



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники



Декан Буднев Н.М.

«02» апреля 2025 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.22 Основы информационной безопасности**

Направление подготовки **09.03.02 Информационные системы и технологии**

Направленность (профиль) подготовки **Электронный и программный инжиниринг**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол № 49 от «26» марта 2025 г.

Председатель Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8 от «24» февраля 2025 г.

И.О. зав. кафедрой Колесник С.Н.

Иркутск 2025 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ	3
II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО	3
III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ	3
IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ	5
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов	5
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине	6
4.3. Содержание учебного материала	8
4.3.1 Перечень семинарских, практических занятий и лабораторных работ	9
4.3.2 Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)	9
4.4. Методические указания по организации самостоятельной работы студентов.....	10
4.5. Примерная тематика курсовых работ	10
V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	10
VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ	11
6.1. Учебно-лабораторное оборудование:	11
6.2. Программное обеспечение:	11
6.3. Технические и электронные средства:	11
VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ	11
VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ	11

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения учебной дисциплины «Информационная безопасность» является формирование у студентов знаний о принципах обеспечения информационной безопасности в информационных сетях.

Задачами освоения учебной дисциплины являются получение:

- знаний об основных видах угроз информационной безопасности,
- знаний о наиболее важных сервисах и механизмах защиты информации,
- навыков работы с программно-аппаратными средствами защиты информации.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность» входит в вариативную часть дисциплин по выбору профессионального цикла ОПОП по направлению 03.03.03 "Радиофизика".

Изучение курса предполагает наличие полученных на предыдущем уровне образования основных знаний по дисциплинам: "Теория информации и базы данных", "Основы цифровой электроники и схемотехники", "Компьютерные вычислительные сети".

Полученные в процессе изучения курса знания и навыки могут быть использованы в процессе выполнения производственной практики и выпускной квалификационной работы, и в дальнейшей профессиональной работе.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **09.03.02 Информационные системы и технологии**.

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

Компетенция	Индикаторы компетенций	Результаты обучения
<i>ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</i>	<i>ИДК_{ОПК-3.3} Выполняет требования информационной безопасности при решении профессиональных задач</i>	Знать: основные виды и типы угроз информационной безопасности, основные способы предотвращения удаленных атак на информационные системы; основные понятия и задачи криптографии, математические модели криптографических систем, основные виды средств криптографической защиты информации Уметь: самостоятельно использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для получения и изучения материалов в области обеспечения информационной безопасности Владеть: навыками применения

		средств криптографической защиты информации для решения задач профессиональной деятельности
--	--	---

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единиц, 108 часов,

Форма промежуточной аттестации: зачёт

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)			Самостоятельная работа	Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися				
					Лекция	Практическое занятие	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Информация как объект защиты	8	4		2	0	0	2	Устный опрос
2	Основные понятия информационной безопасности	8	4		2	0	0	2	Устный опрос
3	Нормативно-правовые основы информационной безопасности в Российской Федерации и международные стандарты информационной безопасности	8	6		2	0	0	4	Устный опрос
4	Угрозы информационной безопасности	8	8,1		2	2	0,1	4	Устный опрос
5	Политика информационной безопасности	8	11,2		2	2	0,2	7	Тестирование
6	Основные понятия криптографии	8	6		2	0	0	4	Устный опрос
7	Простейшие шифры	8	8,1		2	2	0,1	4	Самостоятельная работа

8	Аффинная криптосистема	8	8,1		2	2	0,1	4	Самостоятельная работа
9	Шифр Хилла	8	12,1		2	4	0,1	6	Контрольная работа
10	Система RSA	8	10,1		2	4	0,1	4	Письменный контроль
11	Электронная цифровая подпись	8	10,1		2	4	0,1	4	Самостоятельная работа
12	Хеш-функция	8	12,1		2	4	0,1	6	Контрольная работа

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Информация как объект защиты	повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов самостоятельная подготовка к выполнению практических заданий	Весь семестр	2	Устный опрос	Из перечня литературы
8	Основные понятия информационной безопасности		Весь семестр	2	Устный опрос	
8	Нормативно-правовые основы информационной безопасности в Российской Федерации и международные стандарты информационной безопасности		Весь семестр	4	Устный опрос	
8	Угрозы информационной безопасности		Весь семестр	4	Устный опрос	
8	Политика информационной безопасности		Весь семестр	7	Тестирование	
8	Основные понятия криптографии		Весь семестр	4	Устный опрос	

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Простейшие шифры		Весь семестр	4	Самостоятельная работа	
8	Аффинная криптосистема		Весь семестр	4	Самостоятельная работа	
8	Шифр Хилла		Весь семестр	6	Контрольная работа	
8	Система RSA		Весь семестр	4	Письменный контроль	
8	Электронная цифровая подпись		Весь семестр	4	Самостоятельная работа	
8	Хеш-функция		Весь семестр	6	Контрольная работа	
Общий объем самостоятельной работы по дисциплине (час)				51		

4.3. Содержание учебного материала

Раздел 1. Нормативно-правовые основы информационной безопасности

1. Информация как объект защиты.

Определение информации, свойства информации, уровни представления информации, классификация информации по уровню доступа, классификация информации с точки зрения возможности распространения

2. Основные понятия информационной безопасности

Предметная область и задачи информационной безопасности, составляющие информационной безопасности, средства информационной безопасности

3. Нормативно-правовые основы информационной безопасности в Российской Федерации и международные стандарты информационной безопасности

4. Угрозы информационной безопасности

Определение угроз информационной безопасности, классификация угроз информационной безопасности, классификация источников угроз информационной безопасности, типы атак, модель угроз информационной безопасности

5. Политика информационной безопасности

Основные определения и понятия, аксиомы политики безопасности, формирование политики информационной безопасности

Раздел 2. Основы криптографии

1. Основные понятия криптографии

Предмет и задачи криптографии, основные определения криптографии, криптографические методы защиты информации, регулирование криптографии

2. Простейшие шифры

Шифр подстановки, квадрат Полибия, шифр Атбаш, шифр Цезаря, шифр Тритемиуса, шифр Виженера, шифры перестановки, шифры маршрутной перестановки

3. Аффинная криптосистема

4. Шифр Хилла

5. Система RSA

Алгоритм создания открытого и секретного ключей, алгоритмы шифрования и расшифрования

6. Электронная цифровая подпись

Виды электронной подписи, этапы использования электронной цифровой подписи, алгоритмы формирования и проверки электронной подписи (алгоритм RSA, алгоритм Эль-Гамала), стандарт цифровой подписи DSS, стандарты цифровой подписи в Российской Федерации

7. Хеш-функция

Основные понятия, свойства хеш-функций, применение хеш-функций, виды хеш-функций, стандарты на использование хеш-функций

4.3.1 Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	Раздел 1. Нормативно-правовые основы информационной безопасности	Угрозы информационной безопасности	2		Устный опрос	ОПК-3 ИДК _{ОПК-3.3}
2		Политика информационной безопасности	2		Тестирование	ОПК-3 ИДК _{ОПК-3.3}
3	Раздел 2. Основы криптографии	Простейшие шифры	2		Самостоятельная работа	ОПК-3 ИДК _{ОПК-3.3}
4		Аффинная криптосистема	2		Самостоятельная работа	ОПК-3 ИДК _{ОПК-3.3}
5		Шифр Хилла	4		Контрольная работа	ОПК-3 ИДК _{ОПК-3.3}
6		Система RSA	4		Письменный контроль	ОПК-3 ИДК _{ОПК-3.3}
7		Электронная цифровая подпись	4		Самостоятельная работа	ОПК-3 ИДК _{ОПК-3.3}
8		Хеш-функция	4		Контрольная работа	ОПК-3 ИДК _{ОПК-3.3}

4.3.2 Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	2	3	4	5
1	Информация как объект защиты	- повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов - самостоятельная подготовка к выполнению практических работ.	ОПК-3	ИДК _{ОПК-3.3}
2	Нормативно-правовые основы информационной безопасности в Российской Федерации и международные стандарты информационной безопасности			
3	Угрозы информационной безопасности			

	Политика информационной безопасности			
	Аффинная матричная криптосистема			
	Система RSA			
	Электронная цифровая подпись			
	Хеш-функция			

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа бакалавров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе которой бакалавр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи.

Контроль самостоятельной работы проводится на практических занятиях.

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) перечень литературы

1. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб. : Лань, 2017. — 324 с. (Режим доступа: ЭБС "Лань". - Неогранич. доступ). <https://e.lanbook.com/book/90153>
2. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 252 с. — (Высшее образование). — ISBN 978-5-9916-4299-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/569267>
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2025. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561077>
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2025. — 424 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560426>
5. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2025. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560977>

б) периодические издания

в) список авторских методических разработок

г) базы данных, информационно-справочные и поисковые системы

1. Научная библиотека ИГУ http://library.isu.ru/ru/resources/edu_resources/index.html
2. БД книг и продолжающихся изданий http://ellibnb.library.isu.ru/cgi-bin/irbis64r_15/cgiirbis_64.htm?LNG=&C21COM=F&I21DBN=IRCAT&P21DBN=IRCAT
3. Электронный читальный зал «БиблиоТех» <https://isu.bibliotech.ru/>
4. Электронная библиотечная система «Издательство «Лань» <http://e.lanbook.com>
5. Электронная библиотечная система «РУКОНТ» <http://rucont.ru>

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Экран и проектор для демонстрации видеоматериалов, доска.

6.2. Программное обеспечение:

1. ABBY PDF Transformer 3.0 Пакет из 10 неименных лицензий Per Seat (10лиц.) EDU. Код позиции: AT30-1S1P10-102 Котировка № 03-165-11 от 23.11.2011. Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmс. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmс. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568. Бессрочно.
4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: <http://www.kaspersky.ru/free-antivirus/> . Бессрочно.

6.3. Технические и электронные средства:

Мультимедийный проектор, экран (по необходимости), меловая или маркерная доска.

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

На лекциях используются активные методы обучения (задание вопросов на выяснение понимания наиболее важных моментов излагаемого материала, разработка проектов по отдельным разделам лекционного курса с последующей их защитой). Практические занятия проводятся в интерактивной форме.

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Текущий контроль направлен на выявление сформированности компетенций ОПК-3 и реализуется в виде устного опроса, самостоятельной работы, контрольной работы и тестирования на практических занятиях.

Зачет выставляется по итогам изучения дисциплины в течение семестра при условии положительных результатов по контрольным работам и тестированию.

В случае если во время текущей работы студент выполнил не все контрольные работы и не прошел тестирование, то зачет проводится в устной форме. Зачетный билет содержит два вопроса: первый вопросы по разделу 1, второй вопрос по разделу 2. Для продумывания ответа и, возможно, подготовки письменных набросков ответа студенту дается 20 минут. При оценивании ответа учитывается правильность и полнота ответа на вопросы.

Если замечаний нет или ответ содержит неточности или небольшие ошибки, то выставляется зачет. При низком качестве ответа знания студента оцениваются неудовлетворительно, и ему предлагается прийти на пересдачу зачета.

Пример тестовых заданий для проверки сформированности компетенции ОПК-3:

1. Информация – это
 - а) объект, несущий в себе определенное значение
 - б) материальная сущность, при помощи которой с любой точностью можно описывать любые сущности
 - в) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации
2. Защита информации – это
 - а) деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
 - б) процесс разработки программного продукта для предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий
 - в) нет правильного ответа
3. Что из перечисленного не относится к числу основных аспектов информационной безопасности:
 - а) доступность
 - б) целостность
 - в) защита от копирования
 - г) конфиденциальность
4. Документ, представляющий собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере, называется
 - а) Доктрина информационной безопасности Российской Федерации
 - б) Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности»
 - в) Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
5. Выберите правильное определение термина «криптоанализ»
 - а) криптоанализ – это наука о преодолении криптографической защиты информации
 - б) криптоанализ – это наука, занимающаяся шифрованием данных при передаче по открытым каналам связи
 - в) криптоанализ изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия
6. Как называется функция, которая для строки произвольной длины вычисляет некоторое целое значение или некоторую другую строку фиксированной длины?
 - а) криптографическая функция
 - б) односторонняя функция
 - в) хеш-функция
 - г) функция Эйлера
 - д) функция гаммирования
7. Какие простейшие операции не используются для вычисления хеш-функции по алгоритму MD5?
 - а) возведение в степень
 - б) инверсия
 - в) конъюнкция
 - г) сложение по модулю 2
 - д) получение остатка от деления на большое простое число

- е) циклические сдвиги
8. Что называется хеш-функцией?
- а) функция, позволяющая создать комбинацию бит, служащую для контроля изменений в зашифрованном сообщении
- б) функция, которая позволяет создать электронную цифровую подпись
- в) функция, позволяющая создать контрольную комбинацию бит, служащую для обнаружения искажений в передаваемом сообщении
- функция, которая для строки произвольной длины вычисляет некоторое характерное целое значение или некоторую другую строку фиксированной длины

Разработчик:

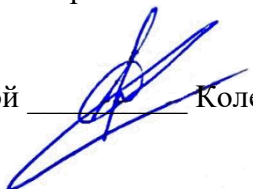


доцент, к.ф.-м.н., Данильчук Е.И.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению и профилю подготовки **09.03.02 Информационные системы и технологии**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «24» февраля 2025 г. протокол № 8

И.О. зав. кафедрой



Колесник С.Н.

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.