

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)

УТВЕРЖДАЮ:

Декан _____ Матросов В.В.

« 29 » _____ июня 2020 г.

Рабочая программа дисциплины

Б1.Б.27 Криптографические методы защиты
информации

(наименование дисциплины (модуля))

Уровень высшего образования
специалитет

(бакалавриат / магистратура / специалитет)

Направление подготовки / специальность

10.05.02 Информационная безопасность телекоммуникационных систем

(указывается код и наименование направления подготовки / специальности)

Направленность образовательной программы

Системы подвижной цифровой защищенной связи

(указывается профиль / магистерская программа / специализация)

Квалификация (степень)

специалист

(бакалавр / магистр / специалист)

Форма обучения

очная

(очная / очно-заочная / заочная)

Нижний Новгород

2018

1. Место и цели дисциплины в структуре ОПОП

Дисциплина «Криптографические методы защиты информации» относится к дисциплинам базовой части основной профессиональной образовательной программы по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем», преподается в 7 и 8 семестрах.

Изучение студентами дисциплины «Криптографические методы защиты информации» базируется на знаниях и умениях, полученных в результате изучения дисциплин «Дискретная математика», «Математическая логика и теория алгоритмов», «Алгоритмы и анализ сложности», «Сети и системы передачи информации», «Операционные системы».

Целями освоения дисциплины являются:

Основной целью дисциплины является изложение основополагающих принципов защиты информации с помощью криптографических методов, примеров реализации этих методов на практике. Содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, основными алгоритмами шифрования и криптографическими протоколами обмена информацией.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников)

Формируемые компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ОПК-2. Способность применять соответствующий математический аппарат для решения профессиональных задач. (этап освоения: завершающий)	31 (ОПК-2). Знать основные понятия криптографии. 32 (ОПК-2). Знать требования к шифрам и основные характеристики шифров. 33 (ОПК-2). Знать типовые поточные и блочные шифры, асимметричные криптосистемы. У1 (ОПК-2). Уметь применять математические методы описания и исследования криптосистем. В1 (ОПК-2). Владеть основами криптографической терминологии. В2 (ОПК-2). Владеть навыками математического моделирования в криптографии. В3 (ОПК-2). Владеть навыками обращения с научно-технической литературой в области криптографической защиты информации.
ПК-3. Способность оценивать технические возможности и вырабатывать рекомендации по построению телекоммуникационных систем и сетей, их элементов и	31 (ПК-3). Знать частотные характеристики открытых текстов и их применение к анализу простейших симметричных криптосистем. 32 (ПК-3). Знать основные криптографические протоколы.

устройств. (этап освоения: базовый)	У1 (ПК-3). Уметь оценивать криптографическую стойкость шифров. В1 (ПК-3). Владеть навыками использования типовых криптографических алгоритмов.
--	---

3. Структура и содержание дисциплины «Криптографические методы защиты информации»

Объем дисциплины составляет 5 зачетных единиц, всего 180 часов, из которых 67 часов составляет контактная работа обучающегося с преподавателем (64 часа занятия лекционного типа, в том числе 4 часа – мероприятия текущего контроля успеваемости, 3 часа – мероприятия промежуточной аттестации), 113 часов составляет самостоятельная работа обучающегося.

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. Введение в криптографические методы защиты информации. Криптографические и стеганографические методы защиты информации.	8	4			4	4
2. Одноалфавитный шифр. Многоалфавитные шифры. Омофонический шифр замены. Диграф.	14	4			4	10
3. Математические основы криптографии. Введение в конечные поля. Операции в группах. Кольцо. Поле. Поле Галуа.	16	6			6	10
4. Китайская теорема об остатках. Теорема Ферма. Функция Эйлера. Теорема	22	8			8	14

Эйлера. Алгоритм Евклида. Расширенный алгоритм Евклида.						
5. Дискретные логарифмы. Разложение составных чисел на множители. Эллиптические кривые.	20	8			8	12
6. Основы теории Шеннона. Надежность шифров.	13	4			4	9
7. Системы симметричного шифрования.	20	8			8	12
8. Системы асимметричного шифрования.	20	8			8	12
9. Открытое распространение ключей. Хеш-функция. Электронная цифровая подпись.	20	6			6	14
10. Криптографические методы защиты информации в телекоммуникационных сетях.	24	8			8	16
В т.ч. текущий контроль	4	4			4	
Промежуточная аттестация: зачет, экзамен						

4. Образовательные технологии

Образовательные технологии, способствующие формированию компетенций, используемые на занятиях лекционного типа:

- лекции с изложением учебного материала.

5. 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.

6. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

6.1. Перечень компетенций выпускников образовательной программы с указанием результатов обучения (знаний, умений, владений), характеризующих этапы их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования.

Индикаторы компетенции	Критерии оценивания	
	«незачтено»	«зачтено»
<u>Знания</u>	Наличие грубых ошибок в основном материале	Знание основного материалом, возможно с рядом погрешностей
<u>Умения</u>	Наличие грубых ошибок при выполнении стандартных заданий	Способность выполнения всех стандартных заданий, возможно с незначительными погрешностями
<u>Навыки</u>	Отсутствие навыка	Достаточное владение навыком

Индикаторы компетенции	Критерии оценивания						
	«плохо»	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«очень хорошо»	«отлично»	«превосходно»
<u>Знания</u>	Отсутствие знаний материала	Наличие грубых ошибок в основном материале	Знание основного материала с рядом негрубых ошибок	Знание основного материала с рядом заметных погрешностей	Знание основного материала с незначительными и погрешностями	Знание основного материала без ошибок и погрешностей	Знание основного и дополнительного материала без ошибок и погрешностей
<u>Умения</u>	Отсутствие способности решения стандартных задач	Наличие грубых ошибок при решении стандартных задач	Способность решения основных стандартных задач с существенными ошибками	Способность решения всех стандартных задач с незначительными погрешностями	Способность решения всех стандартных задач без ошибок и погрешностей	Способность решения стандартных и некоторых нестандартных задач	Способность решения стандартных задач и широкого круга нестандартных задач
<u>Навыки</u>	Полное отсутствие навыка	Отсутствие навыка	Владение навыком в минимальном	Посредственное владение навыком	Достаточное владение навыком	Хорошее владение навыком	Всестороннее владение навыком

			объёме				м
--	--	--	--------	--	--	--	---

6.2. Описание шкал оценивания.

Контроль качества усвоения студентами содержания дисциплины проводится в виде зачета и экзамена.

Зачет проводится в устной форме и заключается в ответе студентом после предварительной подготовки на теоретические вопросы курса и решением практической задачи с последующим его обоснованием. По окончании ответа на вопросы билета в рамках тематики курса проводится собеседование в форме вопросов, на которые студент должен дать краткий ответ.

Итоговый контроль качества усвоения студентами содержания дисциплины проводится в виде экзамена, на котором определяется:

- уровень усвоения студентами основного учебного материала по дисциплине;
- уровень понимания студентами изученного материала;
- способности студентов использовать полученные знания для решения конкретных задач.

Критерии оценок.

Оценка	Уровень подготовки
Зачтено	В целом хорошая подготовка с возможными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы.
Не зачтено	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы.

Оценка	Уровень подготовки
Превосходно	Высокий уровень подготовки, безупречное владение теоретическим материалом, студент демонстрирует творческий подход к решению нестандартных ситуаций. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждая теоретический материал практическими примерами.
Отлично	Высокий уровень подготовки с незначительными ошибками. Студент дал полный и развернутый ответ на все теоретические вопросы билета, подтверждает теоретический материал практическими примерами.
Очень хорошо	Хорошая подготовка. Студент дает ответ на все теоретические вопросы билета при наличии неточностей.
Хорошо	В целом хорошая подготовка с заметными ошибками или недочетами. Студент дает полный ответ на все теоретические вопросы билета при наличии неточностей. Допускаются ошибки при ответах на дополнительные и уточняющие вопросы экзаменатора.
Удовлетворительно	Минимально достаточный уровень подготовки. Студент показывает минимальный уровень теоретических знаний, делает существенные ошибки, но при ответах на наводящие вопросы, может правильно сориентироваться и в общих чертах дать правильный ответ.
Неудовлетворительно	Подготовка недостаточная и требует дополнительного изучения материала. Студент дает ошибочные ответы, как на теоретические вопросы билета, так и на дополнительные вопросы экзаменатора.

Плохо	Подготовка абсолютно недостаточная. Студент не отвечает на поставленные вопросы.
-------	--

6.3. Критерии и процедуры оценивания результатов обучения по дисциплине, характеризующих этапы формирования компетенций.

Для оценивания результатов обучения в виде **знаний** используются следующие процедуры и технологии: экзамен, проводимый в письменной форме с дальнейшим индивидуальным собеседованием.

Для оценивания результатов обучения в виде **умений** и **навыков** используются результаты обсуждения типовых криптографических решений в контексте их использования в реальных ситуациях.

6.4. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций и (или) для итогового контроля сформированности компетенции.

Типовые задания (оценочные средства), выносимые на экзамен.

6.4.1. Задания для оценки компетенции «ОПК-2»:

1. Основные понятия криптографии: шифр, алгоритм шифрования, ключ шифрования, криптосистема. Обобщенная схема для криптосистем с закрытыми ключами шифрования.
2. Основные исторические этапы становления криптографии. Криптографические и стеганографические методы защиты информации. Криптология, криптография и криптоанализ.
3. Многоалфавитные шифры. Омофонический шифр замены.
4. Понятие вычета по модулю. Понятие сравнимости двух чисел.
5. Введение в конечные поля. Понятие группы. Циклическая группа. Правила выполнения операций в группах.
6. Кольцо. Кольцо с единицей. Подкольцо. Целостное кольцо.
7. Поле. Порядок и степень поля. Поле Галуа. Примитивный элемент конечного поля. Неприводимые многочлены. Умножение ненулевых элементов конечного поля.
8. Простые числа. Взаимно простые числа. Утверждение о сравнимости чисел. Понятие обратного числа. Утверждение о существовании обратного числа.
9. Мультипликативность функции.
10. Теорема Ферма.
11. Функция Эйлера. Функция Мебиуса. Теорема Эйлера.
12. Алгоритм Евклида. Расширенный алгоритм Евклида.
13. Дискретные логарифмы.
14. Эллиптические кривые. Безопасность систем дискретных логарифмов над эллиптическими кривыми.
15. Теоретическая и практическая стойкость криптосистем.
16. Стойкость шифров. Правило Керкхоффа.
17. Теорема Шеннона о совершенной секретности.
18. Математические основы криптографии. Ненадежность шифров и расстояние единственности.
19. Понятие блочного и поточного шифра.
20. Алгоритмы шифрования на основе сетей Фейстеля.
21. Режимы работы блочных шифров. Комбинирование блочных шифров.

22. Криптография с открытыми ключами. Односторонние функции. Алгоритмы шифрования и цифровой подписи.
23. Криптографические протоколы. Проблемы криптографических протоколов. Трехэтапный протокол Шамира.
24. Криптографические функции хеширования. Основные требования, предъявляемые к криптографическим функциям хеширования.

6.4.2. Задания для оценки компетенции «ПК-3»:

1. Стандарт шифрования данных DES. Основные характеристики.
2. Российские стандарты шифрования ГОСТ 28147-89, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Основные характеристики.
3. Стандарт шифрования AES. Основные характеристики.
4. Поточковый шифр A5/1. Основные характеристики.
5. Поточковый шифр RC4. Основные характеристики.
6. Алгоритм Диффи-Хеллмана обмена ключевой информацией.
7. Криптосистема RSA.
8. Электронная цифровая подпись. Свойства электронной цифровой подписи.
9. Алгоритм хеширования SHA.
10. Открытое распространение ключей. Инфраструктура открытого распространения ключей (PKI) и ее основные компоненты.
11. Системы электронной безопасности в финансовой сфере. Статическая и динамическая аутентификация данных на картах

6.5. Методические материалы, определяющие процедуры оценивания.

Положение «О проведении текущего контроля успеваемости и промежуточной аттестации обучающихся в ННГУ», утвержденное приказом ректора ННГУ от 13.02.2014 г. №55-ОД.

Положение «О фонде оценочных средств», утвержденное приказом ректора ННГУ от 10.06.2015 г. №247-ОД.

7. 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. Лапониная 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:

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)

8. Материально-техническое обеспечение дисциплины

Аудиторный фонд ННГУ для проведения лекций.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ОПОП ВПО по специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

Автор (ы) _____ С.А. Лапинова

_____ Л.Ю. Ротков

_____ А.А. Горбунов

Рецензент (ы) _____ С.Н. Жуков

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

Программа одобрена на заседании методической комиссии радиофизического факультета от «25» июня 2020 года, протокол № 03/20.