

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
Проректор по учебной и
воспитательной работе
_____ М.В. Темлянецв
подпись
« ____ » _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптография, криптоанализ и защита информации

09.03.03 «Прикладная информатика»
(направленность (профиль): «Прикладная информатика»)

Квалификация выпускника
Бакалавр

Форма обучения
Очная форма

Срок обучения: 4 года

Год начала подготовки 2021

Новокузнецк
2021

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) 09.03.03 «Прикладная информатика».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Современные СУБД и хранилища данных;
- Математика;
- Содержательные основы прикладной информатики и вычислительной техники;
- Архитектура вычислительных систем;
- Базы данных;
- 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;
- Администрирование систем;
- 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	Код и наименование ОПК	Код и наименование индикатора достиже-	Планируемые результаты
------------------------	------------------------	--	------------------------

(группы) ОПК		ния ОПК	обучения
	<p>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</p>	<p>ОПК-3.2 Использует принципы защиты информации и обеспечивает информационную безопасность в своей профессиональной деятельности</p>	<p>– знать: основы защиты информации, основы криптографии и криптоанализа. – уметь: применять методы и средства защиты компьютерных систем, шифровать сообщения и проводить криптоанализ сообщений, строить защищенную компьютерную сеть. – владеть: методами шифрования и расшифрования, программно-аппаратными средствами компьютерной защиты.</p>
	<p>ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью</p>	<p>ОПК-4.3 Использует российские и международные стандарты и сертификаты качества в области профессиональной деятельности</p>	<p>– знать: основные стандарты в сфере информационной безопасности. – уметь: находить в российских и зарубежных стандартах информацию, необходимую для обеспечения защиты компьютерных систем. – владеть: навыками сравнительного анализа стандартов.</p>
	<p>ОПК-8: Способен принимать участие в управлении проектами создания информационных систем на стадиях жизненного</p>	<p>ОПК-8.4 Разрабатывает требования к информационной безопасности и защите информации в инфокоммуникационных системах и сетях</p>	<p>– знать: основы защиты компьютерных сетей. – уметь: разрабатывать требования к инфор-</p>

	цикла		мационной безопасности и защите информации в сетях. – владеть: программно-аппаратными средствами защиты сетей.
--	-------	--	---

4 Объем и содержание учебной дисциплины

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

Контактная работа обучающихся с педагогическим работником включает в себя занятия лекционного типа (лекции), занятия семинарского типа (семинары, практические занятия, практикумы), промежуточную аттестацию обучающихся и иную контактную работу, предусматривающую групповую или индивидуальную работу обучающихся с педагогическим работником. Контактная работа обучающихся с педагогическим работником может быть аудиторной, внеаудиторной, а также проводиться в электронной информационно-образовательной среде.

Объем учебной дисциплины

Семестр / курс		ИТОГО	7 семестр
Форма промежуточной аттестации			<i>экзамен</i>
Трудоёмкость	<i>академ. час.</i>	144	144
	<i>зачетных единиц</i>	4	4
Лекции, <i>академ. час.</i>		36	36
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>		36	36
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>		36	36
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 (шифры замены и перестановки, блочные, потоковые, шифры гаммирования, квантовые шифры, комбинированные шифры);

Тема 2.2 Криптография с открытым ключом (симметричные и асимметричные шифры, система Диффи-Хелмана, шифры Шамира, Эль-Гамала, RSA);

Тема 2.3 Криптографические протоколы (протоколирование и аудит, разновидности протоколов);

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

Раздел 3 Сервисы безопасности;

Тема 3.1 Уровни информационной безопасности (административный уровень: политика безопасности, программа безопасности, управление рисками, процедурный уровень: управление персоналом, физическая защита, поддержание работоспособности, программно-технический уровень информационной безопасности, архитектурная безопасность);

Тема 3.2 Идентификация и аутентификация (основные понятия, виды идентификации, протоколы аутентификации);

Тема 3.3 Управление доступом (логическое управление доступом, ролевое управление доступом, управление доступом в Java-среде);

Тема 3.4 Контроль целостности (основные понятия, функция хэширования, MD5, электронная цифровая подпись, протоколы контроля целостности);

Тема 3.5 Экранирование и туннелирование (основы экранирования, архитектурная безопасность, межсетевые экраны, анализ защищённости, туннелирование).

5 Перечень тем лекций

№ раздела / темы дисциплины	Темы лекций	Трудоемкость, академ. час	
		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	4	
Раздел 2.	Криптография и криптоанализ		
Тема 2.1.	Криптографические шифры	4	
Тема 2.2.	Криптография с открытым ключом	4	
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.	Управление доступом	4	
Тема 3.4.	Контроль целостности	4	
Тема 3.5.	Экранирование и туннелирование	2	
Итого:		36	0

6 Перечень тем практических занятий (семинаров)

№ раздела / темы дисциплины	Темы практических занятий (семинаров)	Трудоемкость, академ. час	
		всего	в форме практической подготовки
Раздел 1; Тема 1.1; Тема 1.2.	Введение в организацию технической защиты персональных данных	2	
Раздел 1; Тема 1.3.	Стандартные средства защиты персонального компьютера	2	
Раздел 2; Тема 2.1.	Шифрование простой заменой. Криптоанализ шифра простой замены	4	
Раздел 2; Тема 2.2.	Шифрование столбцовой перестановкой. Криптоанализ шифра столбцовой перестановки	4	
Раздел 2; Тема 2.3.	Шифрование двойной перестановкой. Криптоанализ	4	

	шифра двойной перестановки		
Раздел 2; Тема 2.4.	Шифр Виженера. Криптоанализ шифра Виженера	8	
Раздел 3; Тема 3.1; Тема 3.2.	Построение инфраструктуры защищённых компьютерных сетей и настройка механизмов их корректного функционирования и защиты	6	
Раздел 3; Тема 3.3; Тема 3.4; Тема 3.5.	Инструментальный анализ защищенности компьютерных сетей	6	
Итого:		36	0

7 Перечень тем лабораторных работ

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

9 Виды самостоятельной работы

№ раздела / темы дисциплины	Виды самостоятельной работы	Трудоемкость, академ. час	
		всего	в форме практической подготовки
Раздел 1.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Подготовка к текущему контролю.	12	
Раздел 2.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию.	12	

	му занятию; 3. Подготовка к текущему контролю.		
Раздел 3.	1. Изучение лекционного материала; 2. Подготовка к практическому занятию; 3. Подготовка к текущему контролю.	12	
<i>Контроль</i>	<i>Подготовка к экзамену</i>	36	
Итого:		72	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: 21.05.2021);

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: 21.05.2021);

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: 21.05.2021);

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: 21.05.2021);

5 Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 209 с. — URL: <https://urait.ru/bcode/469567> (дата обращения: 21.05.2021);

6 Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2021. — 245 с. — URL: <https://urait.ru/bcode/470279> (дата обращения: 21.05.2021).

б) ресурсы информационно-телекоммуникационной сети «Интернет»:

1 Консультант студента. Электронная библиотека технического ВУЗа : электронно-библиотечная система / ООО «Политехресурс». —

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

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

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

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

в) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office 2010;

– Microsoft Windows 7.

г) базы данных и информационно-справочные системы:

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

2 Система ГАРАНТ : электронный периодический справочник / ООО «Правовой центр «Гарант». – Кемерово, [200 –]. – Режим доступа: компьютерная сеть 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.;

4 Электронный реферативный журнал (ЭлРЖ) : база данных / ВИНТИ РАН. – Москва, [200 –]. – Режим доступа: компьютерная сеть библиотеки 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 периферийным оборудованием;
- 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) 09.03.03 «Прикладная информатика».

Составитель(и):

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

Рабочая программа дисциплины рассмотрена и утверждена на заседании кафедры.

Приложение А

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

по направлению подготовки (специальности)
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) 09.03.03 «Прикладная информатика».

Учебная дисциплина базируется на предварительном усвоении обучающимися учебных дисциплин:

- Современные СУБД и хранилища данных;
- Математика;
- Содержательные основы прикладной информатики и вычислительной техники;
- Архитектура вычислительных систем;
- Базы данных;
- 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;
- Администрирование систем;
- 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 Использует принципы защиты информации и обеспечивает информационную безопасность в своей профессиональной деятельности	– знать: основы защиты информации, основы криптографии и криптоанализа. – уметь: применять методы и средства защиты компьютерных систем, шифровать сообщения и проводить криптоанализ сообщений, строить защищённую компьютерную сеть. – владеть: методами шифрования и расшифрования, программно-аппаратными средствами компьютерной защиты.
	ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.3 Использует российские и международные стандарты и сертификаты качества в области профессиональной деятельности	– знать: основные стандарты в сфере информационной безопасности. – уметь: находить в российских и зарубежных стандартах информацию, необходимую для обеспечения защиты компьютерных систем. – владеть: навы-

			ками сравнительного анализа стандартов.
	ОПК-8: Способен принимать участие в управлении проектами создания информационных систем на стадиях жизненного цикла	ОПК-8.4 Разрабатывает требования к информационной безопасности и защите информации в инфокоммуникационных системах и сетях	– знать: основы защиты компьютерных сетей. – уметь: разрабатывать требования к информационной безопасности и защите информации в сетях. – владеть: программно-аппаратными средствами защиты сетей.

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>		36	36
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>		36	36
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>		36	36
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 (шифры замены и перестановки, блочные, потоковые, шифры гаммирования, квантовые шифры, комбинированные шифры);

Тема 2.2 Криптография с открытым ключом (симметричные и асимметричные шифры, система Диффи-Хелмана, шифры Шамира, Эль-Гамала, RSA);

Тема 2.3 Криптографические протоколы (протоколирование и аудит, разновидности протоколов);

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

Раздел 3 Сервисы безопасности;

Тема 3.1 Уровни информационной безопасности (административный уровень: политика безопасности, программа безопасности, управление рисками, процедурный уровень: управление персоналом, физическая защита, поддержание работоспособности, программно-технический уровень информационной безопасности, архитектурная безопасность);

Тема 3.2 Идентификация и аутентификация (основные понятия, виды идентификации, протоколы аутентификации);

Тема 3.3 Управление доступом (логическое управление доступом, ролевое управление доступом, управление доступом в Java-среде);

Тема 3.4 Контроль целостности (основные понятия, функция хэширования, MD5, электронная цифровая подпись, протоколы контроля целостности);

Тема 3.5 Экранирование и туннелирование (основы экранирования, архитектурная безопасность, межсетевые экраны, анализ защищённости, туннелирование).

6 Составитель(и):

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