

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное бюджетное образовательное учреждение высшего образования  
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ  
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»  
(ТУСУР)



УТВЕРЖДАЮ  
Проректор по учебной работе

Документ подписан электронной подписью

Сертификат: a1119608-cdff-4455-b54e-5235117c185c

Владелец: Семенко Павел Васильевич

Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **09.03.03 Прикладная информатика**

Направленность (профиль) / специализация: **Прикладная информатика в экономике**

Форма обучения: **очная**

Факультет: **Факультет систем управления (ФСУ)**

Кафедра: **Кафедра автоматизированных систем управления (АСУ)**

Курс: **4**

Семестр: **7**

Учебный план набора 2020 года

Объем дисциплины и виды учебной деятельности

| Виды учебной деятельности          | 7 семестр | Всего | Единицы |
|------------------------------------|-----------|-------|---------|
| Лекционные занятия                 | 36        | 36    | часов   |
| Лабораторные занятия               | 36        | 36    | часов   |
| Самостоятельная работа             | 72        | 72    | часов   |
| Общая трудоемкость                 | 144       | 144   | часов   |
| (включая промежуточную аттестацию) | 4         | 4     | з.е.    |

| Формы промежуточной аттестация | Семестр |
|--------------------------------|---------|
| Зачет                          | 7       |

## 1. Общие положения

### 1.1. Цели дисциплины

1. Дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации.

### 1.2. Задачи дисциплины

1. Овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами.

2. Приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса.

3. Овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль направления подготовки.

Индекс дисциплины: Б1.О.03.08.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

| Компетенция                             | Индикаторы достижения компетенции | Планируемые результаты обучения по дисциплине |
|---|-----------------------------------|---|
| <b>Универсальные компетенции</b>        |                                   |   |
| -                                       | -                                 | -   |
| <b>Общепрофессиональные компетенции</b> |                                   |   |

|  |   |   |
|--|---|---|
| ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | В результате изучения дисциплины студент должен знать принципы, методы и средства решения стандартных задач профессиональной деятельности, основы информационной и библиографической культуры, современные информационно-коммуникационные технологии для поиска и анализа информации, основные требования информационной безопасности в профессиональной деятельности |
|  | ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности                             | В результате изучения дисциплины студент должен уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности  |
|  | ОПК-3.3. Владеет навыками подготовки и оформления информационных ресурсов, например, в виде обзоров, рефератов, докладов, с применением современных технологий и с учетом основных требований информационной безопасности   | В результате изучения дисциплины студент должен овладеть навыками подготовки и оформления информационных ресурсов с применением современных технологий и с учетом основных требований информационной безопасности   |
| <b>Профессиональные компетенции</b>  |   |   |
| -  | -   | -   |

#### **4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

| Виды учебной деятельности   | Всего часов | Семестры  |
|---|-------------|-----------|
|   |             | 7 семестр |
| <b>Контактная аудиторная работа обучающихся с преподавателем, всего</b>   | 72          | 72        |
| Лекционные занятия  | 36          | 36        |
| Лабораторные занятия  | 36          | 36        |
| <b>Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего</b> | 72          | 72        |
| Подготовка к тестированию   | 30          | 30        |
| Подготовка к зачету   | 34          | 34        |
| Подготовка к лабораторной работе, написание отчета  | 8           | 8         |
| <b>Общая трудоемкость (в часах)</b>   | 144         | 144       |
| <b>Общая трудоемкость (в з.е.)</b>  | 4           | 4         |

#### **5. Структура и содержание дисциплины**

##### **5.1. Разделы (темы) дисциплины и виды учебной деятельности**

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в

таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

| Названия разделов (тем) дисциплины                                 | Лек. зан., ч | Лаб. раб. | Сам. раб., ч | Всего часов (без экзамена) | Формируемые компетенции |
|--|--------------|-----------|--------------|----------------------------|-------------------------|
| <b>7 семестр</b>   |              |           |              |                            |                         |
| 1 Введение в информационную безопасность                           | 2            | -         | 4            | 6                          | ОПК-3                   |
| 2 Законодательные и правовые основы защиты компьютерной информации | 4            | -         | 6            | 10                         | ОПК-3                   |
| 3 Математические методы и модели в задачах защиты информации       | 4            | 14        | 10           | 28                         | ОПК-3                   |
| 4 Математические основы криптографических методов                  | 4            | -         | 8            | 12                         | ОПК-3                   |
| 5 Криптография с открытым ключом                                   | 6            | 22        | 12           | 40                         | ОПК-3                   |
| 6 Методы идентификации и аутентификации пользователей              | 6            | -         | 8            | 14                         | ОПК-3                   |
| 7 Межсетевые экраны и VPN сети                                     | 4            | -         | 8            | 12                         | ОПК-3                   |
| 8 Защита компьютерных систем от вредоносных программ               | 4            | -         | 8            | 12                         | ОПК-3                   |
| 9 Комплексная защита информации                                    | 2            | -         | 8            | 10                         | ОПК-3                   |
| Итого за семестр   | 36           | 36        | 72           | 144                        |                         |
| Итого  | 36           | 36        | 72           | 144                        |                         |

### 5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

| Названия разделов (тем) дисциплины       | Содержание разделов (тем) дисциплины (в т.ч. по лекциям)   | Трудоемкость (лекционные занятия), ч | Формируемые компетенции |
|--|--|--------------------------------------|-------------------------|
| <b>7 семестр</b>                         |  |                                      |                         |
| 1 Введение в информационную безопасность | Исторические аспекты и современная постановка задач обеспечения информационной безопасности (ИБ) и защиты информации. Связь проблем ИБ с развитием информационных технологий и процессами глобализации. Основные понятия и определения: конфиденциальность, целостность, доступность, угроза, уязвимость, риски. Принципы защиты информации. Классы средств защиты информации. | 2                                    | ОПК-3                   |
|  | Итого  | 2                                    |                         |

|  |   |   |       |
|--|---|---|-------|
| 2 Законодательные и правовые основы защиты компьютерной информации | Основы российского законодательства в сфере защиты информации.<br>Ответственность за правонарушения и преступления в сфере компьютерной информации и защиты информации.<br>Политика безопасности. Модели безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем  | 4 | ОПК-3 |
|  | Итого   | 4 |       |
| 3 Математические методы и модели в задачах защиты информации       | Основные понятия и определения криптографии. Краткая история развития криптологии. Методы шифрования.<br>Основные понятия и определения.<br>Классификация методов шифрования.<br>Блочные шифры. Сеть Фейштеля.<br>Алгоритмы блочного шифрования.<br>Режимы выполнения алгоритмов шифрования. Вопросы стойкости блочных шифров. Поточковые шифры.<br>Основные понятия. Алгоритмы потокового шифрования   | 4 | ОПК-3 |
|  | Итого   | 4 |       |
| 4 Математические основы криптографических методов                  | Основные понятия и определения теории информации. Основные теоремы теории чисел. Дискретные логарифмы в конечном поле. Элементы теории сложности проблем. Классы сложности проблем.   | 4 | ОПК-3 |
|  | Итого   | 4 |       |
| 5 Криптография с открытым ключом                                   | Криптография с открытым ключом.<br>Основные способы использования алгоритмов с открытым ключом.<br>Алгоритмы шифрования с открытым ключом. Вопросы стойкости. Задача распределения ключей.<br>Криптографические хеш-функции.<br>Электронная цифровая подпись. Общие сведения об электронной цифровой подписи. Основные процедуры цифровой подписи. Алгоритмы электронной цифровой подписи. Вопросы стойкости электронной цифровой подписи.<br>Сертификат открытого ключа. | 6 | ОПК-3 |
|  | Итого   | 6 |       |

|   |   |    |       |
|---|---|----|-------|
| 6 Методы идентификации и аутентификации пользователей | Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации на основе паролей. Методы строгой аутентификации. Биометрическая аутентификация пользователя.   | 6  | ОПК-3 |
|   | Итого   | 6  |       |
| 7 Межсетевые экраны и VPN сети                        | Межсетевые экраны. Режим функционирования межсетевых экранов и их основные компоненты. Основные схемы сетевой защиты на базе межсетевых экранов. Виртуальные защищенные сети. Концепция построения виртуальных защищенных сетей. Основные понятия и функции.              | 4  | ОПК-3 |
|   | Итого   | 4  |       |
| 8 Защита компьютерных систем от вредоносных программ  | Вредоносные программы и их классификация. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.   | 4  | ОПК-3 |
|   | Итого   | 4  |       |
| 9 Комплексная защита информации                       | Концепция комплексной защиты информации. Анализ схемы функций защиты и результатов защиты информации. Методология создания, организации и обеспечения функционирования систем комплексной защиты информации (КЗИ). Пути и проблемы практической реализации концепции КЗИ. | 2  | ОПК-3 |
|   | Итого   | 2  |       |
| Итого за семестр                                      |   | 36 |       |
| Итого   |   | 36 |       |

### 5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

### 5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

| Названия разделов (тем) дисциплины                           | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|--|---------------------------------|-----------------|-------------------------|
| <b>7 семестр</b>   |                                 |                 |                         |
| 3 Математические методы и модели в задачах защиты информации | Классическая криптография       | 6               | ОПК-3                   |
|  | Блочное симметричное шифрование | 8               | ОПК-3                   |
|  | Итого                           | 14              |                         |

|                                  |  |    |       |
|----------------------------------|--|----|-------|
| 5 Криптография с открытым ключом | Асимметричное шифрование                               | 8  | ОПК-3 |
|                                  | Электронная цифровая подпись                           | 8  | ОПК-3 |
|                                  | Практическое применение криптографии с открытым ключом | 6  | ОПК-3 |
|                                  | Итого  | 22 |       |
| Итого за семестр                 |  | 36 |       |
| Итого                            |  | 36 |       |

### 5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

### 5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов (тем) дисциплины                                 | Виды самостоятельной работы                        | Трудоемкость, ч | Формируемые компетенции | Формы контроля      |
|--|--|-----------------|-------------------------|---------------------|
| <b>7 семестр</b>   |  |                 |                         |                     |
| 1 Введение в информационную безопасность                           | Подготовка к тестированию                          | 2               | ОПК-3                   | Тестирование        |
|  | Подготовка к зачету                                | 2               | ОПК-3                   | Зачёт               |
|  | Итого  | 4               |                         |                     |
| 2 Законодательные и правовые основы защиты компьютерной информации | Подготовка к тестированию                          | 2               | ОПК-3                   | Тестирование        |
|  | Подготовка к зачету                                | 4               | ОПК-3                   | Зачёт               |
|  | Итого  | 6               |                         |                     |
| 3 Математические методы и модели в задачах защиты информации       | Подготовка к тестированию                          | 2               | ОПК-3                   | Тестирование        |
|  | Подготовка к лабораторной работе, написание отчета | 4               | ОПК-3                   | Лабораторная работа |
|  | Подготовка к зачету                                | 4               | ОПК-3                   | Зачёт               |
|  | Итого  | 10              |                         |                     |
| 4 Математические основы криптографических методов                  | Подготовка к тестированию                          | 4               | ОПК-3                   | Тестирование        |
|  | Подготовка к зачету                                | 4               | ОПК-3                   | Зачёт               |
|  | Итого  | 8               |                         |                     |
| 5 Криптография с открытым ключом                                   | Подготовка к тестированию                          | 4               | ОПК-3                   | Тестирование        |
|  | Подготовка к лабораторной работе, написание отчета | 4               | ОПК-3                   | Лабораторная работа |
|  | Подготовка к зачету                                | 4               | ОПК-3                   | Зачёт               |
|  | Итого  | 12              |                         |                     |

|   |                           |    |       |              |
|---|---------------------------|----|-------|--------------|
| 6 Методы идентификации и аутентификации пользователей | Подготовка к тестированию | 4  | ОПК-3 | Тестирование |
|   | Подготовка к зачету       | 4  | ОПК-3 | Зачёт        |
|   | Итого                     | 8  |       |              |
| 7 Межсетевые экраны и VPN сети                        | Подготовка к тестированию | 4  | ОПК-3 | Тестирование |
|   | Подготовка к зачету       | 4  | ОПК-3 | Зачёт        |
|   | Итого                     | 8  |       |              |
| 8 Защита компьютерных систем от вредоносных программ  | Подготовка к тестированию | 4  | ОПК-3 | Тестирование |
|   | Подготовка к зачету       | 4  | ОПК-3 | Зачёт        |
|   | Итого                     | 8  |       |              |
| 9 Комплексная защита информации                       | Подготовка к тестированию | 4  | ОПК-3 | Тестирование |
|   | Подготовка к зачету       | 4  | ОПК-3 | Зачёт        |
|   | Итого                     | 8  |       |              |
| Итого за семестр                                      |                           | 72 |       |              |
| Итого   |                           | 72 |       |              |

### 5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

| Формируемые компетенции | Виды учебной деятельности |           |           | Формы контроля                           |
|-------------------------|---------------------------|-----------|-----------|--|
|                         | Лек. зан.                 | Лаб. раб. | Сам. раб. |  |
| ОПК-3                   | +                         | +         | +         | Зачёт, Лабораторная работа, Тестирование |

## 6. Рейтинговая система для оценки успеваемости обучающихся

### 6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

| Формы контроля           | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|--------------------------|--|---|---|------------------|
| <b>7 семестр</b>         |  |   |   |                  |
| Зачёт                    | 10   | 10  | 10  | 30               |
| Лабораторная работа      | 14   | 14  | 12  | 40               |
| Тестирование             | 10   | 10  | 10  | 30               |
| Итого максимум за период | 34   | 34  | 32  | 100              |
| Нарастающим итогом       | 34   | 68  | 100   | 100              |

### 6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль



| Баллы на дату текущего контроля                       | Оценка |
|---|--------|
| ≥ 90% от максимальной суммы баллов на дату ТК         | 5      |
| От 70% до 89% от максимальной суммы баллов на дату ТК | 4      |
| От 60% до 69% от максимальной суммы баллов на дату ТК | 3      |
| < 60% от максимальной суммы баллов на дату ТК         | 2      |

### 6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка                               | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS)           |
|--------------------------------------|--|-------------------------|
| 5 (отлично) (зачтено)                | 90 – 100   | A (отлично)             |
| 4 (хорошо) (зачтено)                 | 85 – 89  | B (очень хорошо)        |
|                                      | 75 – 84  | C (хорошо)              |
|                                      | 70 – 74  | D (удовлетворительно)   |
| 3 (удовлетворительно) (зачтено)      | 65 – 69  | E (посредственно)       |
|                                      | 60 – 64  |                         |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов   | F (неудовлетворительно) |

## 7. Учебно-методическое и информационное обеспечение дисциплины

### 7.1. Основная литература

1. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: Учебное пособие для вузов. – М.: ФОРУМ, 2012. – 592 с. (наличие в библиотеке ТУСУР - 30 экз.).
2. Конкин, Ю. В. Основы информационной безопасности : учебное пособие / Ю. В. Конкин, Ю. М. Кузьмин, В. Н. Пржегорлинский. — Рязань : РГРТУ, 2021. — 96 с. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/220418>.

### 7.2. Дополнительная литература

1. Бацула А.П. Информационная безопасность: Учебное пособие. – Томск: ТУСУР, 2007. – 137 с. (наличие в библиотеке ТУСУР - 25 экз.).
2. Мошак, Н. Н. Защищенные информационные системы : учебное пособие / Н. Н. Мошак, Л. К. Птицына. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020. — 216 с. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/180099>.
3. Партыка Т.Л. Информационная безопасность: Учебное пособие. 3-е изд., исп. и доп. - М.: Форум, 2007. – 367 с. (наличие в библиотеке ТУСУР - 20 экз.).
4. Мельников В.П. Информационная безопасность и защита информации: учебн. пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. : С. А. Клейменов. - М.: Academia, 2006. - 330 с. (наличие в библиотеке ТУСУР - 30 экз.).
5. Основы информационной безопасности: учебн. пособие для вузов / Е.Б. Белов [и др]. – М.: Горячая линия – Телеком, 2006. – 544 с. (наличие в библиотеке ТУСУР - 80 экз.).
6. Куприянов А.И. Основы защиты информации: учебн. пособие для вузов / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М.: Academia, 2006. - 253 с. (наличие в библиотеке ТУСУР - 50 экз.).
7. Климентьев, К. Е. Введение в защиту компьютерной информации : учебное пособие / К. Е. Климентьев. — Самара : Самарский университет, 2020. — 183 с. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/189043>.

### 7.3. Учебно-методические пособия

#### 7.3.1. Обязательные учебно-методические пособия

1. Горитов А.Н. Информационная безопасность: методические указания к практическим занятиям. – Томск: ТУСУР, 2016. – 8 с. [Электронный ресурс]: — Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-pract.pdf>.

2. Горитов А.Н. Информационная безопасность: методические указания по выполнению лабораторных работ. – Томск: ТУСУР, 2016. – 6 с. [Электронный ресурс]: — Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-lab.pdf>.

3. Горитов А.Н. Информационная безопасность: методические указания по самостоятельной и индивидуальной работе студентов. – Томск: ТУСУР, 2016. – 8 с. [Электронный ресурс]: — Режим доступа: <http://asu.tusur.ru/learning/090303/d40/090303-d40-work.pdf>.

### **7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов**

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

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

### **7.4. Современные профессиональные базы данных и информационные справочные системы**

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: <https://lib.tusur.ru/ru/resursy/bazy-dannyh>.

## **8. Материально-техническое и программное обеспечение дисциплины**

### **8.1. Материально-техническое и программное обеспечение для лекционных занятий**

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

### **8.2. Материально-техническое и программное обеспечение для лабораторных работ**

Учебная вычислительная лаборатория / Лаборатория ГПО "Алгоритм": учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для проведения групповых и индивидуальных консультаций, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы; 634034, Томская область, г. Томск, Вершинина улица, д. 74, 439 ауд.

Описание имеющегося оборудования:

- Рабочие станции Intel Celeron 1.7 (10 шт.);
- Проектор Acer X125H DLP;
- Экран проектора;
- Видеокамера (2 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Code::Blocks;

- Far Manager;
- Free Pascal;
- Lazarus;
- LibreOffice;
- Microsoft PowerPoint Viewer;
- Microsoft Visual Studio 2013 Professional;
- Microsoft Windows 7 Pro;
- Notepad++;

### **8.3. Материально-техническое и программное обеспечение для самостоятельной работы**

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

### **8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов**

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

## **9. Оценочные материалы и методические рекомендации по организации изучения дисциплины**

### **9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации**

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

| Названия разделов (тем) дисциплины                                 | Формируемые компетенции | Формы контроля      | Оценочные материалы (ОМ)            |
|--|-------------------------|---------------------|-------------------------------------|
| 1 Введение в информационную безопасность                           | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 2 Законодательные и правовые основы защиты компьютерной информации | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 3 Математические методы и модели в задачах защиты информации       | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Лабораторная работа | Темы лабораторных работ             |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 4 Математические основы криптографических методов                  | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 5 Криптография с открытым ключом                                   | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Лабораторная работа | Темы лабораторных работ             |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 6 Методы идентификации и аутентификации пользователей              | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 7 Межсетевые экраны и VPN сети                                     | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 8 Защита компьютерных систем от вредоносных программ               | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |
| 9 Комплексная защита информации                                    | ОПК-3                   | Зачёт               | Перечень вопросов для зачета        |
|  |                         | Тестирование        | Примерный перечень тестовых заданий |

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

| Оценка                     | Баллы за ОМ                                | Формулировка требований к степени сформированности планируемых результатов обучения |   |  |
|----------------------------|--|---|---|--|
|                            |  | знать   | уметь   | владеть  |
| 2<br>(неудовлетворительно) | < 60% от максимальной суммы баллов         | отсутствие знаний или фрагментарные знания  | отсутствие умений или частично освоенное умение             | отсутствие навыков или фрагментарные применение навыков              |
| 3<br>(удовлетворительно)   | от 60% до 69% от максимальной суммы баллов | общие, но не структурированные знания   | в целом успешно, но не систематически осуществляемое умение | в целом успешное, но не систематическое применение навыков           |
| 4 (хорошо)                 | от 70% до 89% от максимальной суммы баллов | сформированные, но содержащие отдельные проблемы знания                             | в целом успешное, но содержащие отдельные пробелы умение    | в целом успешное, но содержащие отдельные пробелы применение навыков |
| 5 (отлично)                | ≥ 90% от максимальной суммы баллов         | сформированные систематические знания   | сформированное умение                                       | успешное и систематическое применение навыков                        |

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

| Оценка                     | Формулировка требований к степени компетенции  |
|----------------------------|--|
| 2<br>(неудовлетворительно) | Не имеет необходимых представлений о проверяемом материале или<br>Знать на уровне <b>ориентирования</b> , представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения. |
| 3<br>(удовлетворительно)   | Знать и уметь на <b>репродуктивном</b> уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.   |
| 4 (хорошо)                 | Знать, уметь, владеть на <b>аналитическом</b> уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.   |
| 5 (отлично)                | Знать, уметь, владеть на <b>системном</b> уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.                             |

### 9.1.1. Примерный перечень тестовых заданий

1. Какие виды алгоритмов подразделяются на блочные и поточные  
комбинированные  
асимметричные  
симметричные
2. Для передачи больших сообщений лучше всего соответствуют режимы:  
ECB  
CFB  
OFB  
CBC
3. Режим CBC используется для того, чтобы  
увеличить скорость шифрования  
не было необходимости разбивать сообщение на целое число блоков достаточно большой  
длины  
одинаковые незашифрованные блоки преобразовывались в различные зашифрованные  
блоки
4. Хеш-функции предназначены для  
сжатия сообщения  
шифрования сообщения  
получения дайджеста сообщения
5. Алгоритм Диффи-Хеллмана основан на  
задаче факторизации числа  
задаче определения, является ли данное число простым  
задаче дискретного логарифмирования
6. Алгоритм RSA основан на:  
задаче дискретного логарифмирования  
задаче определения, является ли данное число простым  
задаче факторизации числа
7. Цифровая подпись вычисляется:  
для отправляемого электронного сообщения  
для отправляемого сообщения совместно с дайджестом  
для отправляемого сообщения и адресом отправителя  
для дайджеста отправляемого электронного сообщения
8. Для создания подписи следует использовать  
закрытый ключ получателя  
свой открытый ключ  
свой закрытый ключ
9. В DSS используется следующая хеш-функция  
MD5  
SHA-2  
SHA-1
10. В стандарте ГОСТ 3410 используется следующая хеш-функция  
MD5  
SHA-1  
ГОСТ 3411

### **9.1.2. Перечень вопросов для зачета**

1. Законодательные и нормативные документы информационной безопасности.
2. Алгоритмы симметричного шифрования.
3. Режимы выполнения алгоритмов симметричного шифрования.
4. Потокосое шифрование.
5. Алгоритмы потокового шифрования.
6. Криптографические хеш-функции.
7. Задача распределения ключей.
8. Электронная цифровая подпись.

### **9.1.3. Темы лабораторных работ**

1. Классическая криптография

2. Блочное симметричное шифрование
3. Асимметричное шифрование
4. Электронная цифровая подпись
5. Практическое применение криптографии с открытым ключом

## 9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

- чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

- если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

- осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

## 9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.2.

Таблица 9.2 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

| Категории обучающихся                       | Виды дополнительных оценочных материалов  | Формы контроля и оценки результатов обучения    |
|---|---|---|
| С нарушениями слуха                         | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы                        | Преимущественно письменная проверка             |
| С нарушениями зрения                        | Собеседование по вопросам к зачету, опрос по терминам   | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами         |

|   |  |  |
|---|--|--|
| С ограничениями по<br>общемедицинским<br>показаниям | Тесты, письменные<br>самостоятельные работы, вопросы<br>к зачету, контрольные работы,<br>устные ответы | Преимущественно проверка<br>методами, определяющимися<br>исходя из состояния<br>обучающегося на момент<br>проверки |
|---|--|--|

#### **9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

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

**Для лиц с нарушениями зрения:**

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

- в форме электронного документа;
- в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.



## ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры АСУ  
протокол № 13 от «31» 10 2019 г.

### СОГЛАСОВАНО:

| Должность                          | Инициалы, фамилия | Подпись  |
|------------------------------------|-------------------|--|
| Заведующий выпускающей каф. АСУ    | А.М. Кориков      | Согласовано,<br>9e8ba22e-f8dc-42a7-<br>a705-2441d49ffeee |
| Заведующий обеспечивающей каф. АСУ | А.М. Кориков      | Согласовано,<br>9e8ba22e-f8dc-42a7-<br>a705-2441d49ffeee |
| Начальник учебного управления      | Е.В. Саврук       | Согласовано,<br>fa63922b-1fce-4aba-<br>845d-9ce7670b004c |

### ЭКСПЕРТЫ:

|                               |                |  |
|-------------------------------|----------------|--|
| Доцент, каф. АСУ              | А.И. Исакова   | Согласовано,<br>79bf1038-9d22-4279-<br>a1e8-7806307b7f82 |
| Заведующий кафедрой, каф. АСУ | В.В. Романенко | Согласовано,<br>c3e2018f-3231-48c3-<br>b093-89b6f5342191 |

### РАЗРАБОТАНО:

|                     |              |  |
|---------------------|--------------|--|
| Профессор, каф. АСУ | А.Н. Горитов | Разработано,<br>1fee132a-a2cd-4e8d-<br>bdd5-8e7aa16d873b |
|---------------------|--------------|--|