МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кафедра анализа данных и искусственного интеллекта

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____Хагуров Т.А
подпись
«02» июня 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД Информационная безопасность

Направление подготовки 54.03.03 Искусство костюма и текстиля
54.03.01 Дизайн
07.03.01 Архитектура

Форма обучения очная, заочная

Квалификация бакалавр

Краснодар 2026

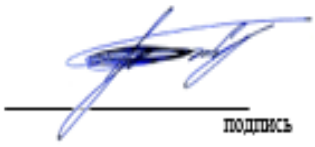
Рабочая программа дисциплины Информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлениям подготовки 54.03.03 Искусство костюма текстиля.

Программу составил(и):
В. И. Грищенко, ст. преподаватель КАДИИ
И.О. Фамилия, должность, ученая степень, ученое звание



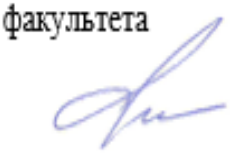
подпись

Рабочая программа дисциплины утверждена на заседании кафедры анализа данных и искусственного интеллекта
протокол № 10 «14» мая 2026 г.
Зав. кафедрой Коваленко А.В.



подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики
протокол № 03 «15» мая 2026 г.
Председатель УМК факультета Добровольская Н.Ю.



подпись

Рецензенты:
Мостовой Евгений Викторович, генеральный директор ООО «Портал-Юг», e-mail: mostovoy@portal-yug.ru

Луценко Евгений Вениаминович, доктор экономических наук, кандидат технических наук, профессор кафедры компьютерных технологий и систем Федерального государственного бюджетное образовательное учреждение высшего образования «Кубанский государственный аграрный университет имени И.Т. Трубилина», e-mail: prof.lutsenko@gmail.com

1. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и задачи дисциплины

Цели изучения дисциплины определены государственным образовательным стандартом высшего образования и соотнесены с общими целями ООП ВО, в рамках которой преподается дисциплина.

Преподавание дисциплины ФТД.01 «Информационная безопасность» строится исходя из требуемого уровня базовой подготовки студентов бакалавриата, обучающихся по направлениям.

В современном мире информационная безопасность является важным аспектом стабильной и успешной работы в различных сферах деятельности человека, предприятий, государств, содружеств и т.д.

Конечными целями преподавания дисциплины являются:

– основы обеспечения компьютерной и сетевой безопасности;

− основы безопасности информационных экономических систем предприятия;

− знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных;

− владение основными алгоритмами математики криптографии;

− знание и использование различных криптосистем шифрования.

Основа изучения дисциплины ФТД.01 «Информационная безопасность» – реализация требований, установленных Федеральным государственным образовательным стандартом высшего профессионального образования к подготовке студентов бакалавриата.

1.2 Задачи дисциплины

– научить студентов использовать в своей практической деятельности различные алгоритмы шифрования;

– ознакомить с компьютерными технологиями в области персональной и сетевой безопасности;

– привить студентам умения и навыки самостоятельного изучения специальной литературы по информационной безопасности.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина ФТД.01 «Информационная безопасность» изучается в 5-м семестре и использует разносторонние знания, полученные в предыдущих семестрах. Преподавание дисциплины ведется в виде лекций, лабораторных и самостоятельных занятий. Большая часть лекционного материала дается в интерактивном режиме. Основнаяцель лабораторных занятий – практическая реализация изученных методов.

Студенты, обучающиеся по данной дисциплине должны владеть навыками логического мышления. Обязательным для них является знание основ безопасности информационных систем. Студент должен уметь использовать навыки работы с алгоритмами защиты информации, технологиями и программами для решения изобретательских и нестандартных задач в области безопасности, в частности безопасности предприятия. Слушатель должен быть ***готов*** использовать знания, полученные в рамках дисциплины ФТД.01 «Информационная безопасность» в своей практической и научно-теоретической деятельности.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
УК 1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	
УК-1.1 Выбирает оптимальный вариант решения задачи, аргументируя свой выбор	Знает типовые алгоритмы выбора решений в стандартных и нестандартных профессиональных ситуациях. Умеет формулировать критерии отбора, релевантные конкретной задаче, и ранжировать их по степени значимости и генерировать не менее 2–3 альтернативных вариантов решения одной задачи. Владеет навыками применения оценочных шкал и чек-листов для сравнения альтернатив.

**Вид индекса индикатора соответствует учебному плану.*

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределениепо видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)
		5
Контактная работа, в том числе:	**34,4**	**34,4**
Аудиторные занятия (всего):	**32**	**32**
Занятия лекционного типа	16	16
Лабораторные занятия	-	-
Занятия семинарского типа (семинары, практические занятия)	16	16
Иная контактная работа:	**2,4**	**2,4**
Контроль самостоятельной работы (КСР)	2	2
Промежуточная аттестация (ИКР)	0,4	0,4
Самостоятельная работа, в том числе:	**37,6**	**37,6**
Курсовая работа	-	-
Проработка учебного (теоретического) материала	17,6	17,6
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	10	10
Подготовка к текущему контролю	10	10
Контроль:	-	-
Подготовка к экзамену	-	-

Общая трудоемкость	**час.**	**72**	**72**
	в том числе контактная работа	**34,4**	**34,4**
	зач. ед	**2**	**2**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 5 семестре

№	Наименование тем	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СР
1	2	3	4	5	6	7
1.	Введение в дисциплину	10	2	2		6
2.	Математика криптографии	10	2	2		6
3.	Алгоритмы шифрования	10	2	2		6
4.	Безопасность информационных систем предприятия	10	2	2		6
5.	Алгоритмы реализации электронно-цифровой подписи	14	4	4		6
6.	Безопасность корпоративной сети	8	2	2		4
7.	Безопасность в клиентско-серверных приложений	7,6	2	2		3,6
	Итого по разделам:	69,6	16	16		**37,6**
	Промежуточная аттестация (ИКР)	0,4				
	Контроль самостоятельной работы (КСР)	**2**				
	Подготовка к экзамену	-				
	ИТОГО по дисциплине	**72**				

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СР – самостоятельная работа студента.Содержание разделов дисциплины**:**

2.2.1 Занятия лекционного типа

№	Наименование темы	Содержание темы	Форма текущего контроля
1	2	3	4
1.	Введение в дисциплину	Информационная безопасность ПК/Предприятия– основные понятия; Криптография - основные понятия, стандартные задачи;	Контрольные вопросы
2.	Математика криптографии	Арифметика целых чисел; Модульная арифметика; Матрицы; Линейное сравнение; Поля Галуа; Простые числа - испытания простоты;	Контрольные вопросы

3.	Алгоритмы шифрования	Основы современных шифров; Стандарт шифрования с симметричным ключом (DES, AES); Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамаля, эллиптических кривых)	Контрольные вопросы.
4.	Безопасность информационных систем предприятия	Законодательство РФ в области защиты информации, обработки персональных данных, организации безопасности информационных систем на предприятии; Службы контроля исполнения законодательства РФ в области безопасности и алгоритмы взаимодействия с ними предприятия; Организация безопасной информационной системы предприятия	Контрольные вопросы
5.	Алгоритмы реализации электронно-цифровой подписи	Криптографические хэш-функции; Цифровая подпись; Установление подлинности объекта	Контрольные вопросы
6.	Безопасность корпоративной сети	Безопасность на транспортном уровне; Безопасность на сетевом уровне;	Контрольные вопросы
7.	Безопасность в клиентско-серверных приложений	Организация защиты клиентско-серверного приложения; Безопасная аутентификация (API)	Контрольные вопросы

2.2.2 Занятия семинарского типа

Занятия семинарского типа не предусмотрены учебным планом.

2.3.3. Лабораторные занятия

	Тематика лабораторных работ	Форма текущего контроля
1	3	4
1.	Практикум по введению в дисциплину	Опрос по теоретическому материалу.
2.	Математика криптографии. Поиск чисел НОД, Алгоритмы Евклида, решение Диофантовых уравнений, Китайская теорема об остатках	Проверка программной реализации рассмотренных алгоритмов
3.	Математика криптографии. Поля Галуа, Многочлены, Примитивность многочлена	Проверка решений практических задач
4.	Алгоритмы шифрования. Стандарт шифрования с симметричным ключом (DES, AES);	Проверка программной реализации рассмотренных алгоритмов
5.	Алгоритмы шифрования. Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамаля, эллиптических кривых)	Проверка программной реализации рассмотренных алгоритмов
6.	Безопасность информационных систем предприятия. Требования по обеспечению информационной безопасности.	Отчет по лабораторной работе.
7.	Безопасность информационных систем предприятия. Обработка персональных данных в организации	Отчет по лабораторной работе.
8.	Безопасность информационных систем предприятия. Обеспечение безопасности персональных данных в организации	Отчет по лабораторной работе.

9.	Алгоритмы реализации электронно-цифровой подписи.	Проверка программной реализации рассмотренных алгоритмов
10.	Безопасность корпоративной сети.	Отчет по лабораторной работе.
11.	Безопасность в клиентско-серверных приложений. Изучение алгоритмов аутентификации.	Отчет по лабораторной работе.

2.3.4 Курсовые работы – не предусмотрены

2.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающегося по дисциплине

Целью самостоятельной работы студента является углубление знаний, полученных в результате аудиторных занятий. Вырабатываются навыки самостоятельной работы. Закрепляются опыт и знания, полученные во время лабораторных занятий.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка и повторение лекционного материала, материала учебной и научной литературы, подготовка к семинарским занятиям	Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
2	Подготовка к лабораторным занятиям	Методические указания по выполнению лабораторных работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
3	Подготовка к решению задач и тестов	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
4	Подготовка докладов	Методические указания для подготовки эссе, рефератов, курсовых работ, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
5	Подготовка к решению расчетно-графических заданий (РГЗ)	Методические указания по выполнению расчетно-графических заданий, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г. Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.
6	Подготовка к текущему контролю	Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры прикладной математики факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №7 от 18.04.2018 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии

В процессе изучения дисциплины лекции, лабораторные занятия, консультации являются ведущими формами обучения в рамках лекционно-семинарской образовательной технологии.

Лекции излагаются в виде презентации с использованием мультимедийной аппаратуры. Данные материалы в электронной форме передаются студентам.

Основной целью лабораторных занятий является разбор практических ситуаций. Дополнительной целью лабораторных занятий является контроль усвоения пройденного материала. На лабораторных занятиях также осуществляется проверка выполнения заданий.

При проведении лабораторных занятий участники закрепляют пройденный материал путем обсуждения вопросов, требующих особого внимания и понимания, отвечают на вопросы преподавателя и других слушателей, осуществляют решения тестов,

направленных на повторение лекционного материала и нормативных документов по изучаемой тематике, выполняют решение задач, которые способствуют развитию практических навыков в области изучаемой дисциплины.

В число видов работы, выполняемой слушателями самостоятельно, входят:

1) поиск и изучение литературы по рассматриваемой теме;

2) поиск и анализ научных статей, монографий по рассматриваемой теме;

3) разработка прикладных программ по рассматриваемой теме.

Интерактивные образовательные технологии, используемые в аудиторных занятиях: при реализации различных видов учебной работы (лекций и практических занятий) используются следующие образовательные технологии: дискуссии, презентации, конференции. В сочетании с внеаудиторной работой они создают дополнительные условия формирования и развития требуемых компетенций обучающихся, поскольку позволяют обеспечить активное взаимодействие всех участников. Эти методы способствуют личностно-ориентированному подходу.

Все перечисленные виды и формы учебной работы и текущего контроля направлены на формирование у обучающихся профессиональных компетенций,предусмотренных при планировании результатов обучения по дисциплине и соотнесенных с планируемыми результатами освоения образовательной программы.

Для инвалидов и лиц с ограниченными возможностями здоровья устанавливается особый порядок освоения указанной дисциплины. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Вышеозначенные образовательные технологии дают наиболее эффективные результаты освоения дисциплины с позиций актуализации содержания темы занятия, выработки продуктивного мышления, терминологической грамотности и компетентности обучаемого в аспекте социально-направленной позиции будущего бакалавра, и мотивации к инициативному и творческому освоению учебного материала.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Освоение дисциплины предполагает две основные формы контроля – текущая и промежуточная аттестация.

Текущий контроль успеваемости осуществляется в течение семестра, в ходе повседневной учебной работы и предполагает овладение материалами лекций, литературы, программы, работу студентов в ходе проведения практических занятий, а также систематическое выполнение тестовых работ, решение практических задач и иных заданий для самостоятельной работы студентов. Данный вид контроля стимулирует у студентов стремление к систематической самостоятельной работе по изучению дисциплины. Он предназначен для оценки самостоятельной работы слушателей по решению задач, выполнению практических заданий, подведения итогов тестирования.Оценивается также активность и качество результатов практической работы на занятиях, участие в дискуссиях, обсуждениях и т.п. Индивидуальные и групповые самостоятельные, аудиторные, контрольные работы по всем темам дисциплины организованы единообразным образом. Для контроля освоения содержания дисциплины используются оценочные средства. Они направлены на определение степени сформированности компетенций.

Промежуточная аттестация студентов осуществляется в рамках завершения изучения дисциплины и позволяет определить качество усвоения изученного материала, предполагает контроль и управление процессом приобретения студентами необходимых знаний, умения и навыков, определяемых по ФГОС ВО по соответствующему направлению подготовки в качестве результатов освоения учебной дисциплины.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

№№ п\п	Код и наименование индикатора	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	**УК-1.1**	Выбирает оптимальный вариант решения задачи, аргументируя свой выбор	Вопросы для устного (письменного) опроса по теме, дискуссия, РМГ, подготовка реферата, эссе, тестирование, решение заданий, коллоквиум, расчетные задания.	Вопрос на зачет: 1-29

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4.1 Оценочные средства для текущего контроля успеваемости

4.1.1. Вопросы контрольного опроса в рамках занятий лекционного и семинарского типа

Контрольные вопросы по темам «Алгоритмы шифрования»

1) Криптоалгоритмы. Общие понятия.
2) Условия Шеннона. Совершенные шифры.
3) Классификация шифров.
4) Классические шифры.

5) Основные компоненты симметричных шифров
6) Шифры Фейстеля, не-Фейстеля.
7) DES
8) AES
9) Российский стандарт шифрования Магма
10) Российский стандарт шифрования Кузнечик
11) Режимы работы симметричных шифров
12) Псевдослучайные последовательности. Линейная конгруэнтная последовательность.
13) Регистр сдвига.
14) Свойства М-последовательности.
15) Тесты NIST качества ПСП
16) Ассиметричное шифрование. Общий подход. Односторонняя и криптографически-односторонняя функция. Общие требования.
17) RSA
18) El-gamal

4.1.2. Комплект тестовых заданий по изучаемой дисциплине

В рамках изучения темы «Безопасность корпоративной сети» проводится тестирование (бланковое). Тесты представляют собой ряд заданий, в которых студенты должны подчеркнуть правильный ответ. Выполнение обучающимся тестовых заданий демонстрирует освоение им необходимых профессиональных компетенций. За каждый правильный ответ выставляется один балл.

Оценка определяется процентом правильных ответов.

Материалы для подготовки к тестированию по теме «Безопасность корпоративной сети»

Задание №1

Установите соответствие

1. Сервер	А) операционные системы и сетевые приложения или сетевые службы
2. Сетевая карта	Б) устройства сети, которое соединяют два отдельных сегмента, ограниченных своей физической длиной, и передают трафик между ними
3. Витая пара	В) специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
4.Коаксиальный кабель	Г) устройство для разделения или объединения нескольких компьютерных сетей
5. Мост	Д) это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
6.Маршрутизатор	Е) специальная плата в корпусе настольного компьютера или ноутбука, позволяющая подключать его в локальную сеть с помощью специального кабеля
7. Рабочая станция	Ж) набор из 8 проводов, скрученных попарно и заключенных в общую изолирующую трубку.
8.Программное обеспечение сетей	З) представляет собой проводник, заключенный в экранирующую оплетку.

Задание № 2
Какой **тип** сетей (**глобальные** или **локальные**) будет использоваться для выполнения

указанных ниже действий?

а) вывод документа на сетевой принтер, расположенный в соседней комнате вашей организации;

б) отправка электронного письма другу из Германии;

в) копирование файла со своего рабочего компьютера на сервер организации;

г) обновление антивирусных баз с сайта разработчика;

д) сетевая компьютерная игра с соседом по подъезду;

е) поиск в Интернет информации о погоде.

Задание № 3

К какому типу сети (локальная или глобальная) относится:

а) сеть, связывающая все административные службы АТП;

б) сеть, объединяющая все университеты России;

в) сеть, объединяющая все оборонные предприятия Урала;

г) сеть, объединяющая все учебные классы Дома творчества школьников?

Задание № 4

Как вы думаете, какой тип локальной сети (одноранговую или сеть с выделенным сервером) и какую конфигурацию удобнее выбрать для:

а) компьютерного класса, где все ученики должны иметь равные возможности связаться с любым другим компьютером;

б) организации, в которой руководитель должен иметь информационную связь с каждым сотрудником, но прямая связь между сотрудниками не допускается;

в) организации со строго иерархическим принципом руководства: директор связан с начальниками отделов, начальники отделов — с руководителями групп, руководители групп — с рядовыми сотрудниками;

г) организации, в которой есть один мощный компьютер с полным набором внешних устройств, выходом в Интернет и множество дешевых компьютеров без периферии на рабочих местах сотрудников.

Выполните задание (правильных ответов может быть несколько)

Перечень компетенций, проверяемых оценочным средством:

ОПК-3 ОПК-8 *Знает* общие принципы построения компьютерных сетей

Критерии оценивания тестовых заданий:

Шкала оценивания результатов тестирования:

«неудовлетворительно» – компетенция не сформирована – выставляется при наличии от 0% до 40% правильных ответов из общего числа предъявленных тестовых заданий;

«удовлетворительно» – обучающийся воспроизводит термины, основные понятия, способен узнавать языковые явления – выставляется при наличии от 51% до 65% правильных ответов из общего числа предъявленных тестовых заданий;

«хорошо» – обучающийся выявляет взаимосвязи, классифицирует, упорядочивает, интерпретирует, применяет на практике пройденный материал – выставляется при наличии от 66% до 85% правильных ответов из общего числа предъявленных тестовых заданий;

«отлично» – обучающийся анализирует, оценивает, прогнозирует, конструирует – выставляется при наличии от 86% до 100% правильных ответов из общего числа предъявленных тестовых заданий студенту выставляется оценка.

4.1.3. Комплект расчетно-графических заданий и расчетных задач

Задачи для подготовки к семинарским занятиям по теме «Математика криптографии»

Задание 1. Введение в теорию чисел
Для данных пар чисел найти НОД
(256,384) (714,218) (516, 438) (735, 525)

Задание 2. Диофантовы уравнения и сравнения первой степени.
Решить заданные Диофантовы уравнения
5x+7y=14 10x+12y=13 14x+27y=49 18x+35y=36
27x+36y=32 54x+48y=128 150x+75y=216 50x+44y=121

Задание 3. Китайская теорема об остатках
Найти решение системы сравнений

$$x=2(\mathrm{mod}\ 5),$$
$$x=15(\mathrm{mod}\ 17),$$
$$x=5(\mathrm{mod}\ 12).$$

Перечень компетенций, проверяемых оценочным средством:

ОПК-3 ОПК-8 *Знает* алгоритмы решений задач математики криптографии. *Владеет* навыками оптимального решения *задач математики криптографии*.

Критерии оценивания разноуровневых заданий и задач:

«неудовлетворительно» – испытывает трудности применения теоретических знаний к решению практических задач; допускает принципиальные ошибки в выполнениитиповых разноуровневых практических заданий;

«удовлетворительно» – применяет теоретические знания к решению практических задач; справляется с выполнением типовых практических задач по известным алгоритмам, правилам, методам;

«хорошо» – правильно применяет теоретические знания к решению практических задач; выполняет типовые практические задания на основе адекватных методов, способов, приемов, решает задачи повышенной сложности, допускает незначительные отклонения;

«отлично» – творчески применяет знания теории к решению практических задач, находит оптимальные решения для выполнения практического задания; свободно выполняет типовые практические задания на основе адекватных методов, способов, приемов; решает задачи повышенной сложности, находит нестандартные решения в проблемных ситуациях.

4.1.4. Контролируемая самостоятельная работа по темам «Стандарт шифрования с симметричным ключом (DES, AES)», «Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамаля, эллиптических кривых)», «Алгоритмы реализации электронно-цифровой подписи»

Компонентом текущего контроля по дисциплине «Информационная безопасность» являются контролируемая самостоятельная работа в виде программирования изученных алгоритмов с привлечением компьютера.

Контролируемая самостоятельная работа определена одной из форм организации обучения, является основой организации образовательного процесса, так как данная форма обучения обеспечивает реализации субъективной позиции студента, требует от него высокой самоорганизации и самостоятельности, формирования у него опыта практической деятельности, а на его основе – овладения профессиональными компетенциями. Контролируемая самостоятельная работа – это планируемая в рамках учебного плана организационно-управленческая деятельность обучающихся по освоению содержания профессиональных компетенций, которая осуществляется по заданию, при методическом

руководстве и контроле преподавателя, но без его непосредственного участия.

Цель контролируемой самостоятельной работы – формирование у обучающихся профессиональных компетенций, обеспечивающих развитие у них способности к самообразованию, самоуправлению и саморазвитию. Специфика контролируемой самостоятельной работы обучающегося как формы обучения заключается в том, что ее основу составляет работа обучающихся над определенным учебным заданием, в специально предоставленное для этого время (на практическом занятии); обучающийся сам выбирает способы выполнения задания, непосредственное фактическое участие преподавателя в руководстве самостоятельной работой отсутствует, но есть опосредованное управление преподавателем самостоятельной познавательной деятельностью обучающихся (на основе инструктажа, консультаций, рекомендаций); обучающиеся сознательно стремятся достигнуть поставленные в задании цели, проявляя свои усилия и выражая в той или иной форме результаты своих действий. Контролируемая самостоятельная работа обладает огромным образовательным потенциалом, поскольку в ее ходе происходит систематизация и закрепление полученных теоретических знаний и практических умений; углубление и расширение теоретических знаний; формирование умения работать с различными видами информации, умения использовать специальную литературу; развиваются познавательные способности и активность обучающихся; формируются такие качества личности, как ответственность и организованность, самостоятельность мышления, способности к саморазвитию, самосовершенствованию и самореализации; воспитывается самостоятельность как личностное качество будущего работника.

Для выполнения контролируемой самостоятельной работы каждому студенту дается 1 индивидуальная задача. Максимальное количество баллов, которое студенты могут получить за правильное решение задачи на контрольной работе, составляет 5 баллов.

Задача для самостоятельной работы к семинарским занятиям по теме «Криптография с асимметричным ключом»

Вариант 1

Реализовать криптосистему RSA для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл

Вариант 2

Реализовать криптосистему El-gamal для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

Вариант 3

Реализовать криптосистему Рабина для шифрования и расшифрования вводимых сообщений. Открытый ключ показывать пользователю, закрытый ключ записывать в файл.

Фонд оценочных средств для проведения промежуточной аттестации

1) Понятие криптосистемы. Основные компоненты и понятия.
2) Криптоалгоритмы. Общие понятия.
3) Условия Шеннона. Совершенные шифры.
4) Классификация шифров.
5) Классические шифры.
6) Основные компоненты симметричных шифров
7) Шифры Фейстеля, не-Фейстеля.
8) DES
9) AES
10) Российский стандарт шифрования Магма
11) Российский стандарт шифрования Кузнечик
12) Режимы работы симметричных шифров
13) Псевдослучайные последовательности. Линейная конгруэнтная последовательность.

14) Регистр сдвига.
15) Свойства М-последовательности.
16) Тесты NIST качества ПСП
17) Ассиметричное шифрование. Общий подход. Односторонняя и криптографически-односторонняя функция. Общие требования.
18) RSA
19) El-gamal
20) Понятие хэш-алгоритмов. Общая структура и классификация.
21) Криптографически стойкий хэш. Коллизии.
22) SHA-512
23) Whirpool
24) Общие понятия электронной цифровой подписи. Фугнкции и область применения.
25) Виды ЭЦП и схемы ЭЦП
26) Правовое обеспечение ЭЦП.
27) Удостоверяющие центры. Структура.
28) Цифровой сертификат. Жизненный цикл.
29) Общая схема протоколов ЭЦП.

Методические рекомендации к сдаче экзамена и критерии оценки ответа

Промежуточная аттестация традиционно служат основным средством обеспечения в учебном процессе «обратной связи» между преподавателем и обучающимся, необходимой для стимулирования работы обучающихся и совершенствования методики преподавания учебных дисциплин.

Итоговой формой контроля сформированности компетенций, обучающихся по дисциплине «Информационная безопасность» является экзамен. Студенты обязаны сдать зачет и экзамен в соответствии с расписанием и учебным планом.

Экзамен по дисциплине преследует цель оценить работу студента за курс, получение теоретических знаний, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы.

Форма проведения экзамена: устно.

Результат сдачи экзамена по прослушанному курсу должен оцениваться как итог деятельности студента в семестре, а именно – по посещаемости лекций, результатам работы на лекционных и практических занятиях, прохождения тестовых заданий, решения расчетно-графических заданий и задач, выполнения контролируемой самостоятельной работы.

Студенту необходимо сдать экзамен. Билет на экзамен включает в себя два теоретических вопроса и одно практическое задание. Преподавателю предоставляется право задавать студентам дополнительные вопросы по всей учебной программе дисциплины. Результат сдачи экзамена заносится преподавателем в ведомость и зачетную книжку.

Критерии оценки экзамена.

«неудовлетворительно» – если студент не знает ответов на вопросы в билете и не выполнил практическое задание, с большими затруднениями отвечает на вопросы преподавателя;

«удовлетворительно» – студент демонстрирует фрагментарные представления о содержании тем билета, усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала, допускается не выполнение практического задания;

«хорошо» – студент демонстрирует общие знания по темам в билете, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения, практическое задание выполнено не менее 50%;

«отлично» – студент демонстрирует глубокие и прочные системные знания потемам билета, исчерпывающе, последовательно, грамотно и логически стройно излагает ответ, не затрудняется с ответом при видоизменении вопроса, умеет самостоятельно обобщать и излагать материал, не допуская ошибок, практическое задание выполнено полностью.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1. Учебная литература

1. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927 (дата обращения: 27.06.2023).;
2. Конституция РФ;
3. Чернова, Е. В. Информационная безопасность человека: учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518441 (дата обращения: 27.06.2023).;
4. Илякова, И. Е. Коммерческая тайна: учебное пособие для вузов / И. Е. Илякова. — Москва: Издательство Юрайт, 2023. — 139 с. — (Высшее образование). — ISBN 978-5-534-14712-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520253 (дата обращения: 27.06.2023).;
5. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512269 (дата обращения: 27.06.2023).

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань», «Юрайт» и др.

5.2. Дополнительная литература:

1. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084 (дата обращения: 27.06.2023).

2. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва: Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519079 (дата обращения: 27.06.2023).

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2023. — 325 с. — (Высшее

образование). — ISBN 978-5-534-03600-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 27.06.2023).

4. Бартош, А. А. Основы международной безопасности. Организации обеспечения международной безопасности: учебное пособие для вузов / А. А. Бартош. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 320 с. — (Высшее образование). — ISBN 978-5-534-11783-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/515578 (дата обращения: 27.06.2023).

5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва: Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239 (дата обращения: 27.06.2023).

6. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях: учебник и практикум для вузов / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 423 с. — (Высшее образование). — ISBN 978-5-534-16546-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531273 (дата обращения: 27.06.2023).

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
4. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
5. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
6. "Лекториум ТВ" http://www.lektorium.tv/
7. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. КиберЛенинка (http://cyberleninka.ru/);
2. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
3. Федеральный портал "Российское образование" http://www.edu.ru/;

4. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
5. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/
.
6. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);
7. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
8. Служба тематических толковых словарей http://www.glossary.ru/;
9. Словари и энциклопедии http://dic.academic.ru/;
10. Образовательный портал "Учеба" http://www.ucheba.com/;
11. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля)

Изучение курса «Информационная безопасность» осуществляется в тесном взаимодействии с другими дисциплинами по программированию. Форма и способы изучения материала определяются с учетом специфики изучаемой темы. Однако во всех случаях необходимо обеспечить сочетание изучения теоретического материала, научного толкования того или иного понятия, даваемого в учебниках и лекциях, с самостоятельной работой студентов, выполнением практических заданий, подготовкой сообщений и докладов.

Лекционное занятие представляет собой систематическое, последовательное, монологическое изложение преподавателем-лектором учебного материала, как правило, теоретического характера. Такое занятие представляет собой элемент технологии представления учебного материала путем логически стройного, систематически последовательного и ясного изложения с использованием образовательных технологий.

Цель лекции – организация целенаправленной познавательной деятельности обучающихся по овладению программным материалом учебной дисциплины. Чтение курса лекций позволяет дать связанное, последовательное изложение материала в соответствии с новейшими данными науки, сообщить слушателям основное содержание предмета в целостном, систематизированном виде.

Задачи лекции заключаются в обеспечении формирования системы знаний по учебной дисциплине, в умении аргументировано излагать научный материал, в формировании профессионального кругозора и общей культуры, в отражении еще не получивших освещения в учебной литературе новых достижений науки, в оптимизации других форм организации учебного процесса.

Для подготовки к лекциям необходимо изучить основную и дополнительную литературу по заявленной теме и обратить внимание на те вопросы, которые предлагаются к рассмотрению в конце каждой темы. При изучении основной и дополнительной литературы, студент может в достаточном объеме усвоить и успешно реализовать конкретные знания, умения, навыки и компетенции при выполнениисследующих условий:

1) систематическая работа на учебных занятиях под руководством преподавателя и

самостоятельная работа по закреплению полученных знаний и навыков;

2) добросовестное выполнение заданий преподавателя на практических занятиях;

3) выяснение и уточнение отдельных предпосылок, умозаключений и выводов, содержащихся в учебном курсе; взаимосвязей отдельных его разделов, используемых методов, характера их использования в практической деятельности менеджера;

4) сопоставление точек зрения различных авторов по затрагиваемым в учебном курсе проблемам; выявление неточностей и некорректного изложения материала в периодической и специальной литературе;

5) разработка предложений преподавателю в части доработки и совершенствования учебного курса;

6) подготовка научных статей для опубликования в периодической печати, выступление на научно-практических конференциях, участие в работе студенческих научных обществ, круглых столах и диспутах по антикоррупционным проблемам.

Лабораторные занятия – являются формой учебной аудиторной работы, в рамках которой формируются, закрепляются и представляются студентами знания, умения и навыки, интегрирующие результаты освоения компетенций как в лекционном формате, так в различных формах самостоятельной работы. К каждому занятию преподавателем формулируются практические задания, требования и методические рекомендации к их выполнению, которые представляются в фонде оценочных средств учебной дисциплины.

В ходе самоподготовки к практическим занятиям студент осуществляет сбор и обработку материалов по тематике его исследования, используя при этом открытые источники информации (публикации в научных изданиях, аналитические материалы, ресурсы сети Интернет и т.п.), а также практический опыт и доступные материалы объекта исследования.

Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на практических (семинарских) занятиях.

Самостоятельная работа студентов по дисциплине «Безопасность информационных систем» проводится с целью закрепления и систематизации теоретических знаний, формирования практических навыков по их применению при решении экономических задач в выбранной предметной области. Самостоятельная работа включает: изучение основной и дополнительной литературы, проработка и повторение лекционного материала, материала учебной и научной литературы, подготовку к практическим занятиям, подготовка к разноуровневым задач и заданиям, а также к контролируемой самостоятельной работе

Самостоятельная работа студентов по данному учебному курсу предполагает поэтапную подготовку по каждому разделу в рамках соответствующих заданий:

Первый этап самостоятельной работы студентов включает в себя тщательное изучение теоретического материала на основе лекционных материалов преподавателя, рекомендуемых разделов основной и дополнительной литературы, материалов периодических научных изданий, необходимых для овладения понятийно-категориальным аппаратом и формирования представлений о комплексе теоретического и аналитического инструментария, используемого в рамках данной отрасли знания.

На втором этапе на основе сформированных знаний и представлений по данному разделу студенты выполняют расчетно-графические задания, нацеленные наформирование умений и навыков в рамках заявленных компетенций. На данном этапе студенты осуществляют самостоятельный поиск эмпирических материалов в рамках конкретного задания, обобщают и анализируют собранный материал по схеме, рекомендованной преподавателем, формулируют выводы, готовят практические рекомендации, материалы для публичного их представления и обсуждения.

Под *контролируемой самостоятельной работой (КСР)* понимают совокупность заданий, которые студент должен выполнить, проработать, изучить по заданию под руководством и контролем преподавателя. Т.е. КСР – это такой вид деятельности, наряду с лекциями, лабораторными и практическими занятиями, в ходе которых студент,

руководствуясь специальными методическими указаниями преподавателя, а также методическими указаниями по выполнению типовых заданий, приобретает и совершенствует знания, умения и навыки, накапливает практический опыт.

Текущий контроль самостоятельной работы студентов осуществляется еженедельно в соответствие с программой занятий Описание заданий для самостоятельной работы студентов и требований по их выполнению выдаются преподавателем в соответствии с разработанным фондом оценочных средств по дисциплине «Безопасность информационных систем».

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты, оснащенные необходимым специализированным оборудованием.

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, ноутбук) и соответствующим программным обеспечением (ПО) Power Point.
2.	Лабораторные занятия	Аудитория оснащенная оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-	Microsoft Windows 8, 10, Microsoft Office Professional Plus

	образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	