

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 УР

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: **заочная (в том числе с применением дистанционных образовательных технологий)**

Факультет: **Факультет дистанционного обучения (ФДО)**

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

Курс: **4**

Семестр: **8**

Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

| Виды учебной деятельности | 8 семестр | Всего | Единицы |
|--|-----------|-------|---------|
| Лабораторные занятия | 16 | 16 | часов |
| Самостоятельная работа | 114 | 114 | часов |
| Самостоятельная работа под руководством преподавателя | 8 | 8 | часов |
| Контрольные работы | 2 | 2 | часов |
| Подготовка и сдача зачета | 4 | 4 | часов |
| Общая трудоемкость (включая промежуточную аттестацию) | 144 | 144 | часов |
| | | 4 | з.е. |

| Формы промежуточной аттестация | Семестр | Количество |
|--------------------------------|---------|------------|
| Зачет | 8 | |
| Контрольные работы | 8 | 1 |

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 (special hard skills – SHS).

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 |
|---|-----------------------------------|---|
| Универсальные компетенции | | |
| - | - | - |
| Общепрофессиональные компетенции | | |

| | | |
|--|---|---|
| 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 |
| Профессиональные компетенции | | |
| - | - | - |

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 |
|---|-------------|-----------|
| | | 8 семестр |
| Контактная аудиторная работа обучающихся с преподавателем, всего | 26 | 26 |
| Лабораторные занятия | 16 | 16 |
| Самостоятельная работа под руководством преподавателя | 8 | 8 |
| Контрольные работы | 2 | 2 |
| Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего | 114 | 114 |
| Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 38 | 38 |
| Подготовка к контрольной работе | 36 | 36 |
| Подготовка к лабораторной работе | 20 | 20 |
| Написание отчета по лабораторной работе | 20 | 20 |
| Подготовка и сдача зачета | 4 | 4 |
| Общая трудоемкость (в часах) | 144 | 144 |
| Общая трудоемкость (в з.е.) | 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 | Лаб. раб. | Контр. раб. | СРП, ч. | Сам. раб., ч | Всего часов (без промежуточной аттестации) | Формируемые компетенции |
|--|-----------|-------------|---------|--------------|--|-------------------------|
| 8 семестр | | | | | | |
| 1 Проблемы и методы защиты компьютерной информации | - | 2 | 1 | 8 | 11 | ОПК-3 |
| 2 Исторические шифры | - | | 1 | 8 | 9 | ОПК-3 |
| 3 Основные понятия криптографии | - | | 1 | 8 | 9 | ОПК-3 |
| 4 Математические основы криптографических методов | - | | 1 | 8 | 9 | ОПК-3 |
| 5 Компьютерные алгоритмы шифрования | 4 | | 1 | 20 | 25 | ОПК-3 |
| 6 Компьютерная безопасность и практическое применение криптографии | 4 | | 1 | 20 | 25 | ОПК-3 |
| 7 Вирусы и угрозы, связанные с вирусами | 4 | | 1 | 21 | 26 | ОПК-3 |
| 8 Брандмауэры | 4 | | 1 | 21 | 26 | ОПК-3 |
| Итого за семестр | 16 | 2 | 8 | 114 | 140 | |
| Итого | 16 | 2 | 8 | 114 | 140 | |

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины

| Названия разделов (тем) дисциплины | Содержание разделов (тем) дисциплины | СРП, ч | Формируемые компетенции |
|--|---|--------|-------------------------|
| 8 семестр | | | |
| 1 Проблемы и методы защиты компьютерной информации | Информационная безопасность. Проблемы защиты информации в компьютерных системах. Традиционные вопросы криптографии. Современные приложения криптографии. Понятие криптографического протокола. Криптография и стеганография | 1 | ОПК-3 |
| | Итого | 1 | |
| 2 Исторические шифры | Подстановочные и перестановочные шифры. Статистические свойства языка шифрования. Шифр сдвига. Шифр замены. Шифр Виженера. Перестановочные шифры. Критерий статистической оценки происхождения шифротекст. Одноразовые блокноты | 1 | ОПК-3 |
| | Итого | 1 | |

| | | | |
|--|--|---|-------|
| 3 Основные понятия криптографии | Криптографическая терминология. Алгоритмы и ключи. Однонаправленные функции. Однонаправленная хэш-функция. Передача информации с использованием криптографии с открытыми ключами. Смешанные криптосистемы. Основные протоколы | 1 | ОПК-3 |
| | Итого | 1 | |
| 4 Математические основы криптографических методов | Теория информации. Теория сложности. Теория чисел. Генерация простого числа. Дискретные логарифмы в конечном поле | 1 | ОПК-3 |
| | Итого | 1 | |
| 5 Компьютерные алгоритмы шифрования | Симметричные шифры. Поточные шифры. Блочные шифры. Шифр Фейстеля. Шифр DE. Режимы работы DES. Шифр Rijndael. Алгоритм криптографического преобразования ГОСТ 28147-8. Стандарт симметричного шифрования данных IDEA. Однонаправленная хэш-функция MD5. Асимметричный алгоритм шифрования данных RSA. Комплекс криптографических алгоритмов PGP | 1 | ОПК-3 |
| | Итого | 1 | |
| 6 Компьютерная безопасность и практическое применение криптографии | Общие сведения. Обзор стандартов в области защиты информации. Подсистема информационной безопасности. Защита локальной рабочей станции. Методы и средства обеспечения информационной безопасности локальных рабочих станций. Защита в локальных сетях | 1 | ОПК-3 |
| | Итого | 1 | |
| 7 Вирусы и угрозы, связанные с вирусами | Вредоносные программы. Лазейки. Логическая бомба. «Троянские кони». Вирус. «Черви». Бактерии. Природа вирусов. Структура вируса. Начальное инфицирование. Типы вирусов. Макровирусы. Антивирусная защита. Перспективные методы антивирусной защиты | 1 | ОПК-3 |
| | Итого | 1 | |
| 8 Брандмауэры | Принципы разработки брандмауэров. Характеристики брандмауэров. Типы брандмауэров. Конфигурации брандмауэров. Высоконадежные системы | 1 | ОПК-3 |
| | Итого | 1 | |
| Итого за семестр | | 8 | |
| Итого | | 8 | |

5.3. Контрольные работы

Виды контрольных работ и часы на контрольные работы приведены в таблице 5.3.
Таблица 5.3 – Контрольные работы

| № п.п. | Виды контрольных работ | Трудоемкость, ч | Формируемые компетенции |
|------------------|---|-----------------|-------------------------|
| 8 семестр | | | |
| 1 | Контрольная работа с автоматизированной проверкой | 2 | ОПК-3 |
| Итого за семестр | | 2 | |
| Итого | | 2 | |

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 |
|--|---|-----------------|-------------------------|
| 8 семестр | | | |
| 5 Компьютерные алгоритмы шифрования | Администрирование учетных записей пользователей | 4 | ОПК-3 |
| Итого | | 4 | |
| 6 Компьютерная безопасность и практическое применение криптографии | Управление параметрами операционной системы | 4 | ОПК-3 |
| Итого | | 4 | |
| 7 Вирусы и угрозы, связанные с вирусами | Дискреционный механизм разграничения доступа | 4 | ОПК-3 |
| Итого | | 4 | |
| 8 Брандмауэры | Политика ограниченного использования программ | 4 | ОПК-3 |
| Итого | | 4 | |
| Итого за семестр | | 16 | |
| Итого | | 16 | |

5.5. Контроль самостоятельной работы (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 |
|--|--|-----------------|-------------------------|---------------------|
| 8 семестр | | | | |
| 1 Проблемы и методы защиты компьютерной информации | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 4 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к контрольной работе | 4 | ОПК-3 | Контрольная работа |
| | Итого | 8 | | |

| | | | | |
|--|--|----|-------|------------------------------|
| 2 Исторические шифры | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 4 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к контрольной работе | 4 | ОПК-3 | Контрольная работа |
| | Итого | 8 | | |
| 3 Основные понятия криптографии | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 4 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к контрольной работе | 4 | ОПК-3 | Контрольная работа |
| | Итого | 8 | | |
| 4 Математические основы криптографических методов | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 4 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к контрольной работе | 4 | ОПК-3 | Контрольная работа |
| | Итого | 8 | | |
| 5 Компьютерные алгоритмы шифрования | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 5 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к лабораторной работе | 5 | ОПК-3 | Лабораторная работа |
| | Написание отчета по лабораторной работе | 5 | ОПК-3 | Отчет по лабораторной работе |
| | Подготовка к контрольной работе | 5 | ОПК-3 | Контрольная работа |
| | Итого | 20 | | |
| 6 Компьютерная безопасность и практическое применение криптографии | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 5 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к лабораторной работе | 5 | ОПК-3 | Лабораторная работа |
| | Написание отчета по лабораторной работе | 5 | ОПК-3 | Отчет по лабораторной работе |
| | Подготовка к контрольной работе | 5 | ОПК-3 | Контрольная работа |
| | Итого | 20 | | |

| | | | | |
|---|--|-----|-------|------------------------------|
| 7 Вирусы и угрозы, связанные с вирусами | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 6 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к лабораторной работе | 5 | ОПК-3 | Лабораторная работа |
| | Написание отчета по лабораторной работе | 5 | ОПК-3 | Отчет по лабораторной работе |
| | Подготовка к контрольной работе | 5 | ОПК-3 | Контрольная работа |
| | Итого | 21 | | |
| 8 Брандмауэры | Самостоятельное изучение тем (вопросов) теоретической части дисциплины | 6 | ОПК-3 | Зачёт, Тестирование |
| | Подготовка к лабораторной работе | 5 | ОПК-3 | Лабораторная работа |
| | Написание отчета по лабораторной работе | 5 | ОПК-3 | Отчет по лабораторной работе |
| | Подготовка к контрольной работе | 5 | ОПК-3 | Контрольная работа |
| | Итого | 21 | | |
| Итого за семестр | | 114 | | |
| | Подготовка и сдача зачета | 4 | | Зачет |
| Итого | | 118 | | |

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 |
|-------------------------|---------------------------|-----------|-----|-----------|--|
| | Лаб. раб. | Конт.Раб. | СРП | Сам. раб. | |
| ОПК-3 | + | + | + | + | Зачёт, Контрольная работа, Лабораторная работа, Отчет по лабораторной работе, Тестирование |

6. Рейтинговая система для оценки успеваемости обучающихся

Рейтинговая система не используется

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Спицын В. Г. Информационная безопасность вычислительной техники: Учебное пособие / Спицын В. Г. - Томск: Эль Контент, 2011. - 148 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://study.tusur.ru/study/library>.

7.2. Дополнительная литература

1. 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. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/180099>.

2. Климентьев, К. Е. Введение в защиту компьютерной информации : учебное пособие / К. Е. Климентьев. — Самара : Самарский университет, 2020. — 183 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/189043>.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Якимук А. Ю. Защита информации. Методические указания по выполнению лабораторной работы: Методические указания / Якимук А. Ю., Конев А. А. - Томск : ФДО, ТУСУР, 2017. – 81 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://study.tusur.ru/study/library>.

2. Горитов А. Н. Защита информации. Методические указания по организации самостоятельной работы: Методические указания / Горитов А. Н., Кориков А. М. - Томск : ФДО, ТУСУР, 2018. – 22 с. Доступ из личного кабинета студента. [Электронный ресурс]: — Режим доступа: <https://study.tusur.ru/study/library>.

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. Иное учебно-методическое обеспечение

1. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс]: электронный курс / В.Г. Спицын. - Томск : ФДО, ТУСУР, 2013. (доступ из личного кабинета студента) .

7.5. 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. Общие требования к материально-техническому и программному обеспечению дисциплины

Учебные аудитории для проведения занятий лабораторного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, для самостоятельной работы студентов

634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- Веб-камера - 6 шт.;
- Наушники с микрофоном - 6 шт.;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Google Chrome;
- Kaspersky Endpoint Security для Windows;
- LibreOffice;
- Microsoft Windows;

8.2. 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, 209 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.

8.3. 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 Проблемы и методы защиты компьютерной информации | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Тестирование | Примерный перечень тестовых заданий |
| 2 Исторические шифры | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Тестирование | Примерный перечень тестовых заданий |
| 3 Основные понятия криптографии | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Тестирование | Примерный перечень тестовых заданий |
| 4 Математические основы криптографических методов | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Тестирование | Примерный перечень тестовых заданий |
| 5 Компьютерные алгоритмы шифрования | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Отчет по лабораторной работе | Темы лабораторных работ |

| | | | |
|--|-------|------------------------------|---|
| 6 Компьютерная безопасность и практическое применение криптографии | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Отчет по лабораторной работе | Темы лабораторных работ |
| 7 Вирусы и угрозы, связанные с вирусами | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Отчет по лабораторной работе | Темы лабораторных работ |
| 8 Брандмауэры | ОПК-3 | Зачёт | Перечень вопросов для зачета |
| | | Контрольная работа | Примерный перечень тем и тестовых заданий на контрольные работы |
| | | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Отчет по лабораторной работе | Темы лабораторных работ |

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 (неудовлетворительно) | < 60% от максимальной суммы баллов | отсутствие знаний или фрагментарные знания | отсутствие умений или частично освоенное умение | отсутствие навыков или фрагментарные применение навыков |

| | | | | |
|--------------------------|--|---|---|--|
| 3 (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 (неудовлетворительно) | Не имеет необходимых представлений о проверяемом материале или Знать на уровне ориентирования , 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 (удовлетворительно) | Знать и уметь на репродуктивном уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях. |
| 4 (хорошо) | Знать, уметь, владеть на аналитическом 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 системном 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
 - 1) комбинированные
 - 2) асимметричные
 - 3) симметричные
2. Для передачи больших сообщений лучше всего соответствуют режимы:
 - 1) ECB
 - 2) CFB
 - 3) OFB
 - 4) CBC

3. Режим CBC используется для того, чтобы
 - 1) увеличить скорость шифрования
 - 2) не было необходимости разбивать сообщение на целое число блоков достаточно большой длины
 - 3) одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки
4. Хеш-функции предназначены для
 - 1) сжатия сообщения
 - 2) шифрования сообщения
 - 3) получения дайджеста сообщения
5. Алгоритм Диффи-Хеллмана основан на
 - 1) задаче факторизации числа
 - 2) задаче определения, является ли данное число простым
 - 3) задаче дискретного логарифмирования
6. Алгоритм RSA основан на:
 - 1) задаче дискретного логарифмирования
 - 2) задаче определения, является ли данное число простым
 - 3) задаче факторизации числа
7. Цифровая подпись вычисляется:
 - 1) для отправляемого электронного сообщения
 - 2) для отправляемого сообщения совместно с дайджестом
 - 3) для отправляемого сообщения и адресом отправителя
 - 4) для дайджеста отправляемого электронного сообщения
8. Для создания подписи следует использовать
 - 1) закрытый ключ получателя
 - 2) свой открытый ключ
 - 3) свой закрытый ключ
9. В DSS используется следующая хеш-функция
 - 1) MD5
 - 2) SHA-2
 - 3) SHA-1
10. В стандарте ГОСТ 3410 используется следующая хеш-функция
 - 1) MD5
 - 2) SHA-1
 - 3) ГОСТ 3411
11. Количество знаков в шифротексте и в исходном тексте в общем случае:
 - 1) не может различаться.
 - 2) может различаться.
 - 3) должно быть равно сумме знаков открытого текста и ключа.
 - 4) должно быть равно разности знаков открытого текста и ключа.
 - 5) должно быть равно длине алфавита.
12. Стойкость современных криптосистем основывается на:
 - 1) секретности долговременных элементов криптозащиты.
 - 2) применении стеганографических алгоритмов.
 - 3) секретности алгоритма шифрования.
 - 4) секретности информации сравнительно малого размера, называемой ключом.
 - 5) секретности алгоритма шифрования и ключа.
13. Конфиденциальность:
 - 1) свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
 - 2) способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
 - 3) свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
 - 4) способность совершать некоторые действия в информационной системе незаметно для других объектов.
 - 5) свойство информации быть доступной ограниченному кругу пользователей

- информационной системы, в которой циркулирует данная информация.
14. Целостность:
 - 1) свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
 - 2) способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
 - 3) свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
 - 4) способность совершать некоторые действия в информационной системе незаметно для других объектов.
 - 5) свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
 15. Достоверность:
 - 1) свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
 - 2) способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
 - 3) свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
 - 4) способность совершать некоторые действия в информационной системе незаметно для других объектов.
 - 5) свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
 16. Оперативность:
 - 1) свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
 - 2) способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
 - 3) свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
 - 4) способность совершать некоторые действия в информационной системе незаметно для других объектов.
 - 5) свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
 17. Неотслеживаемость:
 - 1) свойство информации, выражающееся в строгой принадлежности объекту, который является ее источником, либо тому объекту, от которого эта информация принята.
 - 2) способность информации быть доступной для конечного пользователя в соответствии с его временными потребностями.
 - 3) свойство информации или программного обеспечения сохранять свою структуру и/или содержание в процессе передачи и/или хранения.
 - 4) способность совершать некоторые действия в информационной системе незаметно для других объектов.
 - 5) свойство информации быть доступной ограниченному кругу пользователей информационной системы, в которой циркулирует данная информация.
 18. В случае криптоанализа на основе шифротекста считается, что:
 - 1) криптоаналитик может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа.
 - 2) криптоаналитик имеет возможность подставлять для дешифрирования фиктивные шифротексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог с минимальной трудоемкостью вычислить ключ шифрования.
 - 3) криптоаналитик знает механизм шифрования и ему доступен только шифротекст.
 - 4) многократно подставляет тексты для шифрования (или дешифрирования), причем каждую новую порцию данных выбирает в зависимости от полученного результата преобразований предыдущей порции.
 - 5) криптоаналитику известен шифротекст и та или иная доля исходной информации, а в

- частных случаях и соответствие между шифротекстом и исходным текстом.
19. В случае криптоанализа на основе открытого текста считается, что:
 - 1) криптоаналитик может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа.
 - 2) криптоаналитик имеет возможность подставлять для дешифрирования фиктивные шифротексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог с минимальной трудоемкостью вычислить ключ шифрования.
 - 3) криптоаналитик знает механизм шифрования и ему доступен только шифротекст.
 - 4) многократно подставляет тексты для шифрования (или дешифрирования), причем каждую новую порцию данных выбирает в зависимости от полученного результата преобразований предыдущей порции.
 - 5) криптоаналитику известен шифротекст и та или иная доля исходной информации, а в частных случаях и соответствие между шифротекстом и исходным текстом.
 20. В случае криптоанализа на основе выбранного открытого текста считается, что:
 - 1) криптоаналитик может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа.
 - 2) криптоаналитик имеет возможность подставлять для дешифрирования фиктивные шифротексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог с минимальной трудоемкостью вычислить ключ шифрования.
 - 3) криптоаналитик знает механизм шифрования и ему доступен только шифротекст.
 - 4) многократно подставляет тексты для шифрования (или дешифрирования), причем каждую новую порцию данных выбирает в зависимости от полученного результата преобразований предыдущей порции.
 - 5) криптоаналитику известен шифротекст и та или иная доля исходной информации, а в частных случаях и соответствие между шифротекстом и исходным текстом.

9.1.2. Перечень вопросов для зачета

1. В случае криптоанализа на основе выбранного шифротекста считается, что:
 - 1) криптоаналитик может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа.
 - 2) криптоаналитик имеет возможность подставлять для дешифрирования фиктивные шифротексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог с минимальной трудоемкостью вычислить ключ шифрования.
 - 3) криптоаналитик знает механизм шифрования и ему доступен только шифротекст.
 - 4) многократно подставляет тексты для шифрования (или дешифрирования), причем каждую новую порцию данных выбирает в зависимости от полученного результата преобразований предыдущей порции.
 - 5) криптоаналитику известен шифротекст и та или иная доля исходной информации, а в частных случаях и соответствие между шифротекстом и исходным текстом.
2. В случае криптоанализа на основе адаптированных текстов считается, что:
 - 1) криптоаналитик может ввести специально подобранный им текст в шифрующее устройство и получить криптограмму, образованную под управлением секретного ключа.
 - 2) криптоаналитик имеет возможность подставлять для дешифрирования фиктивные шифротексты, которые выбираются специальным образом, чтобы по полученным на выходе дешифратора текстам он мог с минимальной трудоемкостью вычислить ключ шифрования.
 - 3) криптоаналитик знает механизм шифрования и ему доступен только шифротекст.
 - 4) многократно подставляет тексты для шифрования (или дешифрирования), причем каждую новую порцию данных выбирает в зависимости от полученного результата преобразований предыдущей порции.
 - 5) криптоаналитику известен шифротекст и та или иная доля исходной информации, а в частных случаях и соответствие между шифротекстом и исходным текстом.
3. Имитозащита:
 - 1) дополнительная информация к открытому тексту, называемая имитовставкой.

- 2) дополнительная информация к шифротексту, называемая имитовставкой.
- 3) дополнительная информация к открытому ключу, называемая имитовставкой.
- 4) дополнительная информация к секретному ключу, называемая имитовставкой.
- 5) защита от навязывания ложных сообщений путем формирования в зависимости от секретного ключа специальной дополнительной информации, называемой имитовставкой, которая передается вместе с криптограммой.
4. Идентификация законных пользователей заключается в:
 - 1) сравнении пароля, вводимого пользователем, с паролем, хранящимся в явном виде в ЭВМ.
 - 2) сравнении образа пароля, вводимого пользователем, с образом пароля, хранящегося в явном виде в ЭВМ.
 - 3) сравнении пароля, вводимого пользователем, с образом пароля, хранящимся в ЭВМ.
 - 4) сравнении образа пароля, вводимого пользователем, с паролем, хранящимся в явном виде в ЭВМ.
 - 5) сравнении пароля, вводимого пользователем, с открытым ключом, хранящимся в ЭВМ.
5. Электронная цифровая подпись основывается на:
 - 1) одноключевых криптографических алгоритмах, в которых предусматривается использование одного секретного ключа.
 - 2) двухключевых криптографических алгоритмах, в которых предусматривается использование 2-х ключей — открытого и секретного.
 - 3) трехключевых криптографических алгоритмах, в которых предусматривается использование 3-х ключей — открытого, и двух секретных.
 - 4) трехключевых криптографических алгоритмах, в которых предусматривается использование 3-х ключей — двух открытых и секретного.
 - 5) четырехключевых криптографических алгоритмах, в которых предусматривается использование 4-х ключей — двух открытого и двух секретных.
6. Протокол — это:
 - 1) совокупность действий, выполняемых в случайной последовательности двумя или более субъектами с целью достижения определенного результата.
 - 2) совокупность действий, выполняемых в заданной последовательности одним субъектом с целью достижения определенного результата.
 - 3) совокупность действий, выполняемых случайным образом двумя или более субъектами с целью достижения определенного результата.
 - 4) совокупность действий, выполняемых в случайной последовательности одним субъектом с целью достижения определенного результата.
 - 5) совокупность действий, выполняемых в заданной последовательности двумя или более субъектами с целью достижения определенного результата.
7. Криптографические протоколы – это такие протоколы:
 - 1) в которых совокупность действий выполняется двумя субъектами.
 - 2) в которых совокупность действий выполняется тремя субъектами.
 - 3) в которых используются криптографические преобразования данных.
 - 4) в которых совокупность действий выполняется четырьмя субъектами.
 - 5) в которых совокупность действий выполняется пятью субъектами.
8. Стеганографией называется:
 - 1) техника криптографических преобразований.
 - 2) техника криптоаналитических преобразований.
 - 3) техника криптологических преобразований.
 - 4) техника быстрой записи информации.
 - 5) техника скрытой передачи или скрытого хранения информации
9. В криптографии:
 - 1) скрывается факт передачи сообщения.
 - 2) скрывается факт передачи сообщения и его содержание.
 - 3) скрывается содержание сообщения.
 - 4) скрывается факт передачи сообщения и не скрывается его содержание.
 - 5) не скрывается факт передачи сообщения и не скрывается его содержание.
10. Стеганографические методы могут обеспечить высокий уровень защиты информации только в том случае, когда:

- 1) они будут дополнены предварительными административными мерами.
- 2) они будут сочетаться с облачными технологиями.
- 3) они будут дополнены техникой быстрого копирования информации.
- 4) они будут дополнены предварительным криптографическим преобразованием сообщения.
- 5) они будут дополнены случайным преобразованием сообщения.

9.1.3. Примерный перечень тем и тестовых заданий на контрольные работы

1. Подстановочным шифром называется шифр, в котором:
 - 1) используется матрица чисел размерностью 5×5 .
 - 2) используется открытый ключ.
 - 3) используется фрагмент текста.
 - 4) используется фрагмент текста и открытый ключ.
 - 5) каждый символ открытого текста в шифротексте заменяется другим символом.
2. В однозвучном подстановочном шифре:
 - 1) один символ открытого текста отображается на несколько символов шифротекста.
 - 2) два символа открытого текста отображаются на один символ шифротекста.
 - 3) три символа открытого текста отображаются на один символ шифротекста.
 - 4) четыре символа открытого текста отображаются на один символ шифротекста.
 - 5) пять символов открытого текста отображаются на один символ шифротекста.
3. Полиграмный подстановочный шифр:
 - 1) один символ открытого текста отображается на один символ шифротекста.
 - 2) один символ открытого текста отображает на несколько символов шифротекста.
 - 3) блоки символов шифрует по группам.
 - 4) применяет псевдослучайный ключ.
 - 5) применяет открытый ключ.
4. В полиалфавитном подстановочном шифре:
 - 1) применяется псевдослучайный ключ.
 - 2) применяется имитовставка.
 - 3) применяется открытый ключ.
 - 4) длина ключа равна длине сообщения.
 - 5) применяются несколько простых подстановочных шифров.
5. В шифровании с использованием одноразовых блокнотов должны выполняться условия:
 - 1) ключ должен быть псевдослучайным и может применяться только один раз.
 - 2) ключ должен быть случайным, может применяться только один раз и длина ключа равна длине сообщения.
 - 3) ключ должен быть случайным, может применяться постоянно и длина ключа равна длине сообщения.
 - 4) ключ должен быть случайным, может применяться постоянно и длина ключа произвольна.
 - 5) ключ должен быть псевдослучайным, может применяться только один раз и длина ключа равна длине сообщения.
6. В шифре Цезаря каждый символ открытого текста:
 - 1) заменяется символом, находящимся двумя символами правее по модулю 26.
 - 2) заменяется символом, находящимся девятью символами правее по модулю 26.
 - 3) заменяется символом, находящимся семью символами правее по модулю 26.
 - 4) заменяется символом, находящимся пятью символами правее по модулю 26.
 - 5) заменяется символом, находящимся тремя символами правее по модулю 26.
7. В операции “исключающее или” (XOR):
 - 1) $0+0=1$; $0+1=1$; $1+0=1$; $1+1=0$.
 - 2) $0+0=0$; $0+1=1$; $1+0=1$; $1+1=1$.
 - 3) $0+0=0$; $0+1=0$; $1+0=1$; $1+1=0$.
 - 4) $0+0=0$; $0+1=1$; $1+0=1$; $1+1=0$.
 - 5) $0+0=1$; $0+1=1$; $1+0=0$; $1+1=0$.
8. Наиболее часто встречаемыми символами в английском среднестатистическом тексте в порядке убывания являются:
 - 1) a; t; e.

- 2) o; t; a.
 - 3) e; t; a.
 - 4) e; t; o.
 - 5) e; t; h.
9. Наиболее часто встречаемыми биграммami в английском среднестатистическом тексте в порядке убывания являются:
- 1) in; he; an.
 - 2) th; he; in.
 - 3) an; th; he.
 - 4) th; er; an.
 - 5) th; he; an.
10. Наиболее часто встречаемыми триграммами в английском среднестатистическом тексте в порядке убывания являются:
- 1) the, for, and.
 - 2) the, ing, and.
 - 3) and, ing, her.
 - 4) ing, ere, and.
 - 5) ent, ing, and.

9.1.4. Темы лабораторных работ

1. Администрирование учетных записей пользователей
2. Управление параметрами операционной системы
3. Дискреционный механизм разграничения доступа
4. Политика ограниченного использования программ

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 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 9.4.

Таблица 9.4 – 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 общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент 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 № 1 от «24» 1 2023 г.

СОГЛАСОВАНО:

| Должность | Инициалы, фамилия | Подпись |
|------------------------------------|-------------------|--|
| Заведующий выпускающей каф. АСУ | В.В. Романенко | Согласовано, с3e2018f-3231-48c3- b093-89b6f5342191 |
| Заведующий обеспечивающей каф. АСУ | В.В. Романенко | Согласовано, с3e2018f-3231-48c3- b093-89b6f5342191 |
| Декан ФДО | И.П. Черкашина | Согласовано, 4580bdea-d7a1-4d22- bda1-21376d739cfc |

ЭКСПЕРТЫ:

| | | |
|-------------------------------|----------------|--|
| Доцент, каф. АСУ | А.И. Исакова | Согласовано, 79bf1038-9d22-4279- a1e8-7806307b7f82 |
| Заведующий кафедрой, каф. АСУ | В.В. Романенко | Согласовано, с3e2018f-3231-48c3- b093-89b6f5342191 |

РАЗРАБОТАНО:

| | | |
|---------------------|---------------|--|
| Профессор, каф. АСУ | А.Н. Горитов | Разработано, 1fee132a-a2cd-4e8d- bdd5-8e7aa16d873b |
| Ассистент, каф. ТЭО | Ю.Л. Замятина | Разработано, 1663c03a-62e7-4092- 902a-95591a9d4047 |