

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»

Радиофизический факультет

(факультет / институт / филиал)

УТВЕРЖДЕНО

решением ученого совета ННГУ

протокол от

«31» мая 2023 г. № 6

Рабочая программа дисциплины

Основы прикладной криптографии

(наименование дисциплины (модуля))

Уровень высшего образования

магистратура

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

02.04.02 Фундаментальная информатика и информационные технологии

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Информационная безопасность и защита информации

(указывается профиль / магистерская программа / специализация)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2023

1. Место дисциплины в структуре ООП

Дисциплина «Основы прикладной криптографии» относится к дисциплинам части, формируемой участниками образовательных отношений, основной образовательной программы по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

№ варианта	Место дисциплины в учебном плане образовательной программы	Стандартный текст для автоматического заполнения в конструкторе РПД
2	Блок 1. Дисциплины (модули) Часть, формируемая участниками образовательных отношений	Дисциплина Б1.В.01 «Основы прикладной криптографии» относится к части ООП направления подготовки 02.04.02 «Фундаментальная информатика и информационные технологии», формируемой участниками образовательных отношений.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
УК-2. Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Знает структуру жизненного цикла проекта	Знать: - основные требования, предъявляемые к современным алгоритмам шифрования - основные системы шифрования с открытыми ключами - характеристики электронной подписи, основные требования, предъявляемые к криптографическим функциям	Собеседование
	УК-2.2. Умеет адаптировать жизненный цикл под специфику конкретных проектов	Уметь: - применять основные криптографические средства и системы информационной безопасности	Собеседование
ПК-1. Способен руководить научными исследованиями и опытно-конструкторскими	ПК-1.1. Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области	Знать: - методы научных исследований основных характеристик шифров	Собеседование

разработками, в области фундаментальной информатики и информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	ФИИТ применительно к профессиональной деятельности		
	ПК-1.2. Умеет выполнять научные исследования и опытно-конструкторские разработки в области ФИИТ применительно к профессиональной деятельности.	Уметь: - рассчитывать сложность типовых криптографических алгоритмов	Собеседование

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения	заочная форма обучения
Общая трудоемкость	4 ЗЕТ	___ ЗЕТ	___ ЗЕТ
Часов по учебному плану	144		
в том числе			
аудиторные занятия (контактная работа): - занятия лекционного типа - занятия семинарского типа (практические занятия / лабораторные работы)	32		
самостоятельная работа	65		
КСР	2		
Промежуточная аттестация – экзамен/зачет	экзамен 45		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины, форма промежуточной аттестации по дисциплине	Всего (часы)	В том числе				
		Контактная работа (работа во взаимодействии с преподавателем), часы из них				Самостоятельная работа обучающегося, часы
		Занятия лекционного типа	Занятия семинарского типа	Занятия лабораторного типа	Всего	
1. Основы теории Шеннона. Надежность шифров.	12	4			4	8
2. Системы симметричного шифрования.	22	8			8	14
3. Системы асимметричного шифрования.	20	6			6	14
4. Открытое распространение ключей. Хеш-функция. Электронная цифровая подпись.	20	6			6	14
5. Криптографические методы защиты информации в телекоммуникационных сетях.	23	8			8	15
Итого:	97	32			32	65

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает следующие виды:

- изучение дополнительных разделов дисциплины с использованием учебной литературы;
- изучение и проверка компьютерных настроек и интерфейсов на персональных компьютерах обучающихся.

Текущий контроль усвоения материала проводится путем проведения опроса.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю),

включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	Шкала оценивания сформированности компетенций						
	плохо	неудовлетворительно	удовлетворительно	хорошо	очень хорошо	отлично	превосходно
<u>Знания</u>	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибок.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.
<u>Умения</u>	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продemonстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме.	Продemonстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продemonстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
<u>Навыки</u>	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продemonстрированы базовые навыки при решении стандартных задач без недочетов.	Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продemonстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка	Уровень подготовки
превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
отлично	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне «очень хорошо»
хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно»
неудовлетворительно	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1. Контрольные вопросы

Вопросы	Код формируемой компетенции
1. Теоретическая и практическая стойкость криптосистем.	УК-2
2. Стойкость шифров. Правило Керкхоффа.	УК-2
3. Теорема Шеннона о совершенной секретности.	УК-2
4. Математические основы криптографии. Ненадежность шифров и расстояние единственности.	УК-2
5. Понятие блочного и поточного шифра.	УК-2
6. Алгоритмы шифрования на основе сетей Фейстеля.	УК-2
7. Режимы работы блочных шифров. Комбинирование блочных шифров.	УК-2, ПК-1
8. Стандарт шифрования данных DES. Основные характеристики.	ПК-1
9. Российские стандарты шифрования ГОСТ 28147-89, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Основные характеристики.	ПК-1
10. Стандарт шифрования AES. Основные характеристики.	ПК-1
11. Поточковый шифр A5/1. Основные характеристики.	ПК-1
12. Поточковый шифр RC4. Основные характеристики.	ПК-1
13. Криптография с открытыми ключами. Односторонние	УК-2

функции. Алгоритмы шифрования и цифровой подписи.	
14. Алгоритм Диффи-Хеллмана обмена ключевой информацией.	УК-2, ПК-1
15. Криптосистема RSA.	ПК-1
16. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.	УК-2, ПК-1
17. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования.	УК-2
18. Электронная цифровая подпись. Свойства электронной цифровой подписи.	УК-2
19. Алгоритм хеширования SHA.	ПК-1
20. Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты.	ПК-1
21. Системы электронной безопасности в финансовой сфере. Статическая и динамическая аутентификация данных на картах.	ПК-1
22. Теоретическая и практическая стойкость криптосистем.	ПК-1
23. Стойкость шифров. Правило Керкхоффа.	ПК-1

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Васильева И.Н. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2017. – 349 с.
2. Запечников С.В., Казарин О.В., Тарасов А.А. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2017. – 309 с.
3. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. – М.: Издательство Юрайт, 2017. – 473 с.

б) дополнительная литература:

1. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование. – М.: Издательство Юрайт, 2017. – 220 с.
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. – М.: Лань, 2011. – 400 с.
3. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: БИНОМ, 2007. – 608 с.
4. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 1. Математические аспекты. – М.: Издательство Юрайт, 2017. – 209 с.
5. Фомичев В.М., Мельников Д.А. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты. – М.: Издательство Юрайт, 2017. – 245 с.

в) программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины)

1. Национальный стандарт Российской Федерации ГОСТ Р 34.12–2015 «Информационная технология. Криптографическая защита информации. Блочные шифры». – М.: Стандартинформ, 2015.
(интернет-ресурс: <http://protect.gost.ru/document1.aspx?control=7&id=200990> ,
интернет-ресурс: http://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf)

2. Национальный стандарт Российской Федерации ГОСТ Р 34.13–2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров». – М.: Стандартинформ, 2015.
(интернет-ресурс: <http://protect.gost.ru/document1.aspx?control=7&id=200971> ,
интернет-ресурс: http://www.tc26.ru/standard/gost/GOST_R_3413-2015.pdf)
3. ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – М.: Стандартинформ, 2013.
(интернет-ресурс: <http://protect.gost.ru/document.aspx?control=7&id=180151>)
4. ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». – М.: Стандартинформ, 2013.
(интернет-ресурс: <http://protect.gost.ru/v.aspx?control=7&id=180209>)
5. Федеральный закон «Об электронной подписи» от 06.04.2011 N 63-ФЗ
(интернет-ресурс: http://www.consultant.ru/document/cons_doc_LAW_112701/)
6. ГОСТ Р 34.10–2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». – М.: Госстандарт России, 2001.
(интернет-ресурс: <http://protect.gost.ru/v.aspx?control=7&id=131131> ,
интернет-ресурс: http://standartgost.ru/g/ГОСТ_P_34.10-2001)
7. FIPS Publication 197. Specification for the Advanced Encryption Standard (AES). – National Institute of Standards and Technology (NIST), 2001.
(интернет-ресурс: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>)
8. FIPS Publication 46-3. Specifications for the Data Encryption Standard (DES). – National Institute of Standards and Technology (NIST), 1999.
(интернет-ресурс: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>)
9. ГОСТ Р 34.10–94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма». – М.: Госстандарт России, 1994.
(интернет-ресурс: <http://docs.cntd.ru/document/1200004855> ,
интернет-ресурс: http://standartgost.ru/g/ГОСТ_P_34.10-94)
10. ГОСТ Р 34.11–94 «Информационная технология. Криптографическая защита информации. Функция хэширования». – М.: Госстандарт России, 1994.
(интернет-ресурс: <http://protect.gost.ru/document.aspx?control=7&id=134550> ,
интернет-ресурс: http://standartgost.ru/g/ГОСТ_P_34.11-94)

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению подготовки 02.04.02 «Фундаментальная информатика и информационные технологии».

Автор (ы) _____ Л.Ю. Ротков

_____ А.А. Горбунов

Заведующий кафедрой «Безопасность
информационных систем» _____ Л.Ю. Ротков

Программа одобрена на заседании методической комиссии радиофизического факультета от
«25» мая 2023 года, протокол № 04/23.