ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет водного транспорта"

Б1.В.18
Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационных систем**

Образовательная программа 09.03.02 Направление подготовки "Информационные системы и технологии"
Профиль "Проектирование информационных систем и их компонентов"
год начала подготовки 2026

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 56
самостоятельная работа 82

Виды контроля на курсах:
курсовая работа 6
зачет с оценкой 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	15 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	28	28	28	28
Лабораторные	28	28	28	28
Иная контактная работа	6	6	6	6
Итого ауд.	56	56	56	56
Контактная работа	62	62	62	62
Сам. работа	82	82	82	82
Итого	144	144	144	144

Рабочая программа дисциплины

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 Направление подготовки "Информационные системы и технологии"
Профиль "Проектирование информационных систем и их компонентов"
год начала подготовки 2026

Рабочую программу составил(и):

к.т.н., Доцент, Голышев Д.Н.

Рабочая программа одобрена на заседании кафедры

Заведующий кафедрой Моторин Сергей Викторович

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Целью изучения дисциплины является обеспечение базового уровня подготовки обучающихся в области информационной безопасности и защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Инструментальные средства информационных систем
2.1.2	Основы имитационного моделирования
2.1.3	Ситуационное моделирование информационных систем
2.1.4	Web-технологии и стандарты
2.1.5	Архитектура ЭВМ
2.1.6	Инфокоммуникационные системы и сети
2.1.7	Технологии программирования
2.1.8	Управление данными
2.1.9	Алгоритмы и структуры данных
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Информационно-измерительные системы
2.2.2	Методы искусственного интеллекта
2.2.3	Надежность информационных систем
2.2.4	Экономика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-1: Способен к выполнению работ и управлению работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы

ПК-1.5: Разрабатывает прототипы ИС
ПК-1.9: Управляет доступом к данным

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	Законодательные и нормативные документы, между-народные и национальные стандарты в области ин-формационной безопасности и защиты информации
3.1.2	Основные средства реализации криптографической защиты данных (методические и алгоритмические)
3.2	**Уметь:**
3.2.1	Использовать в профессиональной деятельности со-временные криптографические методы
3.2.2	Осуществлять выбор средств реализации криптогра-фической защиты данных: методических и алгоритми-ческих
3.3	**Владеть:**
3.3.1	Способностью использовать программные и аппаратные компоненты для обеспечения информационной безопасности информационных систем
3.3.2	Навыками создания программных средств реализации криптографической защиты данных: шифрование , электронная подпись, выработка ключей, хэширование

4. СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)					
Вид занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Литература**	**ПрПодгот**
Раздел	**Раздел 1. Теория и практика информационной безопасности и защиты информации**				
Лек	Понятие об информационной безопасности и защите информации /Лек/	6	2	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0

Ср	Понятие об информационной безопасности и защите информации /Ср/	6	5	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лек	Криптографическая и стеганографическая защита информации /Лек/	6	8	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лаб	Криптографическая и стеганографическая защита информации /Лаб/	6	8	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1	0
Ср	Криптографическая и стеганографическая защита информации /Ср/	6	16	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лек	Симметричные и асимметричные криптографические методы /Лек/	6	8	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лаб	Симметричные и асимметричные криптографические методы /Лаб/	6	8	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1	0
Ср	Симметричные и асимметричные криптографические методы /Ср/	6	40	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лек	Контроль целостности и подлинности ин-формации /Лек/	6	6	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лаб	Контроль целостности и подлинности ин-формации /Лаб/	6	12	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1	0
Ср	Контроль целостности и подлинности ин-формации /Ср/	6	10	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Лек	Уровни обеспечения информационной безопасности /Лек/	6	4	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
Ср	Уровни обеспечения информационной безопасности /Ср/	6	11	Л1.1Л2.1 Л2.2 Л2.3 Л2.4	0
ИКР	Курсовая работа /ИКР/	6	4	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.2	0
ИКР	Экзамен /ИКР/	6	2	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1	0

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Тема 1 – Понятие об информационной безопасности и защите информации
Лекция 1 –Введение в дисциплину
Содержание и структура понятий, входящих в название дисциплины. Место дисци-плины в ряду других дисциплин направления подготовки. Составляющие информацион-ной безопасности. Уровни обеспечения информационной безопасности.

Тема 2 – Криптографическая и стеганографическая защита информации
Лекция 2 – Криптография. Простейшие методы шифрования
Криптология, криптография и криптоанализ. Модель криптографической системы. Классификация методов шифрования.
История и этапы развития криптографии: крипто-графия древнего периода, арабского мира, эпохи Возрождения.
Лекция 3 – Криптография. Методы шифрования XVII-XIX веков
История и этапы развития криптографии: криптография в XVII–XVIII веках, крип-тография в XIX веке.
Лекция 4 – Криптография. Методы шифрования XX-XXI веков
История и этапы развития криптографии: криптография в первой половине XX ве-ка, криптография во второй половине XX века, криптография в XXI веке (прогноз).
Лекция 5 – Стеганография
История развития стеганографии. Принципы и модель компьютерной стеганогра-фии. Основные методы компьютерной стеганографии.
Лабораторная работа 1 – Простейшие методы шифрования
Лабораторная работа 2 – Совместное использование методов криптографии и стеганографии

Тема 3 – Симметричные и асимметричные криптографические методы
Лекция 6 – Блочные методы шифрования
Типовая структура блочных шифров. Сеть Фейстела. Подстановочно-перестановочная сеть (SP сеть). Стандарты США DES, AES. Режимы работы блочных шифров. Стандарт ГОСТ 28147-89 (шифр «Магма»). Режимы работы ГОСТ 28147-89. Но-вые стандарты на блочные шифры (ГОСТ Р 34.12-2015 – шифр «Кузнечик» и ГОСТ Р 34.13-2015 – «Режимы работы блочных шифров»).
Лекция 7 – Потоковые методы шифрования
Потоковые шифры. Понятие «М-последовательность». Потоковые шифраторы на базе сдвигового регистра с обратной связью. Потоковый шифр А5.
Лекция 8 – Математика асимметричных методов шифрования
Математические основы асимметричной криптографии: теория конечных полей, модульная арифметика и теория чисел.
Лекция 9 – Асимметричные методы шифрования
Модель криптографической системы с открытым ключом. Односторонняя функция. Алгоритм выработки общего ключа Диффи и Хелмана. Задача о рюкзаке и алгоритм шифрования Меркла и Хелмана. Алгоритм шифрования RSA.
Лабораторная работа 3 – Потоковые методы шифрования
Лабораторная работа 4 – Асимметричные методы шифрования

Тема 4 – Контроль целостности и подлинности информации
Лекция 10 – Контроль целостности информации
Задача контроля целостности информации. Код проверки подлинности сообщения (MAC код). Хэширование информации (алгоритмы семейства SHA и ГОСТ Р 34.11) и MDC код. Способы взлома функций хэширования.
Лекция 11 – Контроль подлинности информации
Задача контроля подлинности информации. Алгоритмы выработки и проверки под-писи электронного документа: симметричный метод шифрования, асимметричный метод шифрования и хэш-функция. Стандарты выработки и проверки электронной подписи: стандарт DSS и алгоритм цифровой подписи DSA, стандарты серии ГОСТ Р 34.10. Ран-домизированные и детерминированные электронные подписи.
Лекция 12 – Криптографические протоколы
Понятие о криптографическом протоколе. Идентификация, аутентификация и авто-ризация. Одноразовые пароли. Сервер аутентификации Kerberos. Управление доступом к ресурсам. Протоколы разделения секрета, предсказания бита, подбрасывания монеты, проведения совместных вычислений.
Лабораторная работа 5 – Методы контроля целостности информации
Лабораторная работа 6 – Методы контроля подлинности информации
Лабораторная работа 7 – Криптографические протоколы

Тема 5 – Уровни обеспечения информационной безопасности
Лекция 13 – Законодательный уровень информационной безопасности
Конституция, Федеральные законы о безопасности, информации, информационных технологиях. Государственные стратегии, программы в сфере информационной безопас-ности. Законодательство в области защиты государственной и коммерческой тайны, пер-сональных данных. Законодательство об электронной подписи, механизм её функциони-рования. Лицензирование, стандартизация и сертификация в сфере информационной без-опасности. Наказание за преступления в сфере информационной безопасности. Нацио-нальные стандарты в сфере информационной безопасности и защиты информации.
Лекция 14 – Административный и процедурный уровни информационной без-опасности
Административный уровень информационной безопасности: классификация угроз безопасности, управление рисками, политика безопасности. Процедурный уровень ин-формационной безопасности: программа безопасности (управление персоналом, физиче-ская защита, поддержание работоспособности, реагирования на нарушения безопасности, планирование восстановительных работ).

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Вопросы к практическим работам
Вопросы к лабораторным работам
Вопросы к курсовой работе
Вопросы к экзамену

6.2. Темы письменных работ

Курсовая работа – Блочные методы шифрования:
Тема 3 – Симметричные и асимметричные криптографические методы
1 Вводное занятие (выдача задания, требования по содержанию, объёму и оформлению курсовой работы)
2 Изучение национальных стандартов в области блочного шифрования
3 Разработка сети Фейстеля
4 Проведение алгоритмов блочного шифрования и дешифрования информации
5 Проверка работы алгоритмов
6 Оформление курсовой работы
7 Защита курсовой работы

6.3. Контрольные вопросы и задания

Фонд оценочных средств (материалов)
1 Криптограмма – это синоним …
А) открытого текста Б) закрытого текста* В) ключа
2 Какая группа методов шифрования известна с древних времён?
А) симметричные* Б) асимметричные В) несимметричные
3 Шифр Цезаря относится к категории шифров … замены.
А) многоалфавитной Б) моноалфавитной* В) монофонической
4 Какая следующая буква после лозунга «SSUWT» будет записана в таблицу лозунгового шифра замены?
А) A Б) Z В) неправильный лозунг*
5 В шифре «Тарабарская грамота» буква «А» заменяется на букву …
А) Я Б) Щ В) останется неизменной*
6 Шифр «Двойной квадрат» относится к категории шифров …
А) моноалфавитной замены Б) биграммных* В) перестановки
7 Какой из методов шифрования теоретически считается единственным абсолютно стой-ким к криптоанализу? Ответ: метод «Одноразовый блокнот».
8 Какое количество ключей используется в симметричных криптографических методах? Ответ: 1.
9 Какое количество ключей используется в асимметричных криптографических методах? Ответ: 2.
10 Какой из методов шифрования можно отнести к стеганографическим?
А) квадрат Полибия Б) решетка Кардано* В) метод Виженера
11 На сколько ветвей разбивается входной блок данных в сети Фейстеля? Ответ: 1.
12 В блочных методах шифрования S блок – блок …
А) перестановки Б) подстановки* В) сдвига
13 На сколько ветвей разбивается входной блок данных в подстановочно-перестановочной (SP) сети? Ответ: 1.
14 Основными элементами схемы стандарта шифрования ГОСТ 28147-89 (шифр «Маг-ма») являются …
А) S блок, блок сдвига* Б) S блок, E блок, блок сдвига В) C блок, блок сдвига
15 Какая группа методов шифрования может вырабатывать M-последовательности?
А) блочные Б) потоковые* В) асимметричные
16 Сколько линейных сдвиговых регистров с обратной связью (LFSR) необходимо для построения прореживаемого генератора? Ответ: 1.
17 Назовите результат вычисления выражения $3 + 5 \bmod 7 = \ldots$ Ответ: 1.
18 Назовите результат вычисления выражения $1 - 5 \bmod 13 = \ldots$ Ответ: 9.
19 Назовите результат вычисления выражения $3 \cdot 5 \bmod 11 = \ldots$ Ответ: 4.
20 Назовите результат вычисления выражения $4 / 3 \bmod 5 = \ldots$ Ответ: 3.
21 Назовите результат вычисления выражения $23 \bmod 5 = \ldots$ Ответ: 3.
22 Чему равно значение функции Эйлера для числа 11? Ответ: 10.
23 Какая односторонняя функция лежит в основе метода RSA?
А) деление двух простых чисел Б) умножение двух простых чисел* В) модульное возве-дение в степень
24 Веса рюкзака в алгоритме об укладке рюкзака Меркла и Хелмана равны 1, 5, 6, 11, 14, 20. С его помощью зашифровано сообщение 111001 и получен результат … Ответ: 32.
25 На обеспечение какого свойства информационной безопасности направлена процеду-ра хэширования информации?
А) доступность Б) целостность* В) конфиденциальность
26 Согласно стандарту РФ на функцию хэширования ГОСТ Р 34.11-2012 (функция «Стрибог») длина её хэш-кода … бит. Ответ: 256 или 512 бит.
27 На обеспечение какого свойства информационной безопасности направлен механизм электронной подписи информации?
А) подлинность* Б) целостность В) конфиденциальность
28 Каков размер электронной подписи в битах согласно стандарту РФ на электронную подпись ГОСТ Р 34.10-2012? Ответ: 256 или 512 бит.
29 Каким свойством должны обладать функции, используемые для получения одноразо-вых паролей?
А) чётность Б) обратимость В) односторонность*
30 С помощью меток (классов) конфиденциальности права доступа определяются в рам-ках … модели.
А) мандатной* Б) матричной В) иерархической

Список вопросов к экзамену
1 Понятия, входящие в название дисциплины
2 Составляющие информационной безопасности
3 Уровни обеспечения информационной безопасности
4 Основные понятия криптологии, криптографии и криптоанализа
5 Классификация криптографических методов
6 Криптография древнего периода и арабского мира
7 Криптография в эпоху Возрождения
8 Криптография в XVII–XVIII веках
9 Криптография в XIX веке
10 Криптография в XX и XXI веках
11 Стеганография: история, принципы, методы
12 Блочные шифры. Стандарты DES, AES
13 Блочные шифры. Шифры «Магма», «Кузнечик»
14 Режимы работы блочных шифров

15 Потоковые шифры. Потоковые генераторы на основе сдвигового регистра
16 Асимметричная криптография. Алгоритм Диффи и Хелмана
17 Асимметричная криптография. Алгоритм RSA
18 Асимметричная криптография. Задача об укладке рюкзака и алгоритм Меркла и Хелмана
19 Контроль целостности информации. MAC код
20 Контроль целостности информации. MDC код
21 Функции хэширования семейства SHA
22 Функции хэширования семейства ГОСТ
23 Контроль подлинности информации. Алгоритм выработки и проверки электронной подписи на основе симметричного метода шифрования
24 Контроль подлинности информации. Алгоритм выработки и проверки электронной подписи на основе асимметричного метода шифрования
25 Стандарты выработки и проверки электронной подписи семейства DSS
26 Стандарты выработки и проверки электронной подписи семейства ГОСТ
27 Криптографические протоколы. Идентификация, аутентификация и авторизация
28 Криптографические протоколы. Управление доступом к ресурсам
29 Криптографические протоколы. Задачи разделения секрета и предсказания бита
30 Криптографические протоколы. Задачи подбрасывания монеты и безопасных совместных вычислений

6.4. Методические материалы, определяющие процедуры оценивания

тоговая оценка является арифметической суммой всех баллов, полученных обучающимся в процессе изучения дисциплины. В учёт итоговой оценки по данной методике принимается шкала оценивания каждого вида занятий по дисциплине: лекции, практики, лабораторные работы, семинары и т.д. Преподавателем на первом занятии озвучивается максимальное количество баллов, которое можно получить за данный вид занятий. Вес каждого вида занятий в баллах зависит от их объёма и утверждается на первом заседании кафедры в текущем учебном году.
Методика получения итоговой оценки по 4-х балльной шкале:
5 (отлично) ≥85
4 (хорошо) 75÷84

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

7.1 Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Голышев Дмитрий Николаевич, Моторин Сергей Викторович	Криптографическая защита информации: учеб. пособие	Новосибирск: НГАВТ, 2008

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Полякова Т. А., Чубукова С. Г., Ниесов В. А., Стрельцов А. А.	Организационное и правовое обеспечение информационной безопасности: Учебник и практикум	Москва: Издательство Юрайт, 2019
Л2.2	Суворова Г. М.	Информационная безопасность: учебное пособие для вузов	Москва: Юрайт, 2023
Л2.3	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов	Москва: Юрайт, 2023
Л2.4	Зенков А. В.	Информационная безопасность и защита информации: учебное пособие для вузов	Москва: Юрайт, 2023

7.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Голышев Дмитрий Николаевич	Информационная безопасность и защита информации: метод. указ. к лаб. работам	Новосибирск: НГАВТ, 2007
Л3.2	Голышев Дмитрий Николаевич	Информационная безопасность и защита информации: метод. указ. к курсовой работе	Новосибирск: НГАВТ, 2007

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Назначение	Оборудование
Компьютерный класс - Лаборатория информационных систем - учебная аудитория для проведения лабораторных занятий	Аудиторная доска; Комплект учебной мебели; ПК-9 шт. (в т.ч. преподавательский); Мультимедийное оборудование: проектор, экран, ПК (переносной)
Учебная аудитория для	Аудиторная доска; Комплект учебной мебели

проведения занятий лекционного типа	
Компьютерный класс - Лаборатория информационных систем - учебная аудитория для проведения лабораторных занятий	Аудиторная доска; Комплект учебной мебели; ПК-9 шт. (в т.ч. преподавательский); Мультимедийное оборудование: проектор, экран, ПК (переносной)