

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Никишкина Татьяна Юрьевна
 Должность: Директор
 Дата подписания: 05.06.2026 15:15:53
 Уникальный программный ключ:
 0a44cc3e5f5bb746f50173cba89718ffd301d635

ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА
Омский институт водного транспорта - филиал Федерального государственного
бюджетного образовательного учреждения высшего образования "Сибирский
государственный университет водного транспорта"

Б1.В.19

Основы криптографии
рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Естественных наук и информационных технологий (ОИВТ)		
Учебный план	ОИВТ-09.03.02.02-ИЦ-26-зфо-26-27.plx		
Образовательная программа	09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ Профиль: Цифровые стартапы		
	год начала подготовки 2026		
Квалификация	бакалавр		
Форма обучения	заочная		
Общая трудоемкость	3 ЗЕТ		
Часов по учебному плану	108	Виды контроля в семестрах: экзамен 5	
в том числе:			
аудиторные занятия	10		
самостоятельная работа	76		
контактная работа во время промежуточной аттестации (ИКР)	4		

Распределение часов дисциплины по курсам

Курс	5		Итого	
	уп	рп		
Вид занятий				
Лекции	4	4	4	4
Лабораторные	6	6	6	6
Иная контактная работа	4	4	4	4
Итого ауд.	10	10	10	10
Контактная работа	14	14	14	14
Сам. работа	76	76	76	76
Часы на контроль	18	18	18	18
Итого	108	108	108	108

Рабочая программа дисциплины

Основы криптографии

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.02 Информационные системы и технологии (приказ Минобрнауки России от 19.09.2017 г. № 926)

составлена на основании учебного плана образовательной программы:

09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

год начала подготовки 2026

Рабочую программу составил(и):

к.ф.-м.н., зав. кафедрой ЕНиИТ, Курнявко Олег Леонидович

Рабочая программа одобрена на заседании кафедры

Заведующий кафедрой Курнявко Олег Леонидович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Целью изучения дисциплины является формирование у обучающихся теоретических знаний и практических навыков в области криптографической защиты информации, необходимых для обеспечения конфиденциальности, целостности, подлинности и доступности данных в современных информационных системах.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Блок. Часть. ООП:		Б1.В
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	Физика	
2.1.2	Инженерная компьютерная графика	
2.1.3	Архитектура ЭВМ	
2.1.4	Web-технологии и стандарты	
2.1.5	Информатика	
2.1.6	Прикладные математические методы	
2.1.7	Теория чисел	
2.1.8	Методы оптимизации	
2.1.9	Дополнительные главы математики	
2.1.10	Дискретная математика	
2.1.11	Линейная алгебра и аналитическая геометрия	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1: Знать: виды ресурсов и ограничений для решения профессиональных задач; основные методы оценки разных способов решения задач; действующее законодательство и правовые нормы, регулирующие профессиональную деятельность

УК-2.2: Уметь: проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности

УК-2.3: Владеть: методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно-правовой документацией.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература и эл. ресурсы	Примечание
	Раздел	Раздел 1. Введение в криптографию				
1.1	Лек	Основные задачи и принципы криптографии /Лек/	5	2	ЛП.1	
1.2	Ср	Исторические шифры /Ср/	5	20	ЛП.1	
1.3	Лаб	Шифр Вижинера /Лаб/	5	2	ЛП.1	
1.4	ИКР	Шифр Вижинера /ИКР/	5	2	ЛП.1	
	Раздел	Раздел 2. Классическая криптография				
2.1	Ср	Криптосистема DES /Ср/	5	20	ЛП.1	
2.2	Ср	Криптосистема AES /Ср/	5	20	ЛП.1	
	Раздел	Раздел 3. Новая (современная) криптография				
3.1	Ср	Элементы теории чисел /Ср/	5	10	ЛП.1	
3.2	Лек	Криптосистема RSA /Лек/	5	2	ЛП.1	

3.3	Ср	Протокол Диффи-Хеллмана /Ср/	5	6	Л1.1	
3.4	Лаб	Криптосистема RSA /Лаб/	5	2	Л1.1	
3.5	Лаб	Протокол электронно-цифровой подписи /Лаб/	5	2	Л1.1	
3.6	ИКР	Протокол электронно-цифровой подписи /ИКР/	5	2	Л1.1	
	Раздел	Раздел 4. Контроль				
4.1	Экзамен	/Экзамен/	5	18	Л1.1	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

1. Кодирование информации
Основные понятия: задачи, объект, предмет, методы криптографической безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации.
2. Симметричное шифрование
Простейшие методы шифрования с закрытым ключом. Общая схема симметричного шифрования. Методы замены. Пропорциональные шифры. Многоалфавитные подстановки. Методы гаммирования. Методы перестановки. Понятие композиционного шифра. Операции, используемые в блочных алгоритмах симметричного шифрования. Структура блочного алгоритма симметричного шифрования. Методы симметричного шифрования. Блочное и потоковое шифрование.
3. Асимметричное шифрование
Основные понятия и классификация средств асимметричной криптографии. Основные свойства асимметричных криптосистем. Предпосылки создания методов шифрования с открытым ключом и основные определения. Односторонние функции. Требования к алгоритмам шифрования с открытым ключом. Использование асимметричных алгоритмов для шифрования. Цифровая подпись на основе алгоритмов с открытым ключом. Генерация и хранение ключей. Формирование секретных ключей с использованием асимметричных алгоритмов. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хеллмана. Алгоритм RSA. Алгоритм Эль-Гамала. Криптографические системы на эллиптических кривых. Возможные атаки при использовании алгоритмов асимметричного шифрования.
4. Электронная подпись
История развития. Виды электронных подписей в Российской Федерации. Общая схема электронной цифровой подписи. Использование хеш-функций. Виды асимметричных алгоритмов цифровой подписи. Электронная подпись на основе алгоритма RSA. Цифровая подпись на основе алгоритма Эль-Гамала. Стандарты на алгоритмы цифровой подписи. Стандарт цифровой подписи ГОСТ Р34.10-94. Новый отечественный стандарт ЭЦП. Управление открытыми ключами.
5. Защита данных в информационных системах
Основные подходы к измерению информации. Энтропия и неопределенность. Норма языка и избыточность сообщений. Понятие совершенно секретной системы. Расстояние единственности.

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Экзамен
Итоговый балл 3 (удовлетворительно), 4(хорошо) или 5 (отлично) соответствует критерию оценивания этапа формирования компетенции «освоен».

Итоговый балл 2 (неудовлетворительно) соответствует критерию оценивания этапа формирования компетенции «не освоен».

Отчеты по лабораторным работам
Итоговая оценка «зачтено» для всех лабораторных работ данного этапа соответствует критерию оценивания этапа формирования компетенций «освоено».

Все остальные случаи соответствуют критерию оценивания этапа формирования компетенций «не освоено».

6.2. Темы письменных работ

6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и (или) навыков

1. Кодирование информации
2. Симметричное шифрование
3. Асимметричное шифрование
4. Электронная подпись
5. Защита данных в информационных системах

6.4. Методические рекомендации к проведению промежуточной аттестации по дисциплине (модулю)

На итоговый контроль выносятся учебный материал, рассмотренный на лекционных и практических занятиях, а также темы, которые представлены для самостоятельного изучения.

Формой проведения итогового контроля по данной дисциплине является экзамен/зачет/дифференцированный зачет, проведение которого может проходить в одном из следующих форматов: устно с использованием билетов в формате беседы, письменно - с использованием билетов, проведение коллоквиума, в формате тестирования, в формате программной

сдачи, по результатам рейтинговых баллов (рейтинговой системы). О форме проведения итогового контроля студенты должны быть оповещены заблаговременно.

1 Методика оценки лабораторных работ

Комплект лабораторных работ по дисциплине направлен на оценку умений и навыков, характеризующих освоение компетенций.

В комплект входят лабораторные работы, каждая из которых оценивается критерием «зачтено» или «не зачтено». Условиями сформированности всех предусмотренных этапов компетенций в процессе освоения образовательной программы в части дисциплины (модуля) является выполнение всех лабораторных работ, соответствующих данному этапу компетенции, на оценку «зачтено». Оценка «зачтено» выставляется обучающемуся, если работа выполнена полностью, правильно оформлен отчет по лабораторной работе. Обучающийся понимает содержание выполненной работы (знает определения понятий, уметь разъяснить значение и смысл любого термина, используемого в работе и т.п.), владеет теоретическим материалом, отсутствуют ошибки при описании теории, формулирует собственные, самостоятельные, обоснованные, аргументированные суждения, допуская незначительные ошибки на дополнительные вопросы. Оценка «не зачтено» выставляется обучающемуся, если работа выполнена полностью, но он не владеет теоретическим материалом, допускает грубые ошибки, испытывает затруднения в формулировке собственных суждений, неспособен ответить на вопросы преподавателя по существу выполненной работы.

2 Методика балльно-рейтинговой системы (БРС) - применяется по усмотрению преподавателя

Сумма баллов, полученных обучающимися в ходе текущего контроля и промежуточной аттестации, составляет оценку результатов освоения дисциплины и переводится в национальный числовой эквивалент (традиционную оценку).

Наименование	Показатель, %
Оценка «отлично»	86...100
Оценка «зачтено»	51...100
Оценка «хорошо»	76...85
Оценка «удовлетворительно»	51...75
Оценка «неудовлетворительно»	0...50

4 Методика оценки дифференцированного зачета по дисциплине

Зачет по дисциплине содержит теоретическую часть, направленную на оценку знаний и практическую часть, направленную на оценку умений и навыков, характеризующих этапы формирования компетенции. Экзаменационный билет содержит два вопроса, охватывающих основные понятия, изучаемые в дисциплине и задачу. Зачет проводится в письменном виде и устной форме - ответы на вопросы. После получения экзаменационного билета обучающемуся предоставляется 60 минут для решения задачи и подготовки к ответам на вопросы билета. Оценка за экзамен выставляется с учетом результатов выполнения теоретической и практической частей в соответствии с приведенными ниже требованиями.

Критерии оценки экзамена по дисциплине

Итоговый балл

5 (отлично)

Процент правильных заданий теоретической части экзамена Обучающийся дает правильные ответы на 2 вопроса, свободно владеет понятийным аппаратом Требования к результатам практической части экзамена

Итоговый балл

4 (хорошо)

Процент правильных заданий теоретической части экзамена Правильный ответ на 1 вопрос и при ответе на 2-ой вопрос обучающийся допускает ошибки принципиального характера, демонстрирует не до конца сформированные компетенции или при ответе на оба вопроса обучающийся допускает непринципиальные неточности при изложении ответов

Требования к результатам практической части экзамена Решение задачи выполнено в полном объеме, но с ошибками не влияющими на алгоритм расчета

Итоговый балл

3 (удовлетворительно)

Процент правильных заданий теоретической части экзамена При ответе на оба вопроса обучающийся допускает ошибки принципиального характера, демонстрирует не до конца сформированные компетенции Требования к результатам практической части экзамена Решение задачи выполнено в неполном объеме

Итоговый балл

2 (неудовлетворительно)

Процент правильных заданий теоретической части экзамена все остальные случаи

Требования к результатам практической части экзамена

все остальные случаи

В спорных случаях преподаватель вправе задавать уточняющие вопросы и давать дополнительные практические задания.

5 Методика оценки экзамена по дисциплине

Экзамен по дисциплине содержит теоретическую часть, направленную на оценку знаний и практическую часть, направленную на оценку умений и навыков, характеризующих этапы формирования компетенции. Экзаменационный билет содержит два вопроса, охватывающих основные понятия, изучаемые в дисциплине. Экзамен проводится в письменном виде и устной форме - ответы на вопросы. После получения экзаменационного билета обучающемуся предоставляется 60

минут для решения задачи и подготовки к ответам на вопросы билета.

Оценка за экзамен выставляется с учетом результатов выполнения теоретической и практической частей в соответствии с приведенными ниже требованиями.

Критерии оценки экзамена по дисциплине

Итоговый балл

5 (отлично)

Процент правильных заданий теоретической части экзамена Обучающийся дает правильные ответы на 2 вопроса, свободно владеет понятийным аппаратом Требования к результатам практической части экзамена

Итоговый балл

4 (хорошо)

Процент правильных заданий теоретической части экзамена Правильный ответ на 1 вопрос и при ответе на 2-ой вопрос обучающийся допускает ошибки принципиального характера, демонстрирует не до конца сформированные компетенции или при ответе на оба вопроса обучающийся допускает не принципиальные неточности при изложении ответов

Требования к результатам практической части экзамена

Итоговый балл

3 (удовлетворительно)

Процент правильных заданий теоретической части экзамена

При ответе на оба вопроса обучающийся допускает ошибки принципиального характера, демонстрирует не до конца сформированные компетенции Требования к результатам практической части экзамена

Итоговый балл

2 (неудовлетворительно)

Процент правильных заданий теоретической части экзамена все остальные случаи

Требования к результатам практической части экзамена все остальные случаи

В спорных случаях преподаватель вправе задавать уточняющие вопросы и давать дополнительные практические задания.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Васильева И. Н.	Криптографические методы защиты информации: учебник и практикум для вузов	М.: Юрайт, 2022

7.3.1 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

7.3.2 Перечень профессиональных баз данных и информационных справочных систем