

Направление подготовки 10.04.01 «Информационная безопасность»
Магистерская программа «Безопасность автоматизированных систем»
РПД Б1.В.05 «Криптографические методы и средства защиты информации»



**Филиал федерального государственного бюджетного образовательного учреждения
высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске**

УТВЕРЖДАЮ

Зам. директора
по учебно-методической работе
филиала ФГБОУ ВО
«НИУ «МЭИ» в г. Смоленске



В.В. Рожков
« 03 » 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: **10.04.01. «Информационная безопасность»**

Профиль: **«Безопасность автоматизированных систем»**

Уровень высшего образования: **магистратура**

Нормативный срок обучения: **2 года**

Форма обучения: **очная**

Год набора: **2024**

Смоленск

Программа составлена с учетом ФГОС ВО по направлению подготовки 10.04.01 «Информационная безопасность», утвержденного приказом Минобрнауки России от «26» ноября 2020 г. № 1455.

Программу составил:

подпись

к.т.н., доцент А.В. Полячков
ФИО

«18» апреля 2024 г.

Программа обсуждена и одобрена на заседании кафедры «Вычислительная техника»
«24» апреля 2024 г., протокол № 7.

Заведующий кафедрой «Вычислительной техники»:

подпись

д.т.н., профессор А.С. Федулов
ФИО

«2» мая 2024 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

**Ответственный в филиале по работе
с ЛОВЗ и инвалидами**

подпись

зам. начальника УУ Е.В. Зуева
ФИО

«2» мая 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к проектной деятельности по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины

- фундаментальная подготовка студентов в области криптографических методов и средств защиты информации;
- формирование подходов к выполнению самостоятельных исследований студентами в области криптографических методов и средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Криптографические методы и средства защиты информации относится к части, формируемой участниками образовательных отношений..

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами:

Б1.В.03 Проектирование программного обеспечения автоматизированных систем

Б1.В.04 Информационная безопасность компьютерных сетей

Б1.В.05 Интеллектуальный анализ и моделирование информационных систем и процессов

Перечень последующих дисциплин и практик, для которых необходимы знания, умения и навыки, формируемые данной дисциплиной:

Б2.В.02(П) Проектно-технологическая практик

Б2.В.03(П) Преддипломная практика

Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-1. Способен активно участвовать в управлении функционированием системы обеспечения информационной безопасности (СОИБ)	ПК-1.1 Способен проектировать программное обеспечение для защиты информации автоматизированных систем	Знает: - принципы и средства проектирования криптографических примитивов/протоколов. Умеет: - применять знания в области обеспечения криптостойкости и сниже-

Компетенция	Индикаторы достижения компетенций	Результаты обучения
организации на основе современных положений СМИБ		ния уязвимости криптографических протоколов и преобразований в разрабатываемом программном обеспечении; Владеет: - навыками оценки рисков информационной безопасности программного обеспечения автоматизированных систем.
	ПК-1.2 Способен проектировать аппаратные средства для защиты информации автоматизированных систем	Знает: -методы и способы реализации криптографических примитивов/протоколов аппаратными средствами. Умеет: - обосновывать применение средств, обеспечивающих криптостойкость криптографических протоколов и преобразований; Владеет: - навыками оценки рисков информационной безопасности аппаратных средств автоматизированных систем.



4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3												Семестр 4												Итого за курс												Каф.	Семестр			
			Контроль	Академических часов									з.е.	Неделя	Контроль	Академических часов									з.е.	Неделя																	
				Всего	Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего				Кон такт.	Лек	Лаб	Пр	КРП	СР	Контроль	Всего	Неделя																			
1	Б1.В.06	Криптографические методы и средства защиты информации	Экз КР	216	104	34	34	18	18	76	36	6																		Экз КР	216	104	34	34	18	18	76	36	6			15	3

ОБОЗНАЧЕНИЯ:

Виды промежуточной аттестации (виды контроля):

- Экз - экзамен;
- ЗаО - зачет с оценкой;
- За – зачет.

Виды работ:

- Контакт. – контактная работа обучающихся с преподавателем;
- Лек. – лекционные занятия;
- Лаб.– лабораторные работы;
- Пр. – практические занятия;
- КРП – курсовая работа (курсовой проект);
- РГР – расчетно-графическая работа (реферат);
- СР – самостоятельная работа студентов;
- з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	<p>Лекционные занятия - 17 шт. по 2 часа.</p> <p>Тема 1. Введение в криптографию.</p> <p>1.1. Введение в криптографию (2 часа). Основные определения. История криптографии. Классификация криптоалгоритмов.</p> <p>Тема 2. Математические основы криптографии.</p> <p>1.2. Модульная арифметика и алгебраические структуры (2 часа) Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Алгебраические структуры. Поля Галуа.</p> <p>1.3. Генерация и тестирование псевдослучайных последовательностей (2 часа). Структура генератора псевдослучайных последовательностей (ГПСП). Алгоритмы генерации псевдослучайных последовательностей Криптографические стойкие ГПСП. Тестирование ГПСП.</p> <p>Тема 3. Симметричная криптография.</p> <p>1.4. Современные блочные шифры (2 часа). Стандарт шифрования DES. Режимы работы алгоритма DES. Стандарт шифрования AES.</p> <p>1.5 Российский стандарт шифрования (2 часа). Стандарт шифрования ГОСТ Р 34. 12-2015 (Магма и Кузнечик)</p> <p>1.6. Современные шифры потока (2 часа). Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании. Шифр RC4.</p> <p>1.7. Шифрование, использующее современные шифры с симметричным ключом (2 часа). Применение современных блочных шифров. Использование шифров потока. Методы повышения криптостойкости симметричных криптосистем.</p> <p>Тема 4. Асимметричная криптография.</p> <p>1.8. Криптосистема RSA (2 часа). Принцип работы современных асимметричных криптосистем. Криптосистема RSA. Криптосистема Эль-Гамала. Криптосистема Рабина.</p> <p>1.9. Криптосистемы на основе метода эллиптических кривых (2 часа). Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа, криптография эллиптической кривой, моделирующая криптосистему Эль-Гамала</p> <p>Тема 5. Целостность и установление подлинности.</p> <p>1.10. Обеспечение целостности передаваемых данных (2 часа). Целостность сообщения. Случайная модель Oacle. Установление подлинности сообщения</p> <p>1.11. Криптографические хеш-функции (2 часа). Итеративные хеш-функции. Схема Меркеля-Дамгарда. Хеш- функции, основанные на блочных шифрах. Схема Рабина. Алгоритм безопасного хеширования SHA. Шифр Whirlpool. Российский стандарт хеширования ГОСТ Р 34.11-2012.</p> <p>1.12. Электронная цифровая подпись (2 часа). Алгоритм формирования электронной цифровой подписи (ЭЦП). Схема ЭЦП RSA. ЭЦП Эль-Гамала. ЭЦП Шнорра. Стандарт цифровой подписи DSS. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10-2012.</p> <p>1.13. Установление подлинности объекта (2 часа). Аутентификация на основе пароля. Одноразовый пароль. Система установления подлинности «запрос-ответ». Подтверждение с нулевым разглашением. Протокол Фиата-Шамира. Биометрия. Физиологические и поведенческие методы биометрии.</p> <p>Тема 6. Управление криптографическими ключами.</p> <p>1.14. Генерация и хранение криптографических ключей (2 часа). Стандарт ANSI. X9.17. Методы хранения ключевой информации.</p> <p>1.15. Алгоритмы безопасного распределения ключей (2 часа). Прямой обмен ключами между пользователями. Система «запрос-ответ». Алгоритм Ниидома-Шредера. Ал-</p>

№	Наименование видов занятий и тематик, содержание
	<p>горитм Диффи-Хеллмана. Использование Центра распределения ключей. Инфраструктура PKI. Стандарт X.509. Система Kerberos.</p> <p>Тема 7. Основы современной стеганографии.</p> <p>1.16. Основы современной стеганографии (2 часа). Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.</p> <p>Тема 8. Основы криптоанализа.</p> <p>1.17. Обзор методов криптоанализа (2 часа). Методы криптоанализа. Криптоанализ блочных шифров. Частотный криптоанализ. Современные методы криптоанализа. Дифференциальный криптоанализ. Линейный криптоанализ. Интерполяционный криптоанализ. Методы криптоанализа, основанные на слабости ключевых разверток.</p>
2	<p>Лабораторные работы, количество - 8 по 4 (2) часа.</p> <p>2.1. Разработка классических криптоалгоритмов.</p> <p>2.2. Генерация и тестирование псевдослучайных последовательностей.</p> <p>2.3 Программные средства реализации современных симметричных криптосистем.</p> <p>2.4. Современные симметричные криптосистемы. Программная реализация существующих симметричных криптоалгоритмов</p> <p>2.5 Асимметричные криптосистемы. Изучение принципов работы асимметричных криптосистем; Изучение реализаций асимметричной криптографии в среде .NET Framework; Реализация существующих асимметричных криптоалгоритмов.</p> <p>2.6. Хеширование и электронная цифровая подпись. Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); Изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; Реализация существующих хэш-функций и алгоритмов ЭЦП.</p> <p>2.7. Безопасное распределение ключей. Изучение методов безопасного распределения ключей в небезопасной среде. Изучение свойств и методов класса ECDiffieHellmanCng пространства имен System.Security.Cryptography для создания ключей по алгоритму Диффи-Хеллмана. Использование алгоритма шифрования RSA для безопасного распределения ключей симметричной криптосистемы</p> <p>2.8. Разработка стеганографической системы. Разработка системы для скрытой передачи сообщений.</p>
3	<p>Практические работы, количество - 9 по 2 часа.</p> <p>3.1. Шифры перестановки</p> <p>3.2. Симметричные криптосистемы</p> <p>3.3. Ассиметричные криптосистемы</p> <p>3.4. Технологии цифровой подписи</p> <p>3.5. Разработка стеганографической системы.</p> <p>3.6. Разработка системы для скрытой передачи сообщений.</p> <p>3.7. Частотный криптоанализ.</p> <p>3.8. Криптоанализ шифра Вижинера</p>
3	<p>Курсовая работа «Криптографические методы и средства защиты информации».</p> <p>Выполнение индивидуального задания, предполагающего разработку программы.</p> <p>Примерная тематика:</p> <ul style="list-style-type: none"> • Криптоанализ блочных симметричных шифров • Криптоанализ поточных симметричных шифров • Криптоанализ хэш-функций • Исследование безопасности генераторов ПСЧ

№	Наименование видов занятий и тематик, содержание
	<ul style="list-style-type: none"> • Разработка системы аутентификации пользователей с нулевым разглашением • Идентификация пользователя по клавиатурному почерку • Разработка криптосистемы на основе метода эллиптических кривых • Библиотека криптографических функций ГОСТ Р 34.12-2015 • Программная реализация криптосистемы Хилла • Исследование методов реализации безопасных и эффективных постквантовых криптосистем • Разработка системы атрибуции документов • Разработка стеганографической системы • Защита информации с помощью цифровых водяных знаков • Система тестирования псевдослучайных последовательностей с помощью статистического теста «Стопка книг» • Генератор псевдослучайных чисел на основе клеточных автоматов
4	<p>Самостоятельная работа студентов:</p> <p>4.1. Подготовка к защите лабораторных работ.</p> <p>4.2. Подготовка к практическим занятиям.</p> <p>4.2. Самостоятельное изучение теоретических материалов по следующим вопросам.</p> <p>Тема 1. Изучение классических криптосистем (Шифр Цезаря, Полибианский квадрат, Двойной квадрат Уитстона, Одноразовая система шифрования, диск Альберти, шифр Вижинера, роторные машины).</p> <p>Тема 2. Изучение следующих материалов: вычисление мультипликативных обратных величин, расширенный алгоритм Евклида, китайская теорема об остатках, квадратичные вычеты, вычисления в конечных полях.</p> <p>Тема 3. Режимы работы алгоритма DES. Алгоритмы 3DES, EDE, IDEA, Blowfish. Формирование ключей алгоритма AES.</p> <p>Тема 4. Ранцевая криптография.</p> <p>Тема 5. Протокол Фейге-Фиата-Шамира. Протокол Кискатера-Гийу.</p> <p>Тема 6. Принцип работы системы Kerberos.</p> <p>Тема 7. Стеганография в современных кибератаках.</p> <p>Тема 8. Математические методы криптоанализа асимметричных криптосистем.</p> <p>4.3. Выполнение курсовой работы.</p>

Текущий контроль:

- проверка конспектов лекций и дополнительных теоретических материалов;
- проверка отчетов по лабораторным работам;
- защита лабораторных работ;
- контрольный опрос и выполнение контрольных заданий на практических занятиях;
- консультации по курсовой работе.

Результаты текущего контроля фиксируются с использованием трехбалльной системы (0, 1, 2) при проведении контрольных недель по графику филиала в течение семестра, а также учитываются преподавателем при осуществлении промежуточной аттестации по настоящей дисциплине.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица - Образовательные технологии, используемые при реализации различных видов учебных занятий по дисциплине

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция. Интерактивная лекция (лекция-визуализация). Интерактивная лекция (проблемная лекция). Лекция, составленная на основе результатов научных исследований, в том числе с учётом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей. Индивидуальные и групповые консультации по дисциплине.
2	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально. Технология проблемного обучения на основе анализа результатов лабораторной работы: индивидуальный опрос, представление студентом результатов лабораторной работы в форме отчета.
3	Практические занятия	Технология коллективного выполнения и разбора примерных заданий по теме занятия с последующим выполнением индивидуальных задач и примеров. Представление студентом результатов работы на практическом занятии в форме протокола.
4	Консультации по курсовой работе	Индивидуальные и групповые консультации с привлечением средств проектирования ПО для контроля работоспособности разработанных средств и демонстрации их возможностей. Для оперативного консультирования на заключительном этапе оформления и тестирования готового продукта используются технологии взаимодействия со студентами в режимах связи «offline» и «online».
5	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине).
6	Контроль (промежуточная аттестация: КРП, экзамен).	Защита КРП. Ответ по билету.

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ – ДЛЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Оценочные средства текущего контроля успеваемости:

Вопросы для защиты лабораторных работ

Лабораторная работа 1 на тему «Разработка классических криптоалгоритмов».

1. К какому классу шифров относится шифр Вижинера
2. К какому классу шифров относится диск Альберти
3. К какому шифру наиболее близок алгоритм работы роторной машины
4. Дана фраза «HGFUBSWGHFUBSW», зашифрованная шифром Цезаря. Криптоаналитику известно, что ключ представляет собой число в диапазоне от 2 до 4. Выполните дешифрование
5. Дана фраза «GQSUGAAC», зашифрованная методом Гронсфельда. Криптоаналитику известно, что длина ключа равна 3 и ключ представляет собой сочетание цифр 1 и 2. Выполните дешифрование

Лабораторная работа 2 на тему «Генерация и тестирование псевдослучайных последовательностей».

1. Перечислите способы получения случайных чисел
2. Какие числа называются псевдослучайными
3. В чем заключается сущность мультипликативного конгруэнтного метода формирования последовательности равномерно распределенных псевдослучайных чисел
4. Какие тесты используются для проверки генераторов псевдослучайных чисел.
5. Объясните метод проверки генераторов псевдослучайных чисел, основанный на использовании критерия хи-квадрат

Лабораторная работа 3 на тему «Программные средства реализации современных симметричных криптосистем».

1. Перечислите основные классы пространства имен System.Security.Cryptography. Кратко опишите назначение каждого класса
2. Перечислите основные методы класса System.Security.Cryptography. SymmetricAlgorithm
3. Перечислите классы, производные от класса System.Security.Cryptography. SymmetricAlgorithm. Кратко опишите назначение каждого класса
4. С помощью какого метода пространства имен System.Security.Cryptography производится проверка ключей криптографическую слабость

Лабораторная работа 4 на тему «Современные симметричные криптосистемы».

1. Сравните DES и AES. Какой из них ориентирован на работу с битом, а какой с байтом
2. Сравните подстановку в DES и AES. Почему в AES только одна таблица перестановки (S-блок), а в DES- несколько
3. Сравните ключи раунда в DES и AES. В каком шифре размер ключа раунда равен размеру блока.
4. Для каких целей используется режим выработки имитовставки в алгоритме Магма (ГОСТ Р 34.12-2015)
5. Сравните алгоритмы ГОСТ 8147-89 и Магма (ГОСТ Р 34.12-2015)
6. Сравните алгоритмы AES и Кузнечик (ГОСТ Р 34.12-2015)

Лабораторная работа 5 на тему «Асимметричные криптосистемы».

1. Для числа $a=5$ найдите обратное число по модулю $n=7$. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.

2. Для числа $a=72$ найдите обратное число по модулю $n=8$. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.
3. Для числа $N=7*11$ с помощью функции Эйлера $\varphi(N)$ определите количество положительных целых чисел, меньших N и взаимно простых с N . В каких криптосистемах используется функция Эйлера?
4. Определите хотя бы одно возможное значение открытого ключа алгоритма RSA, если $P=3$ $Q=11$.
5. Определите значение закрытого ключа для алгоритма RSA, если открытый ключ $E=7$, а функция Эйлера имеет значение $\varphi(N)=20$
6. В криптосистеме RSA дано $N=221$ и $E=5$, найдите D .
7. В криптосистеме RSA дано $N=3937$ и $E=17$, найдите D .
8. В криптосистеме RSA дано $P=19$, $Q=23$ и $E=3$, найдите N , $\varphi(N)$ и D .
9. В криптосистеме RSA дано $E=13$ и $N=100$. Зашифруйте сообщение «HOW ARE YOU», кодируя английский алфавит числами от 00 до 25 и используя число 26 для пробела. Используйте различные блоки, чтобы сделать $P < N$

Лабораторная работа 6 на тему «Хеширование и электронная цифровая подпись».

1. Что называется «электронной цифровой подписью»?
2. Для чего используется электронная цифровая подпись?
3. Что такое дайджест сообщения?
4. Используя схему RSA, при $P=809$, $Q=751$ и секретный ключ $D=23$, вычислите открытый ключ E , затем, подпишите и проверьте сообщение $M_1=100$. Получите подпись S_1 .
5. Используя схему RSA, при $P=809$, $Q=751$ и секретный ключ $D=23$, вычислите открытый ключ E , затем, подпишите и проверьте сообщение $M_2=50$. Получите подпись S_2 .
6. Используя схему RSA, при $P=809$, $Q=751$ и секретный ключ $D=23$, вычислите открытый ключ E , затем, покажите, что если $M=M_1 \times M_2=5000$, то $S=S_1 \times S_2$.

Лабораторная работа 7 на тему «Безопасное распределение ключей».

1. В протоколе Диффи-Хеллмана $g=7$, $p=23$, секретный ключ пользователя $A=3$, секретный ключ пользователя $B=5$. Какое значение имеет симметричный ключ? Какие значения имеют открытые ключи пользователей A и B ?
2. Что случится в протоколе Диффи-Хеллмана, если секретные ключи пользователей A и B имеют одно и то же значение? Будут ли совпадать открытые ключи пользователей A и B ? Будут ли совпадать симметричные ключи, вычисленные пользователями A и B ? Приведите пример, для доказательства Ваших умозаключений.
3. В протоколе Диффи-Хеллмана значение $p=53$. Найдите соответствующее значение для g .
4. Какие классы содержит пространство имен System.Net.Sockets. Опишите назначение, особенности и функциональные возможности каждого класса.
5. Укажите преимущества и недостатки протокола UDP. Ответ обоснуйте.
6. Укажите преимущества и недостатки протокола TCP. Ответ обоснуйте.
7. Дайте определение сокета. Какую информацию должен содержать сокет?

Лабораторная работа 8 на тему «Разработка стеганографической систем».

1. Перечислите базовые принципы компьютерной стеганографии
2. Особенности упаковки информации в файлы формата JPEG
3. Какие звуковые файлы рекомендуется выбирать в качестве контейнеров
4. Какие графические файлы рекомендуется выбирать в качестве контейнеров
5. Изменяются ли размеры файлов-контейнеров разных типов после сокрытия в них информации

6. Как происходит сокрытие информации в текстовых и html-файлах

Оценочные средства для промежуточной аттестации – защита КР

Когда курсовая работа полностью выполнена (т.е. курсовая работа выполнена и оформлена, проверена руководителем, продемонстрирована работающая программа), она допускается к защите. Требования к содержанию и оформлению КР приведены в методических указаниях по КР.

Дата, место защиты и состав членов комиссии назначаются заранее распоряжением по кафедре.

На защиту представляется:

курсовая работа в печатном виде, в обложке и переплетенная (сшитая);

курсовая работа в электронном виде;

программа в исходной форме;

программа откомпилированная.

Студент должен подготовить краткий доклад по курсовой работе, в котором должен коротко изложить:

особенности своего задания;

способы реализации;

выбор средств реализации;

функциональные особенности и логическую структуру разработанных средств,

а также подтвердить работоспособность программы на практике.

Доклад должен подкрепляться показом соответствующих материалов из курсовой работы и демонстрацией разработанных средств.

По итогам доклада студенту могут быть заданы вопросы, на которые необходимо получить ответы.

Оценка курсовой работы определяется коллегиально членами назначенной комиссии.

Критерии оценивания результатов уровня сформированности компетенции в процессе выполнения и защиты курсовой работы представлены в таблице.

Таблица

Оценочный лист курсовой работы по дисциплине «Криптографические методы и средства защиты информации»

Критерии оценки (компетенции)	Уровень освоения компетенций (оценка в баллах)				Баллы
	эталонный (5)	продвинутый (4)	пороговый (3)	ниже порогового (2)	
Актуальность темы	Актуальность темы работы аргументирована.	Актуальность темы работы сравнительно аргументирована.	Актуальность темы работы недостаточно аргументирована.	Актуальность темы работы не аргументирована.	
Содержание (раскрытие темы, достижение цели, выполнение задач)	Теоретическое содержание темы полностью раскрыто; проведен полный анализ практического материала; аргументированы выводы, обоснованы предложения. Цель достигнута. Задачи выполнены.	Теоретическое содержание темы в основном раскрыто; анализ практического материала недостаточно полный; выводы недостаточно аргументированы, предложения в основном обоснованы. Цель достигнута. Задачи выполнены.	Теоретическое содержание темы раскрыто поверхностно; анализ практического материала не полный; выводы сформулированы в общей форме и не конкретны; неполное обоснование предложений. Цель достигнута частично. Некоторые задачи не выполнены.	Теоретическое содержание темы не раскрыто; достаточно поверхностный анализ практического материала; выводы и предложения не сформулированы. Поставленная цель не достигнута. Задачи не выполнены.	
Сроки вы-	Строгое выполнение	График выполнения	Незначительные	Значительные нару-	

полнения курсовой работы	графика	курсовой работы в основном выполнялся (в 2-х контрольных неделях по 1 баллу)	нарушения графика (в одной контрольной неделе 0 баллов)	шения графика (в 2-х контрольных неделях по 0 баллов)	
Оформление работы	Строго в соответствии с требованиями.	Допущено несколько незначительных неточностей.	Оформление с допустимыми погрешностями.	Значительные нарушения требований.	
Публикации	Имеются публикации по теме работы	<i>При отсутствии публикации проставляется оценка – 0 баллов</i>			
Доклад	Доклад содержателен, логичен; отражает результаты работы, лимит времени не превышен. Студент не читает доклад с листа, показывает высокое владение профессиональным языком.	Доклад относительно содержателен, логичен, в основном отражает результаты работы, лимит времени превышен незначительно. Студент не читает доклад с листа, хорошо владеет профессиональным языком.	Доклад логически не проработан, плохо отражает результаты работы, лимит времени превышен значительно. Студент в основном читает доклад с листа, удовлетворительно владеет профессиональным языком.	Доклад не содержателен, логически не выстроен, не отражает результаты работы, лимит времени превышен значительно. Студент читает доклад с листа, слабо владеет профессиональным языком.	
Презентация	Не повторяет текст доклада, содержит графики, схемы, иллюстрирующие результаты работы. Информация отлично читаема с экрана; цветовое оформление не мешает восприятию информации, текст не содержит ошибок.	Незначительно повторяет текст доклада, содержит графики, схемы, в основном иллюстрирующие результаты работы. Информация хорошо читаема с экрана; цветовое оформление не способствует хорошему восприятию информации, текст не содержит ошибок	Значительно повторяет текст доклада, содержит графики, схемы, недостаточно полно иллюстрирующие результаты работы. Информация удовлетворительно читаема с экрана; цветовое оформление неудачное, текст содержит небольшое количество ошибок	Значительно повторяет текст доклада; содержит в основном текстовые слайды слабо иллюстрирующие результаты работы. Информация плохо читаема с экрана; цветовое оформление мешает восприятию информации, текст содержит большое количество ошибок	
Ответы на вопросы	Ответы правильные, полные, логичные, убедительные; высокое владение профессиональным языком, аргументированная защита своей точки зрения.	Ответы в основном правильные, полные, логичные; хорошее владение профессиональным языком, средняя аргументация и защита своей точки зрения	Не на все вопросы даны полные, логичные ответы; удовлетворительное владение профессиональным языком, низкая способность защиты своей точки зрения	Отсутствие правильных ответов на вопросы; плохое владение профессиональным языком, неспособность защиты своей точки зрения	

Оценочные средства для промежуточной аттестации:

Примеры вопросов к экзамену по дисциплине

1. Криптография. Основные термины и определения. Задачи криптографии. Классификация алгоритмов шифрования
2. Этапы развития криптографии
3. Стеганография
4. Американский стандарт шифрования DES
5. Режимы работы алгоритма DES
6. Симметричная криптосистема AES
7. Российский стандарт шифрования ГОСТ 28147-89
8. Российский стандарт шифрования ГОСТ Р 34.12-2015
9. Шифр одноразового блокнота. Принцип использования ГПСП при поточном шифровании.
10. Шифр RC4
11. Применение современных блочных шифров. Использование шифров потока.
12. Методы повышения криптостойкости симметричных криптосистем
13. Асимметричные системы шифрования. Основной принцип работы. Однонаправленные функции

14. Система шифрования RSA.
15. Криптосистема Эль-Гамала.
16. Криптосистема Рабина.
17. Эллиптические кривые в вещественных числах, эллиптические кривые в полях Галуа
18. Криптография эллиптической кривой, моделирующая криптосистему Эль-Гамала.
19. Хэш-функции. Основные требования и примеры построения.
20. Целостность сообщения. Случайная модель Oracle.
21. Схема Меркеля-Дамгарда.
22. Хеш- функции, основанные на блочных шифрах. Схема Рабина.
23. Алгоритм хеширования SHA
24. Шифр Whirlpool.
25. Российский стандарт хеширования ГОСТ Р 34.11-2012.
26. Электронная цифровая подпись RSA.
27. ЭЦП Эль-Гамала.
28. ЭЦП Шнорра.
29. Стандарт цифровой подписи DSS.
30. Схема ЭЦП эллиптической кривой. Российский стандарт ЭЦП ГОСТ Р 34.10-2012.
31. Аутентификация на основе пароля. Одноразовый пароль.
32. Система установления подлинности «запрос-ответ».
33. Подтверждение с нулевым разглашением. Протокол Фиата-Шамира.
34. Биометрия. Физиологические и поведенческие методы биометрии.
35. Управление ключами. Генерация ключей и хранение ключей. Стандарт ANSI. X9.17.
36. Алгоритм Ниидома-Шредера.
37. Алгоритм безопасного распределения ключей Диффи-Хэллмана
38. Сертификаты открытых ключей.
39. Цели стеганографии. Практическое применение стеганографии. Классификация алгоритмов стеганографии.
40. Цифровые метки. Цифровые водяные знаки. Скрытая передача данных. Защита подлинности документов и авторских прав стеганографическими методами.
41. Методы криптоанализа. Криптоанализ блочных шифров.
42. Частотный криптоанализ.
43. Дифференциальный криптоанализ.
44. Линейный криптоанализ.
45. Интерполяционный криптоанализ.
46. Методы криптоанализа, основанные на слабости ключевых разверток.

Пример практических заданий, выносимых на экзамен, для проверки практических умений и навыков студентов по дисциплине

Задача к билету № 1

Алгоритм шифрования RSA. Пользователь выбирает $P=5$, $Q=9$. Определите, можно ли использовать в качестве открытого ключа E число 11. Если возможно, то определите значение секретного ключа D .

Задача к билету № 2

Для числа $N=7*11$ с помощью функции Эйлера $\varphi(N)$ определите количество положительных целых чисел, меньших N и взаимно простых с N .

Задача к билету № 3

Фраза «КОМПАНИЯ «ЛЮЦИФЕР» ИСПОЛЬЗУЕТ ЕДКИЙ НАТР, ТЯЖЕЛЫЕ ГРУЗИЛА, ОСТРОГУ ТРЕХЗУБУЮ, ОБВЕТШАЛЫЙ ВАТНИК» содержит скрытую информацию. Для сокрытия информации используется стеганографический метод. Прочитайте скрытую информацию.

Задача к билету № 4

Даны восемь чисел: 128, 192, 224, 240, 248, 252, 254, 255. Как расположить эти числа на плоскости, чтобы образовалось два прямоугольных треугольника

Формы промежуточной аттестации по настоящей дисциплине – экзамен.

В филиале используется система с традиционной шкалой оценок – "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", "зачтено", "не зачтено" (далее - пятибалльная система).

Применяемые критерии оценивания по дисциплинам (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23):

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «эталонный».
«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом не принципиальные ошибки. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «продвинутый».
«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «пороговый».
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (непра-

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	<p>вильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля.</p> <p>Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.</p>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

Для проведения лекционных занятий используется учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения практических занятий и занятий лабораторного типа используются учебные аудитории оснащенные специализированной мебелью; доской аудиторной; персональными компьютерами, связанными локальной вычислительной сетью с подключением к сети Интернет и доступом в ЭИОС филиала.

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное специализированной мебелью; доской аудиторной; персональными компьютерами с подключением к сети Интернет и доступом в ЭИОС филиала.

Программное обеспечение

При проведении лекционных занятий предусматривается использование пакета офисных приложений (система для подготовки и проведения презентаций).

При проведении лабораторных и практических работ студентами предусматривается использование .NET Framework и текстового редактора для оформления отчетов.

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;
 - зачёт проводится в устной форме или выполняется в письменной форме на компьютере.
- для глухих и слабослышащих:**

- лекции оформляются в виде электронного документа;
- письменные задания выполняются на компьютере в письменной форме;
- зачёт проводится в письменной форме на компьютере; возможно проведение в форме тестирования.

для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- зачёт проводится в устной форме или выполняется в письменной форме на компьютере;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены филиалом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1 Лапонина О.Р. Криптографические основы безопасности [Электронный ресурс]. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 244 с. — Режим доступа : <http://biblioclub.ru/index.php?page=book&id=429092>.

2 Аверченков В.И. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. — Москва : ФЛИНТА, 2017. — 215 с. — Режим доступа: <https://e.lanbook.com/book/92914..>

3 Кирпичников А.П. Криптографические методы защиты компьютерной информации [Электронный ресурс] : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Казань : КНИТУ, 2016. — 100 с. — Режим доступа: <https://e.lanbook.com/book/101905>.

4. Методические указания к лабораторным работам по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 112 с.

5. Методические указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 8 с.

Дополнительная литература

1 Ищукова Е.А. Криптографические протоколы и стандарты [Электронный ресурс] : учебное пособие / Е.А. Ищукова, Е.А. Лобова. — Таганрог : Издательство Южного федерального университета, 2016. — 80 с. — Режим доступа : <http://biblioclub.ru/index.php?page=book&id=493059>.

2 Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / авт.-сост. И.А. Калмыков, Д.О. Науменко, Т.А. Гиш ; Министерство образования и науки Российской Федерации и др. — Ставрополь : СКФУ, 2015. — 109 с. — Режим доступа : <http://biblioclub.ru/index.php?page=book&id=458059>.

3 Фороузан Б.А. Математика криптографии и теория шифрования [Электронный ресурс] : — 2-е изд., испр. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 511 с. — Режим доступа : <http://biblioclub.ru/index.php?page=book&id=428998>.

4 Рябко Б.Я. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — Москва : Горячая линия-Телеком, 2017. — 230 с. — Режим доступа: <https://e.lanbook.com/book/111097>.

5 Бутакова Н.Г. Криптографические методы защиты информации, учебное пособие [Электронный ресурс] : учебное пособие / Н.Г. Бутакова, Н.В. Федоров. — Санкт-Петербург : ИЦ Интермедия, 2016. — 384 с. — Режим доступа: <https://e.lanbook.com/book/90270>.

6 Стеганографические и криптографические методы защиты информации [Электронный ресурс] : учебное пособие. — Уфа : БГПУ имени М. Акмуллы, 2016. — 112 с. — Режим доступа: <https://e.lanbook.com/book/90963>.

Список авторских методических разработок.

Методическое обеспечение по дисциплине «Криптографические методы и средства защиты информации» включает также следующие авторские разработки преподавателей кафедры вычислительной техники:

1. Методические указания к лабораторным работам по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А.,

Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 112 с.

2. Методические указания по выполнению курсовой работы по дисциплине «Криптографические методы и средства защиты информации» [Электронный ресурс]: электронные методические рекомендации для студентов очной формы обучения (квалификация (степень) «магистр» по направлению 10.04.01 «Информационная безопасность» / Малашенкова И.В., Панкратова Е.А., Федулова С.А. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019. – 8 с.

- комплект лекций в формате мультимедийных презентаций;
- учебно-методические материалы размещены на ресурсах кафедры.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Но- мер из- ме- не- ния	Номера страниц				Всего стра- ниц в доку- менте	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего измене- ния в данный эк- земпляр	Дата внесения из- менения в данный эк- земпляр	Дата введения из- менения
	из- ме- нен- ных	за- ме- нен- ных	но- вых	ан- ну- ли- ро- ванн ых					
1	2	3	4	5	6	7	8	9	10