Приложение 4

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

УТВЕРЖДЕНО

решением президиума Ученого совета ННГУ

протокол № 1 от 16.01.2024 г.

Рабочая программа дисциплины

Основы прикладной криптографии

Уровень высшего образования
Магистратура

Направление подготовки / специальность
02.04.02 - Фундаментальная информатика и информационные технологии

Направленность образовательной программы
Информационная безопасность и защита информации

Форма обучения
очная

г. Нижний Новгород

2024 год начала подготовки

1. Место дисциплины в структуре ОПОП

Дисциплина Б1.В.01 Основы прикладной криптографии относится к части, формируемой участниками образовательных отношений образовательной программы.

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**	**Для текущего контроля успеваемости**	**Для промежуточной аттестации**
УК-2: Способен управлять проектом на всех этапах его жизненного цикла	*УК-2.1: Знает структуру жизненного цикла проекта* *УК-2.2: Умеет адаптировать жизненный цикл под специфику конкретных проектов* *УК-2.3: Владеет методами управления проектом на всех этапах его жизненного цикла*	*УК-2.1:* *Знать:* *- основные требования, предъявляемые к современным алгоритмам шифрования* *- основные системы шифрования с открытыми ключами* *- характеристики электронной подписи, основные требования, предъявляемые к криптографическим функциям* *УК-2.2:* *Уметь:* *- применять основные криптографические средства и системы информационной безопасности* *УК-2.3:* *Владеть:* *- навыками использования основных криптографических средств*	*Собеседование*	*Экзамен: Контрольные вопросы*
ПК-1: Способен руководить научными исследованиями и опытно-конструкторскими разработками, в области информатики и	*ПК-1.1: Знает проблематику и методы научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности*	*ПК-1.1:* *Знать:* *- методы научных исследований основных характеристик шифров* *ПК-1.2:* *Уметь:*	*Собеседование*	*Экзамен: Контрольные вопросы*

информационных технологий (ФИИТ), и формировать их новые направления в области профессиональной деятельности	*ПК-1.2: Имеет навыки выполнения научных исследований и опытно-конструкторских разработок в области ФИИТ применительно к профессиональной деятельности* *ПК-1.3: Имеет навыки руководства исследованиями и опытно-конструкторскими разработками в области ФИИТ применительно к профессиональной деятельности, и формирования их новых направлений*	*- рассчитывать сложность типовых криптографических алгоритмов* *ПК-1.3:* *Владеть:* *- навыками расчета сложности типовых криптографических алгоритмов*		

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная
Общая трудоемкость, з.е.	**4**
Часов по учебному плану	**144**
в том числе	
аудиторные занятия (контактная работа):	
- занятия лекционного типа	**32**
- занятия семинарского типа (практические занятия / лабораторные работы)	**0**
- КСР	**2**
самостоятельная работа	**65**
Промежуточная аттестация	**45** **Экзамен**

3.2. Содержание дисциплины

(структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий)

Наименование разделов и тем дисциплины	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 (практические занятия/лабораторные работы), часы	Всего	
	ооо	ооо	ооо	ооо	ооо

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
Аттестация	45				
КСР	2			2	
Итого	144	32	0	34	65

Содержание разделов и тем дисциплины

1. Основы теории Шеннона. Надежность шифров.
2. Системы симметричного шифрования.
3. Системы асимметричного шифрования.
4. Открытое распространение ключей. Хеш-функция. Электронная цифровая подпись.
5. Криптографические методы защиты информации в телекоммуникационных сетях.

Практические занятия /лабораторные работы организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.
На проведение практических занятий / лабораторных работ в форме практической подготовки отводится: очная форма обучения - 4 ч.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся включает в себя подготовку к контрольным вопросам и заданиям для текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведенным в п. 5.

Электронно-библиотечная система "Юрайт"
Электронно-библиотечная система "Лань"

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

5.1 Типовые задания, необходимые для оценки результатов обучения при проведении текущего контроля успеваемости с указанием критериев их оценивания:

5.1.1 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции УК-2:

1. Стойкость шифров. Правило Керкхоффа.
2. Ненадежность шифров и расстояние единственности.
3. Понятие блочного и поточного шифра.

4. Российские стандарты шифрования. Основные характеристики.
5. Криптография с открытыми ключами. Односторонние функции.
6. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
7. Электронная цифровая подпись. Свойства электронной цифровой подписи.

5.1.2 Типовые задания (оценочное средство - Собеседование) для оценки сформированности компетенции ПК-1:

1. Комбинирование блочных шифров.
2. Основные характеристики шифров DES, AES.
3. Криптосистема RSA.
4. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты.
5. Криптографические протоколы.
6. Криптографические функции хеширования.

Критерии оценивания (оценочное средство - Собеседование)

Оценка	Критерии оценивания
зачтено	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно»
не зачтено	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно» или на уровне «плохо»

5.2. Описание шкал оценивания результатов обучения по дисциплине при промежуточной аттестации

Шкала оценивания сформированности компетенций

Уровень сформированности компетенций (индикатора достижения компетенций)	**плохо**	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	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. Ошибок нет.	Уровень знаний в объеме, превышающем программу подготовки.
Умения	Отсутствие минимальных умений.	При решении стандартных задач не	Продемонстрированы основные	Продемонстрированы все	Продемонстрированы все	Продемонстрированы все	Продемонстрированы все основные

	Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	продемонстрированы основные умения. Имели место грубые ошибки	умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания, но не в полном объеме	основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания в полном объеме, но некоторые с недочетами	основные умения. Решены все основные задачи. Выполнены все задания в полном объеме, но некоторые с недочетами.	основные умения. Решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	умения. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие базовых навыков. 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	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценивания при промежуточной аттестации

Оценка		Уровень подготовки
зачтено	**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».
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «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»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно».
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения на промежуточной аттестации с указанием критериев их оценивания:

5.3.1 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции УК-2

1. Теоретическая и практическая стойкость криптосистем.
2. Стойкость шифров. Правило Керкхоффа.
3. Теорема Шеннона о совершенной секретности.
4. Математические основы криптографии. Ненадежность шифров и расстояние единственности.
5. Понятие блочного и поточного шифра.
6. Алгоритмы шифрования на основе сетей Фейстеля.
7. Режимы работы блочных шифров. Комбинирование блочных шифров.
8. Криптография с открытыми ключами. Односторонние функции. Алгоритмы шифрования и цифровой подписи.
9. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
10. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
11. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования.
12. Электронная цифровая подпись. Свойства электронной цифровой подписи.

5.3.2 Типовые задания (оценочное средство - Контрольные вопросы) для оценки сформированности компетенции ПК-1

1. Режимы работы блочных шифров. Комбинирование блочных шифров.
2. Стандарт шифрования данных DES. Основные характеристики.
3. Российские стандарты шифрования ГОСТ 28147-89, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Основные характеристики.
4. Стандарт шифрования AES. Основные характеристики.
5. Потоковый шифр A5/1. Основные характеристики.
6. Потоковый шифр RC4. Основные характеристики.
7. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
8. Криптосистема RSA.
9. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
10. Алгоритм хеширования SHA.
11. Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты.
12. Системы электронной безопасности в финансовой сфере. Статическая и динамическая аутентификация данных на картах.

Критерии оценивания (оценочное средство - Контрольные вопросы)

Оценка	Критерии оценивания
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

Оценка	Критерии оценивания
	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»

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература:

1. Васильева И. Н. Криптографические методы защиты информации : учебник и практикум / И. Н. Васильева. - Москва : Юрайт, 2023. - 349 с. - (Высшее образование). - ISBN 978-5-534-02883-6. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=839932&idb=0.
2. Запечников С. В. Криптографические методы защиты информации : учебник / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-02574-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=842677&idb=0.
3. Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд. - Москва : Юрайт, 2023. - 473 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=840431&idb=0.

Дополнительная литература:

1. Введение в теоретико-числовые методы криптографии / Глухов М. М.,Круглов И. А.,Пичкур А. Б.,Черемушкин А. В. - Санкт-Петербург : Лань, 2022. - 400 с. - Допущено УМО вузов по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Криптография». - Книга из коллекции Лань - Информатика. - ISBN 978-5-8114-1116-0., https://e-lib.unn.ru/MegaPro/UserEntry?

Action=FindDocs&ids=799760&idb=0.
2. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. - Москва : Юрайт, 2023. - 209 с. - (Высшее образование). - ISBN 978-5-9916-7088-3. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=846028&idb=0.
3. Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. - Москва : Юрайт, 2023. - 245 с. - (Высшее образование). - ISBN 978-5-9916-7090-6. - Текст : электронный // ЭБС "Юрайт"., https://e-lib.unn.ru/MegaPro/UserEntry?Action=FindDocs&ids=847475&idb=0.

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_Р_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_Р_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_Р_34.11-94)

7. Материально-техническое обеспечение дисциплины (модуля)

Учебные аудитории для проведения учебных занятий, предусмотренных образовательной программой, оснащены мультимедийным оборудованием (проектор, экран), 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/специальности 02.04.02 - Фундаментальная информатика и информационные технологии.

Автор(ы): Ротков Леонид Юрьевич, кандидат технических наук, доцент
Горбунов Александр Александрович.

Заведующий кафедрой: Ротков Леонид Юрьевич, кандидат технических наук.

Программа одобрена на заседании методической комиссии от 18 декабря 2023 года, протокол № 09/23.