

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение высшего  
образования  
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
Факультет компьютерных технологий и прикладной математики

УТВЕРЖДАЮ

Проректор по учебной работе,  
качеству образования – первый  
проректор

честву

Хагуров Т.А.

подпись

«31» мая 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**ФТД.03 «Информационная безопасность»**

Направление подготовки 35.03.08 Водные биоресурсы и аквакультура

Направленность (профиль) Аквакультура

Форма обучения очная

Квалификация бакалавр

Краснодар 2024

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 35.03.08 Водные биоресурсы и аквакультура

Программу составил:

Е.В. Казаковцева, старший преподаватель кафедры анализа данных и искусственного интеллекта



Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры анализа данных и искусственного интеллекта протокол №9 от 20.05.2024

Заведующий кафедрой (разработчика)  
А. В. Коваленко



подпись

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол №3 от «21» мая 2024 г.

Председатель УМК факультета  
А. В. Коваленко



подпись

Рецензенты:

Шапошникова Татьяна Леонидовна.

Доктор педагогических наук, кандидат физико-математических наук, профессор. Почетный работник высшего профессионального образования РФ. Директор института фундаментальных наук (ИФН) ФГБОУ ВО «КубГТУ».

Марков Виталий Николаевич.

Доктор технических наук. Профессор кафедры информационных систем и программирования института компьютерных систем и информационной безопасности (ИКСиИБ) ФГБОУ ВО «КубГТУ».

## 1 Цели и задачи учебной дисциплины(модуля)

**1.1 Цель освоения дисциплины** формирование системных представлений об информационной безопасности, знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных, владение основными алгоритмами математики криптографии.

### 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 «Информационная безопасность» относится к Блоку ФТД. Факультативы.

Для изучения данной дисциплины необходимо знание по предмету «Математические методы в биологии» и закладывание основ для дальнейшего образования посредством курсов «Системы искусственного интеллекта и анализ данных в профессиональной сфере».

### 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: ИОПК-7.6

| Код и наименование индикатора*                                                                                                                               | Результаты обучения по дисциплине                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>ИОПК-7.6 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации;</b> |                                                                                |
| ИПК-07.6.1 Анализирует и оценивает современные цифровые технологии                                                                                           | Знает критерии современных цифровых технологий.                                |
|                                                                                                                                                              | Умеет анализировать и оценивать современные цифровые технологии.               |
|                                                                                                                                                              | Владеть навыками работы с современными цифровыми технологиями                  |
| ИПК-07.6.2 Применяет современные цифровые технологии в информационной безопасности                                                                           | Знает нормы и стандарты информационной безопасности.                           |
|                                                                                                                                                              | Уметь применять современные цифровые технологии в информационной безопасности. |
|                                                                                                                                                              | Владеть навыками работы шифрования данных.                                     |

*\*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 зачетных единиц (72 часа), их

распределение по видам работ представлено в таблице

| Виды работ                                                                                                                                                                                           |                                      | Всего часов | Форма обучения   |                  |                  |               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-------------|------------------|------------------|------------------|---------------|
|                                                                                                                                                                                                      |                                      |             | очная            |                  | очно-заочная     | заочная       |
|                                                                                                                                                                                                      |                                      | ОФО         | 6 семестр (часы) | 7 семестр (часы) | X семестр (часы) | 3 курс (часы) |
| <b>Контактная работа, в том числе:</b>                                                                                                                                                               |                                      | <b>30,2</b> | <b>30,2</b>      | -                | -                | -             |
| <b>Аудиторные занятия (всего):</b>                                                                                                                                                                   |                                      |             |                  |                  |                  |               |
| занятия лекционного типа                                                                                                                                                                             |                                      | 14          | 14               | -                | -                | -             |
| лабораторные занятия                                                                                                                                                                                 |                                      | -           | -                | -                | -                | -             |
| практические занятия                                                                                                                                                                                 |                                      | 14          | 14               | -                | -                | -             |
| <b>Иная контактная работа:</b>                                                                                                                                                                       |                                      |             |                  |                  |                  |               |
| Контроль самостоятельной работы (КСР)                                                                                                                                                                |                                      | 2           | 2                | -                | -                | -             |
| Промежуточная аттестация (ИКР)                                                                                                                                                                       |                                      | 0,2         | 0,2              | -                | -                | -             |
| <b>Самостоятельная работа, в том числе:</b>                                                                                                                                                          |                                      | <b>41,8</b> | <b>41,8</b>      | -                | -                | -             |
| Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, и т.д.) |                                      | 41,8        | 41,8             | -                | -                | -             |
| Подготовка к текущему контролю                                                                                                                                                                       |                                      | -           | -                | -                | -                | -             |
| <b>Контроль:</b>                                                                                                                                                                                     |                                      | -           | -                | -                | -                | -             |
| зачет                                                                                                                                                                                                |                                      | -           | -                | -                | -                | -             |
| <b>Общая трудоемкость</b>                                                                                                                                                                            | <b>час.</b>                          | <b>72</b>   | <b>72</b>        |                  | -                | -             |
|                                                                                                                                                                                                      | <b>в том числе контактная работа</b> | <b>30,2</b> | <b>30,2</b>      |                  | -                | -             |
|                                                                                                                                                                                                      | <b>зач. ед</b>                       | <b>2</b>    | <b>2</b>         |                  | -                | -             |

## 2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 семестре (очная форма обучения)

| №  | Наименование тем                                 | Количество часов |                   |           |          |                            |
|----|--------------------------------------------------|------------------|-------------------|-----------|----------|----------------------------|
|    |                                                  | Всего            | Аудиторная работа |           |          | Внеаудиторная работа<br>СР |
|    |                                                  |                  | Л                 | ПЗ        | ЛР       |                            |
| 1  | 2                                                | 3                | 4                 | 5         | 6        | 7                          |
| 1. | Введение в дисциплину                            | 2                | 2                 | -         | -        |                            |
| 2. | Математика криптографии                          | 8                | 2                 | 2         | -        | 4                          |
| 3. | Алгоритмы шифрования                             | 14               | 2                 | 2         | -        | 10                         |
| 4. | Безопасность информационных систем предприятия   | 12               | 2                 | 2         | -        | 8                          |
| 5. | Алгоритмы реализации электронно-цифровой подписи | 12               | 2                 | 4         | -        | 6                          |
| 6. | Безопасность корпоративной сети                  | 12               | 2                 | 2         | -        | 8                          |
| 7. | Безопасность в клиентско-серверных приложениях   | 9,8              | 2                 | 2         | -        | 5,8                        |
|    | <b>Итого по разделам:</b>                        | <b>69,8</b>      | <b>14</b>         | <b>14</b> | <b>-</b> | <b>41,8</b>                |
|    | Промежуточная аттестация (ИКР)                   | 0,2              |                   |           |          |                            |
|    | Контроль самостоятельной работы (КСР)            | 2                |                   |           |          |                            |
|    | Подготовка к экзамену                            | -                |                   |           |          |                            |
|    | <b>ИТОГО по дисциплине</b>                       | <b>72</b>        |                   |           |          |                            |

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные

занятия, СР – самостоятельная работа студента.

## 2.3 Содержание разделов дисциплины

### 2.3.1 Занятия лекционного типа

| №  | Наименование раздела (темы)                      | Содержание раздела (темы)                                                                                                                                                                                                                                                                                                     | Форма текущего контроля |
|----|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 1  | 2                                                | 3                                                                                                                                                                                                                                                                                                                             | 4                       |
| 1. | Введение в дисциплину                            | Информационная безопасность ПК/Предприятия – основные понятия;<br>Криптография - основные понятия, стандартные задачи;                                                                                                                                                                                                        | Конспект лекции         |
| 2. | Математика криптографии                          | Арифметика целых чисел; Модульная арифметика; Матрицы; Линейное сравнение; Поля Галуа; Простые числа - испытания простоты;                                                                                                                                                                                                    | Конспект лекции         |
| 3. | Алгоритмы шифрования                             | Основы современных шифров;<br>Стандарт шифрования с симметричным ключом (DES, AES);<br>Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамала, эллиптических кривых)                                                                                                                                      | Конспект лекции         |
| 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 | Конспект лекции         |
| 5. | Алгоритмы реализации электронно-цифровой подписи | Криптографические хэш-функции; Цифровая подпись; Установление подлинности объекта                                                                                                                                                                                                                                             | Конспект лекции         |
| 6. | Безопасность корпоративной сети                  | Безопасность на транспортном уровне;<br>Безопасность на сетевом уровне;                                                                                                                                                                                                                                                       | Конспект лекции         |
| 7. | Безопасность в клиентско-серверных приложениях   | Организация защиты клиентско-серверного приложения;<br>Безопасная аутентификация (API)                                                                                                                                                                                                                                        | Конспект лекции         |

### 2.3.2 Занятия семинарского типа (практические / лабораторные работы)

| №  | Наименование раздела (темы)                      | Тематика занятий                                                                                                          | Форма текущего контроля |
|----|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------|
| 1. | Математика криптографии                          | Математика криптографии. Поиск чисел НОД, Алгоритмы Евклида, решение Диофантовых уравнений, Китайская теорема об остатках | Практическое задание    |
| 2. | Алгоритмы шифрования                             | Поля Галуа, Многочлены, Примитивность многочлена                                                                          | Практическое задание    |
| 3. | Безопасность информационных систем предприятия   | Безопасность информационных систем предприятия. Обеспечение безопасности персональных данных в организации                | Практическое задание    |
| 4. | Алгоритмы реализации электронно-цифровой подписи | Алгоритмы реализации электронно-цифровой подписи.                                                                         | Практическое задание    |

|    |                                               |                                                                                    |                      |
|----|-----------------------------------------------|------------------------------------------------------------------------------------|----------------------|
|    | подписи                                       |                                                                                    |                      |
| 5. | Безопасность корпоративной сети               | Безопасность корпоративной сети.                                                   | Практическое задание |
| 6. | Безопасность в клиентско-серверных приложений | Безопасность в клиентско-серверных приложений. Изучение алгоритмов аутентификации. | Практическое задание |

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

### **2.3.2. Лабораторные занятия**

Занятия лабораторного типа не предусмотрены учебным планом.

### **2.3.3 Примерная тематика курсовых работ (проектов)**

Курсовые работы не предусмотрены.

## **2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)**

| № | Вид самостоятельной работы                                                                                                                                                                           | Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 2                                                                                                                                                                                                    | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1 | Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, и т.д.) | Методические указания для подготовки к лекционным и семинарским занятиям, утвержденные на заседании кафедры анализа данных и искусственного интеллекта факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №8 от 18.05.2023 г.<br>Методические указания по выполнению самостоятельной работы, утвержденные на заседании кафедры анализа данных и искусственного интеллекта факультета компьютерных технологий и прикладной математики ФГБОУ ВО «КубГУ», протокол №8 от 18.05.2023 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, применяемые при освоении дисциплины (модуля)**

Для развития и формирования профессиональных навыков студентов в процессе освоения дисциплины предусмотрены традиционные лекции, практические занятия, лабораторные

занятия, аудиторные самостоятельная работа с учебниками и учебными пособиями по основным темам курса.

#### *Лекционные занятия (Л).*

Лекции являются аудиторными занятиями, которые рассчитаны на максимальное использование творческого потенциала слушателей.

Вузовская лекция – главное звено дидактического цикла обучения. Её цель – формирование у обучающихся ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

- изложение материала от простого к сложному, от известного к неизвестному;
- логичность, четкость и ясность в изложении материала;
- возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности обучающихся в ходе лекции;
- опора смысловой части лекции на подлинные факты, события, явления, статистические данные;
- тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью обучающихся;
- научность и информативность (современный научный уровень), доказательность и аргументированность, наличие достаточного количества ярких, убедительных примеров, фактов, обоснований, документов и научных доказательств;
- активизация мышления слушателей, постановка вопросов для размышления, четкая структура и логика раскрытия последовательно излагаемых вопросов;
- разъяснение вновь вводимых терминов и названий, формулирование главных мыслей и положений, подчеркивание выводов, повторение их;
- эмоциональность формы изложения, доступный и ясный язык.

#### *Практические занятия (ПЗ).*

Практические занятия являются также аудиторными, проводятся в виде семинаров по заранее известным темам и предполагают не только обязательную предварительную подготовку, но и активное включение в семинар с помощью современных методов обучения. Они предназначены для более глубокого изучения определенных аспектов лекционного материала и обучения решению проблемных вопросов на практике.

Данный вид занятий предназначены для проведения текущего контроля успеваемости студентов, а также контроля самостоятельной (внеаудиторной) работы в форме опросов, оценки рефератов, презентаций. Время на подготовку к семинарским занятиям предоставляется студенту в соответствии графиком самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

#### **4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации**

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включают контрольные материалы для проведения текущего контроля в форме, практических работ, презентации по проблемным вопросам, разноуровневых заданий, и промежуточной аттестации в форме вопросов к зачету.

#### **Структура оценочных средств для текущей и промежуточной аттестации**

| № п/п | Код и наименование индикатора | Результаты обучения | Наименование оценочного средства |                          |
|-------|-------------------------------|---------------------|----------------------------------|--------------------------|
|       |                               |                     | Текущий контроль                 | Промежуточная аттестация |

|   |                                                                                                                                                      |                                                                                                                                                                                      |                                                                               |                       |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------|
| 1 | ОПК-6.6 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации; | Знает критерии современных цифровых технологий.<br>Умеет анализировать и оценивать современные цифровые технологии.<br>Владеть навыками работы с современными цифровыми технологиями | Вопросы для устного опроса по темам 2-6;<br>практические занятия к темам 2-7. | Вопросы к зачету 1-30 |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-----------------------|

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.

**Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы**

### **Примеры практических заданий (разноуровневые задачи и задания)**

#### **Задание № 1**

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 № 2**

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 № 3

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-6.5 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации

*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.

**Контролируемая самостоятельная работа по темам «Стандарт шифрования с симметричным ключом (DES, AES)», «Криптография с асимметричным ключом (криптосистемы RSA, Рабина, Эль-Гамала, 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.

**Вопросы для подготовки к зачету**

**Примерный перечень вопросов на зачет по дисциплине**

- 1) Криптоалгоритмы. Общие понятия.
- 2) Классификация шифров.
- 3) Классические шифры.
- 4) DES
- 5) AES
- 6) Асимметричное шифрование. Общий подход. Односторонняя и криптографически-односторонняя функция. Общие требования.
- 7) RSA
- 8) El-gamal
- 9) Понятие хэш-алгоритмов. Общая структура и классификация.
- 10) SHA-512
- 11) Общие понятия электронной цифровой подписи. Функции и область применения.

- 12) Виды ЭЦП и схемы ЭЦП
- 13) Правовое обеспечение ЭЦП.
- 14) Удостоверяющие центры. Структура.
- 15) Цифровой сертификат. Жизненный цикл.
- 16) Общая сохема протоколов ЭЦП.
- 17) Алгоритмы построения ЭЦП на основе RSA и El-gamal
- 18) ГОСТ 34.10-2018
- 19) ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
- 20) Свойства информации. Угрозы информационной безопасности.
- 21) Атаки на информационную систему. Понятие и классификация.
- 22) Сетевые атаки.
- 23) Принципы обеспечения информационной безопасности.
- 24) Методы и средства обеспечения ИБ. Общие подходы.
- 25) Понятие несанкционированного доступа. Математическая модель системы управления доступом. Общие термины.
- 26) Механизмы аутентификации пользователей.
- 27) Организация и хранение базы данных учетных записей пользователей.
- 28) Государственное регулирование систем защиты от НСД. Реестры ФСТЭК и ФСБ России.
- 29) Терминология ФСТЭК защиты АС от НСД.
- 30) Уровни защиты и классы защищенности систем защиты от НСД.

### **Методические рекомендации к сдаче зачета 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 зачет. Студенты обязаны сдать зачет в соответствии с расписанием и учебным планом.

Зачет по дисциплине преследует цель оценить работу студента за курс, получение практических знаний, их прочность, развитие творческого мышления, приобретение навыков самостоятельной работы, умение применять полученные знания для решения практических задач и является формой контроля усвоения студентом учебной программы по дисциплине, выполнения практических, контрольных, реферативных работ.

## **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. Периодическая литература**

Не предусмотрена

## **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](http://www.biblioclub.ru)
3. ЭБС «BOOK.ru» <https://www.book.ru>
4. ЭБС «ZNANIUM.COM» [www.znanium.com](http://www.znanium.com)
5. ЭБС «ЛАНЬ» <https://e.lanbook.com>

**Профессиональные базы данных:**

1. Научная электронная библиотека (НЭБ) <http://www.elibrary.ru/>
2. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) <https://rusneb.ru/>
3. 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. Справочно-информационный портал "Русский язык" <http://gramota.ru/>;
2. Служба тематических толковых словарей <http://www.glossary.ru/>;
3. Словари и энциклопедии <http://dic.academic.ru/>;
4. Образовательный портал "Учеба" <http://www.ucheba.com/>;
5. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы [http://xn--273--84d1f.xn--p1ai/voprosy\\_i\\_otvety](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)**

### **Методические рекомендации, определяющие процедуры оценивания самостоятельной работы студентов**

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

В процессе самостоятельной работы студент приобретает навыки самоорганизации, самоконтроля, самоуправления, саморефлексии и становится активным самостоятельным субъектом учебной деятельности.

*Выполняя самостоятельную работу под контролем преподавателя студент должен:*

- освоить минимум содержания, выносимый на самостоятельную работу студентов и предложенный преподавателем в соответствии с Государственными образовательными стандартами высшего профессионального образования.

- планировать самостоятельную работу в соответствии с графиком самостоятельной работы, предложенным преподавателем.

- самостоятельную работу студент должен осуществлять в организационных формах, предусмотренных учебным планом и рабочей программой преподавателя.

- выполнять самостоятельную работу и отчитываться по ее результатам в соответствии с графиком представления результатов, видами и сроками отчетности по самостоятельной работе студентов.

*студент может:*

- сверх предложенного преподавателем (при обосновании и согласовании с ним) и минимума обязательного содержания, определяемого ФГОС ВО:

- самостоятельно определять уровень (глубину) проработки содержания материала;

- предлагать дополнительные темы и вопросы для самостоятельной проработки;

- в рамках общего графика выполнения самостоятельной работы предлагать обоснованный индивидуальный график выполнения и отчетности по результатам самостоятельной работы;

- предлагать свои варианты организационных форм самостоятельной работы;

- использовать для самостоятельной работы методические пособия, учебные пособия, разработки сверх предложенного преподавателем перечня;

- использовать не только контроль, но и самоконтроль результатов самостоятельной работы в соответствии с методами самоконтроля, предложенными преподавателем или выбранными самостоятельно.

Самостоятельная работа студентов должна оказывать важное влияние на формирование личности будущего специалиста, она планируется студентом самостоятельно. Каждый студент самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием по каждой дисциплине. Он выполняет внеаудиторную работу по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Изучение дисциплины «Информационная безопасность» осуществляется в форме учебных занятий под руководством профессорско-преподавательского состава кафедры и самостоятельной подготовки обучающихся. Основными видами учебных занятий по изучению данной дисциплины являются: лекционное занятие; практическое занятия; консультация преподавателя (индивидуальная, групповая). При проведении учебных занятий используются элементы классических и современных педагогических технологий.

Предусматриваются следующие формы работы обучающихся:

- прослушивание лекционного курса;
- чтение и конспектирование рекомендованной литературы;
- проведение практических занятий,
- проведение лабораторных занятий.

Внеаудиторная работа предполагает выполнение индивидуальных и групповых заданий по дисциплине, а также самостоятельную работу студентов. Индивидуальные занятия предполагают работу каждого студента по индивидуальному (групповому) заданию и личный устный/письменный отчет и презентацию результатов группе и преподавателю во время практических занятий.

#### **Методические рекомендации, определяющие процедуры оценивания практических занятий**

Одной из важных форм самостоятельной работы является подготовка к практическому занятию. При подготовке к практическим занятиям студент должен придерживаться следующей технологии:

1. внимательно изучить основные вопросы темы и план практического занятия, определить место темы занятия в общем содержании, ее связь с другими темами;
2. найти и проработать соответствующие разделы в рекомендованных нормативных документах, учебниках и дополнительной литературе;
3. после ознакомления с теоретическим материалом ответить на вопросы для самопроверки;
4. продумать свое понимание сложившейся ситуации в изучаемой сфере, пути и способы решения проблемных вопросов;
5. продумать развернутые ответы на предложенные вопросы темы, опираясь на лекционные материалы, расширяя и дополняя их данными из учебников, дополнительной литературы.

#### **Критерии оценки:**

**оценка «зачтено»** ставится студенту, продемонстрировавшему:

- глубокие знания всего программного материала, логически последовательные, полные, грамматически правильные и конкретные ответы на вопросы по теме;
- твёрдые и достаточно полные знания материала, последовательные, правильные, конкретные ответы на поставленные вопросы при свободном реагировании на замечания по отдельным вопросам;
- знание и понимание основных вопросов программы, наличие ошибок при недостаточной способности их корректировки, наличие определенного количества (не более 50%) ошибок в освещении отдельных вопросов;

**оценка «незачтено»** ставится студенту, продемонстрировавшему:

- непонимание сущности излагаемых вопросов, грубые ошибки в ответе, неуверенные и неточные ответы на дополнительные вопросы преподавателя.

#### **Методические рекомендации, определяющие процедуру оценивания презентации**

1. Презентация – это сжатое изложение информации по проблеме, актуальной для профессиональной деятельности.
2. Подготовка презентации предполагает сбор информации по проблеме из различных источников, анализ полученных данных и их обобщенное изложение в виде слайдов. Доклад по подготовленной презентации исключает дословное чтение слайдов.
3. Презентация составляется в программе Microsoft Power Point (версия 2003 и др.).

4. Количество слайдов определяется структурой ответа на вопрос, сформулированный в теме.
5. Слайды оформляются в единой цветовой гамме, оформление определяется одним из форматов, предлагаемых конструктором программы.
6. Фотографии и рисунки непременно подписываются. Если студент не является автором текста, а приводит его дословно или в пересказе, пользуется статистическими данными, то необходимо привести библиографическое описание источника с указанием автора/авторов, дать ссылку на страницы цитируемого издания, указать электронный адрес материала в сети Интернет.
7. Список источников и материалов из сети Интернет оформляется в соответствии с нормами составления библиографического описания (см. методические указания к оформлению курсовых и дипломных работ)

#### *Структура презентации (типовая)*

- 1) Тема – слайд 1
- 2) Цель и задачи презентации – слайд 2
- 3) Структура презентации (содержание, где после названия раздела указывается номер слайда/слайдов) – слайд 3 (3-4, если разделов много)
- 4) Название раздела – слайд 5 (6)
- 5) Серия слайдов к разделу, таблицы, схемы графики приводятся на отдельных слайдах и непременно озаглавливаются, если используются материалы из других источников, это указывается в примечаниях к слайду – слайды 7-10 (7-...). В случаях сравнения, сопоставления данных «до» и «после», приведение динамических показателей роста/снижения чего-либо слова и фразы заменяются символами (пиктограммами, рисунками).
- 6) Слайды следующего раздела ...
- 7) Список источников (оформляется в соответствии с правилами: см. методические указания к оформлению курсовых и дипломных работ, ГОСТ 2003 г.)
- 8) Сведения об авторе презентации (не приветствуется шумовой эффект аплодисментов, художественное фото автора)

#### *Матрица оценки презентации (до 50 баллов)*

| №<br>п/п | Критерий                                                                                                                                       | Максимальное количество баллов |   |   |   |   |   |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|---|---|---|---|---|
|          |                                                                                                                                                | 0*                             | 1 | 2 | 3 | 4 | 5 |
| 1)       | Цветовое решение (фон, цвет шрифта, сочетаемость цветов, учет психологических особенностей реципиента), соответствие фирменным цветам компании | 0                              | 1 | 2 | 3 | 4 | 5 |
| 2)       | Удобочитаемость (кегель шрифта, количество строк в слайде, тень, «засечки»)                                                                    | 0                              | 1 | 2 | 3 | 4 | 5 |
| 3)       | «Прозрачная» структура презентации, ее соответствие плану, сформулированным цели и задачам, разделам сайта компании                            | 0                              | 1 | 2 | 3 | 4 | 5 |
| 4)       | Грамотность                                                                                                                                    | 0                              | 1 | 2 | 3 | 4 | 5 |
| 5)       | Ссылки на источники данных и цитат в презентации /сноски                                                                                       | 0                              | 1 | 2 | 3 | 4 | 5 |
| 6)       | Наличие схем/таблиц/графиков/авторских рисунков-пиктограмм = заменителей текста                                                                | 0                              | 1 | 2 | 3 | 4 | 5 |
| 7)       | Вид схем, графиков, таблиц, диаграмм, их авторство                                                                                             | 0                              | 1 | 2 | 3 | 4 | 5 |
| 8)       | Иллюстрации (фотографии, рисунки) (наличие/отсутствие подписей к ним, качество)                                                                | 0                              | 1 | 2 | 3 | 4 | 5 |
| 9)       | Оформление библиографического описания                                                                                                         | 0                              | 1 | 2 | 3 | 4 | 5 |
| 10)      | Оформление сведений об авторе                                                                                                                  | 0                              | 1 | 2 | 3 | 4 | 5 |

|                                              |              |  |  |  |  |  |    |
|----------------------------------------------|--------------|--|--|--|--|--|----|
|                                              | Итого баллов |  |  |  |  |  | 50 |
| * 0 баллов – если этот компонент отсутствует |              |  |  |  |  |  |    |

Презентация засчитывается, если студент набрал минимально 25 баллов.

Оценка «**зачтено**» при защите презентации ставится, если:

- презентация представлена грамотным научным языком, имеет чёткую структуру и логику изложения, точка зрения студента обоснованна, в работе присутствуют ссылки на нормативно-правовые акты, примеры из практики, мнения известных учёных в данной области. Студент демонстрирует готовностью к саморазвитию, самореализации, использованию творческого потенциала.

Оценка «**незачтено**» выставляется, если:

- студент не выполнил задание, или выполнил его формально, ответил на заданный вопрос, при этом не ссылаясь на мнения учёных, не высказывая своего мнения, не проявил способность к анализу, то есть в целом цель учебного проекта не достигнута.

## 7. Материально-техническое обеспечение по дисциплине (модулю)

| Наименование специальных помещений                                                                                                                                          | Оснащенность специальных помещений                                                            | Перечень лицензионного программного обеспечения                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Учебные аудитории для проведения занятий лекционного типа (441, 308, 408, 209)                                                                                              | Мебель: учебная мебель<br>Технические средства обучения: экран, проектор, компьютер (ноутбук) | Microsoft Office 2019, Photoshop, InDesign, Антивирус Касперский |
| Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (307, 308, 404, 407, 406) | Мебель: учебная мебель<br>Технические средства обучения: экран, проектор, компьютер (ноутбук) | Microsoft Office 2019, Photoshop, InDesign, Антивирус Касперский |
| Учебные аудитории для проведения лабораторных работ (404, 307, 308, 409, 304)                                                                                               | Мебель: учебная мебель<br>Технические средства обучения: экран, проектор, компьютер (ноутбук) | Microsoft Office 2019, Photoshop, InDesign, Антивирус Касперский |

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<br>Комплект специализированной мебели: компьютерные столы<br>Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi) |                                                 |



|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                         |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <p>Помещение для самостоятельной работы обучающихся (ауд. 301)</p> | <p>Мебель: учебная мебель<br/>Комплект специализированной мебели: компьютерные столы<br/>Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)</p> | <p>Microsoft Office 2019, Photoshop, InDesign, Антивирус Касперский</p> |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|