплине «Математические основы защиты информации и информационной безопасности».
- Лабораторный практикум по дисциплине «Математические основы защиты информации и информационной безопасности».

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Математические основы защиты информации и информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Профессор кафедры прикладной информатики и теории вероятностей

Должность, БУП



Подпись

Д.С. Кулябов

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной
информатики и теории вероятностей

Наименование БУП



Подпись

К.Е. Самуйлов

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Профессор кафедры прикладной
информатики и теории вероятностей

Должность, БУП



Подпись

Л.А. Севастьянов

Фамилия И.О.