МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

26.01.2022 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

# *ЦИФРОВЫЕ ТЕХНОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ*

Направление подготовки (специальность)
09.04.01 Информатика и вычислительная техника

Направленность (профиль/специализация) программы
Программное обеспечение для цифровизации предприятий и организаций

Уровень высшего образования - магистратура

Форма обучения
очная

| | |
|---|---|
| Институт/ факультет | Институт энергетики и автоматизированных систем |
| Кафедра | Вычислительной техники и программирования |
| Курс | 2 |
| Семестр | 3 |

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

Рабочая программа рассмотрена и одобрена на заседании кафедры Вычислительной техники и программирования
19.01.2022г. протокол № 4

Зав. кафедрой _____ О.С. Логунова

Рабочая программа одобрена методической комиссией ИЭ и АС
26.01.2022 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры ВТиП, канд. техн. наук _____ Ю.В. Кочержинская

Рецензент:
Начальник отдела технологических платформ ООО "Компас Плюс", канд. техн. наук

_____ Д.С. Сафонов

**Лист актуализации рабочей программы**

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

**1 Цели освоения дисциплины (модуля)**

Дисциплина "Цифровые технологии криптографической защиты информации" содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами , электронной подписью. Объясняется математическая теория, лежащая в основе криптографии (теория групп, полей Галуа, неприводимые многочлены, теория чисел, псевдослучайные последовательности и др.). Ставятся вопросы реализации алгоритмов шифрования и криптоанализа.

**2 Место дисциплины (модуля) в структуре образовательной программы**

Дисциплина Цифровые технологии криптографической защиты информации входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Интеллектуальные системы

Методы и средства высокопроизводительного программирования

Администрирование высоконагруженных систем

Современные проблемы цифровизации предприятий и организаций

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Выполнение и защита выпускной квалификационной работы

**3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения**

В результате освоения дисциплины (модуля) «Цифровые технологии криптографической защиты информации» обучающийся должен обладать следующими компетенциями:

| Код индикатора | Индикатор достижения компетенции |
|---|---|
| ОПК-5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем; | |
| ОПК-5.1 | Определяет необходимость и участвует в разработке и модернизации программного и аппаратного обеспечение информационных и автоматизированных систем |
| ОПК-6 Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования; | |
| ОПК-6.1 | Определяет необходимость в разработке компонент программно-аппаратных комплексов обработки информации и автоматизированного проектирования |

**4. Структура, объём и содержание дисциплины (модуля)**

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 37,15 акад. часов:

– аудиторная – 34 акад. часов;

– внеаудиторная – 3,15 акад. часов;

– самостоятельная работа – 71,15 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

| Раздел/ тема дисциплины | Семестр | Аудиторная контактная работа (в акад. часах) | | | Самостоятельная работа студента | Вид самостоятельной работы | Форма текущего контроля успеваемости и промежуточной аттестации | Код компетенции |
|---|---|---|---|---|---|---|---|---|
| | | Лек. | лаб. зан. | практ. зан. | | | | |
| 1. Основы криптографии | | | | | | | | |
| 1.1 Основные задачи криптосистемы. Симметричные криптосистемы. Блочные и поточные шифры. Алгоритм 3DES. Криптография с открытым ключом. Криптографические хэш-функции | 3 | 2 | 4/2И | | 10 | Повторение основных вопросов по дисциплине "Защита информации". Подготовка к выполнению лабораторной работе. | Дискуссия. Проверка выполнения лабораторной работы. | |
| 1.2 Форматы PIN-блока. Методы проверки PIN. Методы проверки карты. Аутентификация сообщений | | 3 | 4/4И | | 15 | Повторение основных вопросов по дисциплине "Защита информации". Подготовка к выполнению лабораторной работе. | Дискуссия. Проверка выполнения лабораторной работы. | |
| 1.3 Криптографические ключи: иерархия ключей; ключи терминалов; ключи карточных префиксов; хостовые | | 4 | 4/2И | | 11,15 | Подготовка к выполнению лабораторной работе. | Дискуссия. Проверка выполнения лабораторной работы. | |
| Итого по разделу | | 9 | 12/8И | | 36,15 | | | |
| 2. Криптография процессинговой системы | | | | | | | | |
| 2.1 Настройка модуля процессинговой системы: поддерживаемое оборудование; модуль «Криптосервер»; настройка системы | 3 | 4 | 3 | | 20 | Подготовка к выполнению лабораторной работе. | Дискуссия. Проверка выполнения лабораторной работы. | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2.2 Система учета и генерации криптоключей: основные функции; статусы ключей; список ответственных лиц; шаблоны печати открытых компонент; задачи пакетной генерации ключей; пакетные процедуры; операции с ключами | | 4 | 2 | | 15 | Подготовка к выполнению лабораторной работе. | Дискуссия. Проверка выполнения лабораторной работы. | |
| Итого по разделу | | 8 | 5 | | 35 | | | |
| 3. Экзамен | | | | | | | | |
| 3.1 Экзамен | 3 | | | | | Подготовка к экзамену | Экзамен | |
| Итого по разделу | | | | | | | | |
| Итого за семестр | | 17 | 17/8И | | 71,15 | | экзамен | |
| Итого по дисциплине | | 17 | 17/8И | | 71,15 | | экзамен | |

**5 Образовательные технологии**

1. Традиционные образовательные технологии, ориентированные на организацию образовательного процесса и предполагающую прямую трансляцию знаний от преподавателя к студенту.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности стуудентов.

3. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-конференция.

4. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении программных сред и технических средств работы со знаниями в различных предметных областях.

**6 Учебно-методическое обеспечение самостоятельной работы обучающихся**

Представлено в приложении 1.

**7 Оценочные средства для проведения промежуточной аттестации**

Представлены в приложении 2.

**8 Учебно-методическое и информационное обеспечение дисциплины (модуля)**

**а) Основная литература:**

1.Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. Режим доступа: http://znanium.com/bookread.php?book=474838 Электронный ресурс

2.Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. Режим доступа: http://znanium.com/bookread.php?book=432654 Электронный ресурс

**б) Дополнительная литература:**

1. Техническая документация открытой технологической платформы TranzAxis.

2. Ищукова, Е. А. Криптографические протоколы и стандарты: Учебное пособие / Ищукова Е.А., Лобова Е.А. - Таганрог:Южный федеральный университет, 2016. - 80 с.: ISBN 978-5-9275-2066-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/991903 (дата обращения: 26.05.2021). – Режим доступа: по подписке.

**в) Методические указания:**

Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. Режим доступа: http://znanium.com/bookread.php?book=476047 Электронный ресурс

**г) Программное обеспечение и Интернет-ресурсы:**

**Программное обеспечение**

| Наименование ПО | № договора | Срок действия лицензии |
|---|---|---|
| FlowVision | К-93-09 от 19.06.2009 | бессрочно |
| Borland Turbo C++ | №112301 от 23.11.2005 | бессрочно |
| Eclipse | свободно распространяемое ПО | бессрочно |

**Профессиональные базы данных и информационные справочные системы**

| Название курса | Ссылка |
|---|---|
| Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности» | URL: http://www1.fips.ru/ |
| Поисковая система Академия Google (Google Scholar) | URL: https://scholar.google.ru/ |
| Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ) | URL: https://elibrary.ru/project_risc.asp |

**9 Материально-техническое обеспечение дисциплины (модуля)**

Материально-техническое обеспечение дисциплины включает:

1. Лекционная аудитория ауд. 282. Мультимедийные средства хранения, передачи и представления информации.

2. Компьютерные классы Центра информационных технологий ФГБОУ ВО «МГТУ». Персональные компьютеры, объединенные в локальные сети с выходом в Internet, оснащенные современными программно-методическими комплексами для решения задач в области информатики и вычислительной техники.

3. Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки. Все классы УИТ и АСУ с персональными компьютерами, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

4. Аудиторий для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Ауд. 282 и классы УИТ и АСУ.

5. Помещения для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и наличием доступа в электронную информационно-образовательную среду организации. Классы УИТ и АСУ.

6. Помещения для хранения и профилактического обслуживания учебного оборудования. Центр информационных технологий – ауд. 372

**Приложение 1. Учебно-методическое обеспечение самостоятельной работы обучающихся**

По дисциплине «Цифровые технологии криптографической защиты иннформации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа студентов предполагает выполнение лабораторных работ.

Лабораторные работы находятся в электронном источнике:

1. Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. Режим доступа: http://znanium.com/bookread.php?book=476047 Электронный ресурс

**Приложение 2. Оценочные средства для проведения промежуточной аттестации**

**а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:**

| Код индикатора | Индикатор достижения компетенции | Оценочные средства |
|---|---|---|
| ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем; | | |
| ОПК-5.1 | Определяет необходимость и участвует в разработке и модернизации программного и аппаратного обеспечение информационных и автоматизированных систем | Характеристика шифра, определяющая стойкость шифра к дешифрованию без знания ключа, называется<br>1) криптостойкостью<br>2) надежностью<br>3) эффективностью<br>4) уровнем безопасности |
| | | Что позволяет предотвратить использование криптографических преобразований:<br>1) отказ от информации;<br>2) обеспечение аутентификации;<br>3) утечку информации;<br>4) использование алгоритмов асимметричного шифрования. |
| | | Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:<br>1) идентификация и аутентификация пользователей и субъектов доступа;<br>2) управление доступом;<br>3) обеспечение постоянного числа пользователей сети;<br>4) обеспечения целостности;<br>5) регистрация и учет. |
| ОПК-6: Способен разрабатывать компоненты программно-аппаратных комплексов обработки информации и автоматизированного проектирования; | | |
| ПК-6.1 | Определяет необходимость в разработке компонент программно-аппаратных комплексов обработки информации и автоматизированного проектирования | Какой из режимов алгоритма DES используется для построения шифров гаммирования?<br>1) электронная кодовая книга;<br>2) сцепление блоков шифра;<br>3) обратная связь по шифротексту;<br>4) обратная связь по выходу. |
| | | Что означает «многократное шифрование» применительно к блочным шифрам:<br>1) повторное применение алгоритма шифрования к шифротексту с теми же ключами;<br>2) шифрование одного и того же блока открытого текста несколько раз с несколькими ключами;<br>3) повторное применение алгоритма шифрования к шифротексту с другими ключами;<br>4) увеличение числа этапов шифрования открытого текста. |
| | | Что в криптографии понимается под термином «элементарное опробование»:<br>1) операция над двумя «-разрядными двоичными |

| | | |
|---|---|---|
| | | числами;<br>2) проверка ключа на целостность;<br>3) сопоставление двух паролей;<br>4) передача ключа по какому-либо каналу связи. |

**б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:**

Промежуточная аттестация по дисциплине «Цифровые технологии криптографической защиты информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена изучения дисциплины.

Экзамен по дисциплине проводится в устной форме по билетам.

**Показатели и критерии оценивания экзмена:**

– на оценку **«отлично» –** обучающийся показывает высокий уровень сформированности компетенций, т.е. полно раскрыто содержание материала; чётко и правильно даны определения и раскрыто содержание материала; ответ самостоятельный, при ответе использованы знания, приобретённые ранее;

– на оценку **«хорошо» –** обучающийся показывает средний уровень сформированности компетенций, т.е. раскрыто основное содержание материала в объёме; в основном правильно даны определения, понятия; материал изложен неполно, при ответе допущены неточности, нарушена последовательность изложения; допущены небольшие неточности при выводах и использовании терминов; практические навыки нетвёрдые;

– на оценку **«удовлетворительно» –** обучающийся показывает пороговый уровень сформированности компетенций, т.е. усвоено основное содержание материала, но изложено фрагментарно, не всегда последовательно; определения и понятия даны не чётко; практические навыки слабые;

– на оценку **«неудовлетворительно»** – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач