

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сибирский государственный индустриальный университет»
Кафедра прикладных информационных технологий и программирования

УТВЕРЖДАЮ
Директор института
информационных технологий и
автоматизированных систем
_____ Л.Д. Павлова
подпись
« ____ » _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография, криптоанализ и защита информации

(* Перечень направлений подготовки (специальностей) и
направленностей (профилей) на следующей странице)

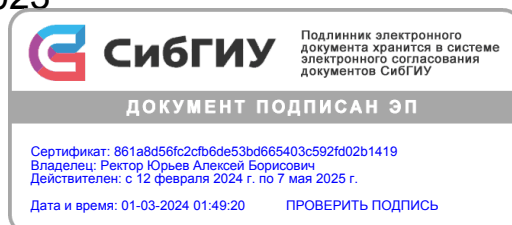
Квалификация выпускника
Бакалавр

Форма обучения
Очная форма

Срок обучения: 4 года

Год начала подготовки 2023

Новокузнецк
2023



Перечень направлений подготовки (специальностей) и направленностей
(профилей):

09.03.01 «Информатика и вычислительная техника»

(направленность (профиль): «Информатика и вычислительная техника»)

09.03.03 «Прикладная информатика»

(направленность (профиль): «Прикладная информатика»)

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

- формирование у обучающихся знаний в области криптографии, криптоанализа и основ информационной безопасности, а также навыков практической защиты информации в организациях.

Задачами учебной дисциплины являются:

- обеспечить знание обучающимися методов и средств криптографии и криптоанализа;
- выработать у обучающихся навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
- научить обучающихся практически решать задачи защиты данных, программ и компьютерных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.01 «Информатика и вычислительная техника», 09.03.03 «Прикладная информатика».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Базы данных;
- Современные технологии программирования;
- Информатика;
- Программирование;
- Обработка и анализ данных;
- Инфокоммуникационные системы и сети.

Учебная дисциплина дополняет знания, умения и навыки, получаемые по одновременно изучаемым и последующим дисциплинам:

- Проектирование информационных систем;
- Архитектура информационных систем;
- Производственные информационные системы;
- Инженерия качества программных продуктов;
- Проектная деятельность 3;
- Преддипломная практика.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

- **Общепрофессиональные компетенции**

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	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	ОПК-3.2 Понимает и использует принципы защиты информации и обеспечивает информационную безопасность	<ul style="list-style-type: none"> – знать: основы информационной безопасности, основные угрозы безопасности, сервисы и механизмы обеспечения информационной безопасности. – уметь: выполнять шифрование и дешифрование текстов и сообщений разными методами, строить модели защищённых компьютерных сетей. – владеть: навыками стандартной защиты компьютерных сред и систем.
ОПК-3.3 Решает поставленные задачи на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий		<ul style="list-style-type: none"> – знать: основы информационной и библиографической культуры, основные электронные ресурсы, их особенности и различия. – уметь: использовать электронные ресурсы и сервисы для поиска информации по защите персональных данных. – владеть: навыками организации технической защиты персональных данных. 	

4 Объем и содержание учебной дисциплины

Учебные занятия по учебной дисциплине проводятся в форме контактной работы и в форме самостоятельной работы обучающихся.

Контактная работа включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия,

практикумы), промежуточную аттестацию обучающихся и иные формы взаимодействия обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации ООП на иных условиях, в том числе при проведении промежуточной аттестации обучающихся. Контактная работа может проводиться с применением электронного обучения, дистанционных образовательных технологий.

Объем учебной дисциплины

Семестр / курс		ИТОГО	7 семестр
Форма промежуточной аттестации			экзамен
Трудоёмкость	<i>академ. час.</i>	144	144
	<i>зачетных единиц</i>	4	4
Лекции, <i>академ. час.</i>		32	32
в форме практической подготовки		0	0
Лабораторные работы, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Практические занятия, <i>академ. час.</i>		32	32
в форме практической подготовки		0	0
Курсовая работа / проект, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Консультации, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Самостоятельная работа, <i>академ. час.</i>		44	44
в форме практической подготовки		0	0
Контроль, <i>академ. час.</i>		36	36
в форме практической подготовки		0	0

Содержание учебной дисциплины

Раздел 1 Базовые понятия информационной безопасности и защиты информационных систем;

Тема 1.1 Понятие информационной безопасности (определение информационной безопасности, основные составляющие информационной безопасности);

Тема 1.2 Основные угрозы информационной безопасности (основные определения и критерии классификации угроз, вредоносное программное обеспечение, каналы утечки информации);

Тема 1.3 Оценочные стандарты информационной безопасности (классификация стандартов, «Оранжевая книга», «Рекомендации X.800», стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»);

Раздел 2 Криптография и криптоанализ;

Тема 2.1 Криптографические шифры (аутентичность сообщений, составные элементы шифра, классификация шифров);

Тема 2.2 Криптография с открытым ключом (симметричные и асимметричные шифры, управление криптографическими ключами, алгоритмы асимметричного шифрования);

Тема 2.3 Криптографические протоколы (основные понятия, разновидности протоколов, протоколы обмена ключами);

Тема 2.4 Криптоанализ (основные понятия, классификация криптоатак, методы криптоанализа);

Раздел 3 Сервисы безопасности;

Тема 3.1 Уровни информационной безопасности (административный уровень, процедурный уровень, программно-технический уровень информационной безопасности);

Тема 3.2 Идентификация и аутентификация (основные понятия, виды идентификации, парольная и биометрическая аутентификация);

Тема 3.3 Протоколирование и аудит (основные понятия протоколирования и аудита, сигнатурный метод выявления подозрительной активности);

Тема 3.4 Управление доступом (логическое управление доступом, методы управления доступом, ролевое управление доступом, управление доступом в Java-среде);

Тема 3.5 Контроль целостности (функция хэширования, электронная цифровая подпись, протоколы контроля целостности);

Тема 3.6 Экранирование (основы экранирования, архитектурная безопасность, межсетевые экраны);

Тема 3.7 Туннелирование и управление (туннелирование пакетов, управление информационной безопасностью, анализ защищённости систем).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Базовые понятия информационной безопасности и защиты информационных систем		
Тема 1.1.	Понятие информационной безопасности	2	
Тема 1.2.	Основные угрозы информационной безопасности	2	
Тема 1.3.	Оценочные стандарты информационной безопасности	2	
Раздел 2.	Криптография и криптоанализ		
Тема 2.1.	Криптографические	4	

	шифры		
Тема 2.2.	Криптография с открытым ключом	2	
Тема 2.3.	Криптографические протоколы	2	
Тема 2.4.	Криптоанализ	4	
Раздел 3.	Сервисы безопасности		
Тема 3.1.	Уровни информационной безопасности	2	
Тема 3.2.	Идентификация и аутентификация	2	
Тема 3.3.	Протоколирование и аудит	1	
Тема 3.4.	Управление доступом	2	
Тема 3.5.	Контроль целостности	4	
Тема 3.6.	Экранирование	2	
Тема 3.7.	Туннелирование и управление	1	
Итого:		32	0

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	Базовые понятия информационной безопасности и защиты информационных систем		
Тема 1.1.	Введение в организацию технической защиты персональных данных	2	
Тема 1.2; Тема 1.3.	Стандартные средства защиты персонального компьютера	6	
Раздел 2.	Криптография и криптоанализ		
Тема 2.1; Тема 2.2; Тема 2.3.	Криптография. Шифры замены и перестановки	6	
Тема 2.4.	Криптоанализ шифров замены и перестановки	8	
Раздел 3.	Сервисы безопасности		
Тема 3.1; Тема 3.2; Тема 3.3; Тема 3.4; Тема 3.5; Тема 3.6; Тема 3.7.	Построение инфраструктуры защищённых компьютерных сетей	10	
Итого:		32	0

7 Перечень тем лабораторных работ

№ раздела / темы дисциплины	Темы лабораторных работ	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
	<i>Отсутствуют</i>		
Итого:		0	0

8 Перечень тем курсовых работ (проектов)

№ раздела / темы дисциплины	Темы курсовых работ (проектов)	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
	<i>Отсутствуют</i>		
Итого:		0	0

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, <i>академ. час</i>	
		всего	в форме практической подготовки
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	14	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию.	14	
Раздел 3.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Прохождение тестирования.	16	
<i>Контроль</i>	<i>Подготовка к экзамену</i>	36	
Итого:		80	0

10 Учебно-методическое и информационное обеспечение учебной дисциплины

а) литература:

1 Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с. — URL: <https://urait.ru/bcode/450998> (дата обращения: 28.04.2023);

2 Запечников, С. В. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2020. — 309 с. — URL: <https://urait.ru/bcode/450538> (дата обращения: 28.04.2023);

3 Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — URL: <https://urait.ru/bcode/470131> (дата обращения: 28.04.2023);

4 Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — URL: <https://urait.ru/bcode/467370> (дата обращения: 28.04.2023).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Консультант студента : электронно-библиотечная система / ООО «КОНСУЛЬТАНТ СТУДЕНТА». — Москва, [200 –]. — URL: <http://www.studentlibrary.ru>. — Режим доступа: для авторизир. пользователей;

2 ЛАНЬ : электронно-библиотечная система : [коллекция «Инженерно-технические науки»] / ООО «Издательство ЛАНЬ». — Санкт-Петербург, [200 –]. — URL: <http://e.lanbook.com>. — Режим доступа: для авторизир. пользователей;

3 НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU : база данных / ООО «НЭБ». — Москва, [200 –]. — URL: <http://elibrary.ru>. — Режим доступа: по подписке;

4 Национальная электронная библиотека (НЭБ) : информационная система / ФГБУ «РГБ». — Москва, [2015 –]. — URL: <http://rusneb.ru>. — Режим доступа: по подписке;

5 Образовательная платформа ЮРАЙТ / ООО «Электронное издательство ЮРАЙТ». — Москва, [200 –]. — URL: <https://urait.ru>. — Режим доступа: для авторизир. пользователей;

6 Университетская библиотека онлайн : электронно-библиотечная система / ООО «Директ-Медиа». — Москва, [200 –]. — URL: <https://biblioclub.ru>. — Режим доступа: для авторизир. пользователей. — URL: <http://www.biblioclub.ru>;

7 Электронная библиотека // Научно-техническая библиотека СибГИУ : сайт. — Новокузнецк, [200 –]. — URL: <http://library.sibsiu.ru/LibrELibraryFullText.asp>. — Режим доступа: для авторизир. пользователей. — URL: <https://library.sibsiu.ru/LibrELibraryFullText.asp>;

8 Электронные периодические издания ИВИС : универсальная база данных / ООО «ИВИС». — Москва, [200 –]. — URL: <http://eivis.ru>. — Режим доступа: по подписке;

9 Электронный каталог : сайт / Научно-техническая библиотека СибГИУ. – Новокузнецк, [199 –]. – URL: <http://libr.sibsiu.ru>. – URL: <https://libr.sibsiu.ru>.

в) лицензионное и свободно распространяемое программное обеспечение:

- Astra Linux Special Edition;
- LibreOffice;
- Microsoft Office;
- Microsoft Windows;
- VirtualBox.

г) базы данных и информационно-справочные системы:

1 ГАРАНТ : справочно-правовая система / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.;

2 КонсультантПлюс : справочно-правовая система / ООО «Информационный центр АНВИК». – Новокузнецк, [199 –]. – Режим доступа: компьютерная сеть библиотеки Сиб. гос. индустр. ун-та.;

3 Техэксперт : информационно-справочная система / ООО «Группа компаний «Кодекс». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть Сиб. гос. индустр. ун-та.

11 Материально-техническое обеспечение учебной дисциплины

Материально-техническое обеспечение учебной дисциплины включает учебные аудитории, оснащенные оборудованием, компьютерной техникой, и техническими средствами обучения, в том числе:

- учебную аудиторию для проведения занятий лекционного типа, оборудованную учебной доской, экраном и мультимедийным проектором;
- учебную аудиторию для проведения занятий семинарского типа (практических занятий), оснащенную компьютерной техникой и периферийными устройствами;
- учебную аудиторию (помещения) для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду, научно-техническую библиотеку СибГИУ.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) 09.03.01 «Информатика и вычислительная техника», 09.03.03 «Прикладная информатика».

Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Приложение

Аннотация рабочей программы дисциплины «Криптография, криптоанализ и защита информации»

по направлению подготовки (специальности)

Перечень направлений подготовки (специальностей) и направленностей
(профилей):

09.03.01 «Информатика и вычислительная техника»

(направленность (профиль): «Информатика и вычислительная техника»)

09.03.03 «Прикладная информатика»

(направленность (профиль): «Прикладная информатика»)

форма обучения – Очная форма

1 Цели и задачи освоения учебной дисциплины

Целями учебной дисциплины являются:

- формирование у обучающихся знаний в области криптографии, криптоанализа и основ информационной безопасности, а также навыков практической защиты информации в организациях.

Задачами учебной дисциплины являются:

- обеспечить знание обучающимися методов и средств криптографии и криптоанализа;
- выработать у обучающихся навыки работы с современными техническими и программно-аппаратными средствами защиты информации;
- научить обучающихся практически решать задачи защиты данных, программ и компьютерных систем.

2 Место учебной дисциплины в структуре ООП по направлению подготовки (специальности)

Учебная дисциплина относится к учебным дисциплинам обязательной части **Блока 1 «Дисциплины (модули)»** ООП по направлению подготовки (специальности) 09.03.01 «Информатика и вычислительная техника», 09.03.03 «Прикладная информатика».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Базы данных;
- Современные технологии программирования;
- Информатика;
- Программирование;
- Обработка и анализ данных;
- Инфокоммуникационные системы и сети.

Учебная дисциплина дополняет знания, умения и навыки, получаемые по одновременно изучаемым и последующим дисциплинам:

- Проектирование информационных систем;

- Архитектура информационных систем;
- Производственные информационные системы;
- Инженерия качества программных продуктов;
- Проектная деятельность 3;
- Преддипломная практика.

3 Планируемые результаты обучения по учебной дисциплине

Процесс изучения учебной дисциплины направлен на формирование следующих компетенций:

– Общепрофессиональные компетенции

Наименование категории (группы) ОПК	Код и наименование ОПК	Код и наименование индикатора достижения ОПК	Планируемые результаты обучения
	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	ОПК-3.2 Понимает и использует принципы защиты информации и обеспечивает информационную безопасность	<ul style="list-style-type: none"> – знать: основы информационной безопасности, основные угрозы безопасности, сервисы и механизмы обеспечения информационной безопасности. – уметь: выполнять шифрование и дешифрование текстов и сообщений разными методами, строить модели защищённых компьютерных сетей. – владеть: навыками стандартной защиты компьютерных сред и систем.
		ОПК-3.3 Решает поставленные задачи на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	<ul style="list-style-type: none"> – знать: основы информационной и библиографической культуры, основные электронные ресурсы, их особенности и различия. – уметь: использовать электронные ресурсы и сервисы для поиска информации по защите персональных

			данных. – владеть: навыками организации технической защиты персональных данных.
--	--	--	--

4 Объем учебной дисциплины

Семестр / курс		ИТОГО	7 семестр
Форма промежуточной аттестации			экзамен
Трудоёмкость	<i>академ. час.</i>	144	144
	<i>зачетных единиц</i>	4	4
Лекции, <i>академ. час.</i>		32	32
в форме практической подготовки		0	0
Лабораторные работы, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Практические занятия, <i>академ. час.</i>		32	32
в форме практической подготовки		0	0
Курсовая работа / проект, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Консультации, <i>академ. час.</i>		0	0
в форме практической подготовки		0	0
Самостоятельная работа, <i>академ. час.</i>		44	44
в форме практической подготовки		0	0
Контроль, <i>академ. час.</i>		36	36
в форме практической подготовки		0	0

5 Краткое содержание учебной дисциплины

В структуре учебной дисциплины выделяются следующие основные разделы (темы):

Раздел 1 Базовые понятия информационной безопасности и защиты информационных систем;

Тема 1.1 Понятие информационной безопасности (определение информационной безопасности, основные составляющие информационной безопасности);

Тема 1.2 Основные угрозы информационной безопасности (основные определения и критерии классификации угроз, вредоносное программное обеспечение, каналы утечки информации);

Тема 1.3 Оценочные стандарты информационной безопасности (классификация стандартов, «Оранжевая книга», «Рекомендации X.800», стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»);

Раздел 2 Криптография и криптоанализ;

Тема 2.1 Криптографические шифры (аутентичность сообщений, составные элементы шифра, классификация шифров);

Тема 2.2 Криптография с открытым ключом (симметричные и асимметричные шифры, управление криптографическими ключами, алгоритмы асимметричного шифрования);

Тема 2.3 Криптографические протоколы (основные понятия, разновидности протоколов, протоколы обмена ключами);

Тема 2.4 Криптоанализ (основные понятия, классификация криптоатак, методы криптоанализа);

Раздел 3 Сервисы безопасности;

Тема 3.1 Уровни информационной безопасности (административный уровень, процедурный уровень, программно-технический уровень информационной безопасности);

Тема 3.2 Идентификация и аутентификация (основные понятия, виды идентификации, парольная и биометрическая аутентификация);

Тема 3.3 Протоколирование и аудит (основные понятия протоколирования и аудита, сигнатурный метод выявления подозрительной активности);

Тема 3.4 Управление доступом (логическое управление доступом, методы управления доступом, ролевое управление доступом, управление доступом в Java-среде);

Тема 3.5 Контроль целостности (функция хэширования, электронная цифровая подпись, протоколы контроля целостности);

Тема 3.6 Экранирование (основы экранирования, архитектурная безопасность, межсетевые экраны);

Тема 3.7 Туннелирование и управление (туннелирование пакетов, управление информационной безопасностью, анализ защищённости систем).

6 Составитель(и):

доцент Пермякова Елена Павловна (кафедра прикладных информационных технологий и программирования).