Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Уральский государственный лесотехнический университет»
Социально-экономический институт
Кафедра интеллектуальных систем

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

включая фонд оценочных средств и методические указания
для самостоятельной работы обучающихся

Б1.В.16 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки – 09.03.03 Прикладная информатика
Направленность (профиль) – Администрирование информационных систем
Квалификация – бакалавр
Количество зачётных единиц (часов) – 5 (180)

г. Екатеринбург, 2021

Разработчики:
ст.преподаватель_____/С.В.Ченушкина/

Рабочая программа утверждена на заседании кафедры интеллектуальных систем (протокол №7 от «26» апреля 2021 года).

Зав. кафедрой _____ /В.В.Побединский/

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией социально-экономического института
(протокол №3 от «17» мая 2021 года).

Председатель методической комиссии СЭИ _____ /А.В. Чевардин /

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ _____ /Ю.А. Капустина/
«21» мая 2021 года

Оглавление

1. Общие положения

Дисциплина «Информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)» учебного плана, входящего в состав образовательной программы высшего образования 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем»).

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Информационная безопасность» являются:

– Федеральный закон «Об образовании в Российской Федерации», утвержденный приказом Минобрнауки РФ № 273-ФЗ от 29.12.2012;

– Приказ Минобрнауки России № 301 от 05.04.2017 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

– Приказ Министерства труда и социальной защиты от 18.11.2014 г. №896н «Об утверждении профессионального стандарта «Специалист по информационным системам»;

– Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата), утвержденный приказом Министерства образования и науки РФ №922 от 19.09.2017;

– Учебный план образовательной программы высшего образования направления 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем») подготовки бакалавров по очной форме обучения, одобренный Ученым советом УГЛТУ (протокол №2 от 18.02.2021).

Обучение по образовательной программе 09.03.03 «Прикладная информатика» (профиль «Администрирование информационных систем») осуществляется на русском языке.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемыми результатами обучения по дисциплине являются знания, умения, владения и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом.

Цели и задачи курса

Цель курса – ознакомление обучающихся с угрозами информационной безопасности, методами и средствами защиты информации.

З**адачи дисциплины**:

– формирование у обучающихся системы знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования;

– изучение математических основ защиты информации; методов, средств и инструментов шифрования, применяемых в сфере информационных технологий и бизнеса;

– приобретение навыков работы с методами шифрования и криптоанализа;

– формирование представлений об информационной безопасности, включая аппаратную часть и математическое обеспечение.

Процесс изучения дисциплины направлен на формирование следующих профессиональных компетенций:

– **ПК-1** – Способен устанавливать и настраивать серверную часть информационной системы;

– **ПК-2** – Способен устанавливать и настраивать системное и прикладное программное обеспечение, необходимое для функционирования информационной системы;

– **ПК-3** – Способен настраивать оборудование, необходимое для работы ИС.

В результате изучения дисциплины студент должен:

знать: основные виды угроз безопасности информации; правила защиты информации; методы и средства защиты информации; основы шифрования и криптографии;

уметь: использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; уметь выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач; оперативно реагировать на различные угрозы информационной безопасности, в том числе при использовании компьютерных программ для тестирования ИС.

владеть: способами повышения сохранности информации; методами защиты информации; технологиями шифрования и парольной защитой операционной системы; навыками решения задач криптоанализа и шифрования; обнаружения сетевых проникновений, применения, установки и настройки антивирусных систем и систем распознавания угроз и атак.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к дисциплинам части, формируемой участниками образовательных отношений, блока Б1 «Дисциплины (модули)», что означает формирование в процессе обучения у бакалавра профессиональных компетенций в рамках выбранного профиля подготовки. Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин ОПОП и написания выпускной квалификационной работы.

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие дисциплины	Сопутствующие дисциплины	Обеспечиваемые дисциплины
Информатика Операционные системы Компьютерные сети и телекоммуникации	Системное администрирование Сетевое администрирование Администрирование систем управления базами данных Производственная практика (технологическая (проектно-технологическая практика))	Производственная практика (преддипломная) Выполнение и защита выпускной квалификационной работы

Указанные связи дисциплины дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины

Вид учебной работы	Всего академических часов
Контактная работа с преподавателем*:	**34,25**
лекции (Л)	12
практические занятия (ПЗ)	-
лабораторные работы (ЛР)	22
иные виды контактной работы	0,25
Самостоятельная работа обучающихся:	**145,75**

Вид учебной работы	Всего академических часов
изучение теоретического курса	121
подготовка к текущему контролю	13
курсовая работа (курсовой проект)	-
подготовка к промежуточной аттестации	11,75
Вид промежуточной аттестации:	**Зачет с оценкой**
Общая трудоемкость, з.е./ часы	**5/180**

*Контактная работа обучающихся с преподавателем, в том числе с применением дистанционных образовательных технологий, включает занятия лекционного типа, и (или) занятия семинарского типа, лабораторные занятия, и (или) групповые консультации, и (или) индивидуальную работу обучающегося с преподавателем, а также аттестационные испытания промежуточной аттестации. Контактная работа может включать иные виды учебной деятельности, предусматривающие групповую и индивидуальную работу обучающихся с преподавателем. Часы контактной работы определяются Положением об организации и проведении контактной работы при реализации образовательных программ высшего образования, утвержденным Ученым советом УГЛТУ от 25 февраля 2020 года.

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов

5.1. Трудоемкость разделов дисциплины

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Раздел 1. Основные составляющие информационной безопасности	2		4	6	28
1.1	Тема 1. Понятие информационной безопасности, ее основные составляющие	1		2	3	14
1.2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	1		2	3	14
2	Раздел 2. Уровни информационной безопасности	3		6	9	42
2.1	Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	1		2	3	14
2.2	Тема 4. Административный уровень информационной безопасности	1		2	3	14
2.3	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	1		2	3	14
3	Раздел 3. Программно-технические меры	7		12	19	74
3.1	Тема 6. Основные программно-технические меры	1		2	3	10
3.2	Тема 7. Идентификация и аутентификация, управление доступом	1		2	3	10
3.3	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	1		2	3	10
3.4	Тема 9. Экранирование, анализ защищенности.	1		2	3	10
3.5	Тема 10. Обеспечение высокой доступности	1		2	3	10

3.6	Тема 11. Туннелирование и управление	1		1	2	10
3.7	Тема 12. Криптографические методы защиты информации	1		1	2	14
Итого по разделам:		**12**	**-**	**22**	**34**	**134**
Промежуточная аттестация		x	x	x	0,25	11,75
Курсовая работа (курсовой проект)		x	x	x	x	x
Всего		**180**				

5.2 Содержание занятий лекционного типа

Раздел 1. Основные составляющие информационной безопасности.

Тема 1. Понятие информационной безопасности, ее основные составляющие

Понятие информационной безопасности; Основные составляющие информационной безопасности; Важность и сложность проблемы информационной безопасности Основные определения и критерии классификации угроз. Некоторые примеры угроз доступности; Вредоносное программное обеспечение.

Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность

О необходимости объектно-ориентированного подхода к информационной безопасности; Основные понятия объектно-ориентированного подхода; Применение объектно-ориентированного подхода к рассмотрению защищаемых систем; Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

Раздел 2. Уровни информационной безопасности

Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности

Важность законодательного уровня информационной безопасности; Обзор российского законодательства в области информационной безопасности; Правовые акты общего назначения. Стандарты и спецификации в области информационной безопасности: основные понятия, механизмы безопасности, классы безопасности, информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Гармонизированные критерии Европейских стран. Руководящие документы Федеральной службы по техническому и экспортному контролю Российской Федерации.

Тема 4. Административный уровень информационной безопасности

Основные понятия. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем.

Тема 5. Процедурный уровень информационной безопасности. Управление рисками

Основные классы мер процедурного уровня; Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Управление рисками: основные понятия. Подготовительные этапы управления рисками. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Раздел 3. Программно-технические меры

Тема 6. Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.

Тема 7. Идентификация и аутентификация, управление доступом

Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Ролевое управление доступом. Управление доступом в Java-среде. Возможный подход к управлению доступом в распределенной объектной среде.

Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит

Основные понятия. Активный аудит. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты.

Тема 9. Экранирование, анализ защищенности.

Экранирование. Основные понятия. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности.

Тема 10. Обеспечение высокой доступности

Доступность. Основные понятия. Основы мер обеспечения высокой доступности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости. Программное обеспечение промежуточного слоя. Обеспечение обслуживаемости.

Тема 11. Туннелирование и управление

Туннелирование. Управление. Основные понятия. Возможности типичных систем.

Тема 12. Криптографические методы защиты информации.

История криптографии. Шифры и их свойства. Системы шифрования с открытыми ключами. Классификация алгоритмов шифрования информации. Симметричные и асимметричные криптосистемы. Сеть Фештеля, стандарт AES. Методы рандомизации сообщений. Архивация - алгоритмы Хаффмана, Лемпеля-Зива. Криптографические хеш-функции. Алгоритмы RSA. Электронные цифровые подписи. Обмен ключами по алгоритму Диффи-Хеллмана. Криптографические стандарты.

5.3 Темы и формы занятий семинарского типа

Учебным планом по дисциплине предусмотрены лабораторные работы

№ п/п	Наименование занятий семинарского типа (практических занятий)	Форма проведения занятия	Трудоёмкость, час.
Раздел 1. Основные составляющие информационной безопасности			
1.	Тема 1. Понятие информационной безопасности, ее основные составляющие	Практические задания	2
2.	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	Практические задания	2
Раздел 2. Уровни информационной безопасности			
3.	Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	Практические задания	2
4.	Тема 4. Административный уровень информационной безопасности	Практические задания	2
5.	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	Практические задания	2
Раздел 3. Программно-технические меры			
6.	Тема 6. Основные программно-технические меры	Практические задания	2
7.	Тема 7. Идентификация и аутентификация, управление доступом	Практические задания	2
8.	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	Практические задания	2
9.	Тема 9. Экранирование, анализ защищенности.	Практические задания	2
10.	Тема 10. Обеспечение высокой доступности	Практические задания	2
11.	Тема 11. Туннелирование и управление	Практические задания	1
12.	Тема 12. Криптографические методы защиты информации	Практические задания	1
Всего часов			22

5.4 Самостоятельная работа обучающихся

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.
Раздел 1. Основные составляющие информационной безопасности			
1	Тема 1. Понятие информационной безопасности, ее основные составляющие	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
Раздел 2. Уровни информационной безопасности			
3	Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
4	Тема 4. Административный уровень информационной безопасности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
5	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
Раздел 3. Программно-технические меры			
6	Тема 6. Основные программно-технические меры	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
7	Тема 7. Идентификация и аутентификация, управление доступом	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
8	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
9	Тема 9. Экранирование, анализ защищенности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
10	Тема 10. Обеспечение высокой доступности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
11	Тема 11. Туннелирование и управление	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	10
12	Тема 12. Криптографические методы защиты информации	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю в тестовой форме	14
Итого по разделам			134
Промежуточная аттестация			11,75
Всего часов			145,75

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная литература

№ п/п	Автор, наименование	Год издания	Количество экземпляров в научной библиотеке
Основная литература			
1	Информационная безопасность и защита информации: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
2	Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические рекомендации / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 1 — 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163932. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
3	Моргунов, А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов. — Новосибирск: НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227. — Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*
4	Гультяева, Т. А. Основы информационной безопасности: учебное пособие / Т. А. Гультяева. — Новосибирск: НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/118233. — Режим доступа: для авториз. пользователей.	2018	Полнотекстовый доступ при входе по логину и паролю*
5	Информационная безопасность : учебное пособие. — Пермь : ПГГПУ, 2018. — 87 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129509. — Режим доступа: для авториз. пользователей.	2018	Полнотекстовый доступ при входе по логину и паролю*
Дополнительная литература			
6	Информационная безопасность и защита информации: учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна: Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490. — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
7	Защита компьютерной информации: учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург: БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086. — Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*
8	Бурова, М. А. Информационная безопасность и криптографическая защита информации : учебное пособие / М. А. Бурова. — Самара : СамГУПС, 2009. — 98 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130271. — Режим доступа: для авториз. пользователей.	2009	Полнотекстовый доступ при входе по логину и паролю*

*- прежде чем пройти по ссылке, необходимо войти в систему

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий.

Электронные библиотечные системы

Каждый обучающийся обеспечен доступом к электронной библиотечной системе УГЛТУ (http://lib.usfeu.ru/), ЭБС Издательства Лань http://e.lanbook.com/, ЭБС

Университетская библиотека онлайн http://biblioclub.ru/, содержащих издания по основным изучаемым дисциплинам и сформированных по согласованию с правообладателями учебной и учебно- методической литературы.

Справочные и информационные системы

1. Справочно-правовая система «Консультант Плюс». – Режим доступа: для авториз. пользователей.

2. Информационно-правовой портал Гарант. – URL: http://www.garant.ru/. – Режим доступа: свободный.

Профессиональные базы данных

1. Президентская библиотека им. Б.Н. Ельцина. – URL: https://www.prlib.ru/. – Режим доступа: свободный.

2. Научная электронная библиотека elibrary. – URL: http://elibrary.ru/. Режим доступа: свободный.

3. Национальная электронная библиотека. – URL: https://нэб.рф/. – Режим доступа: свободный.

4. Хабр. Сообщество ИТ-специалистов. – URL: https://habr.com/ru/. – Режим доступа: свободный.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формируемые компетенции	Вид и форма контроля
– **ПК-1** – Способен устанавливать и настраивать серверную часть информационной системы; – **ПК-2** – Способен устанавливать и настраивать системное и прикладное программное обеспечение, необходимое для функционирования информационной системы; – **ПК-3** – Способен настраивать оборудование, необходимое для работы ИС	**Текущий контроль:** выполнение практических заданий и заданий в тестовой форме, **Промежуточный контроль:** контрольные вопросы к зачету с оценкой

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии оценивания ответа на контрольные вопросы зачета с оценкой (промежуточный контроль формирования компетенции ПК-1, ПК-2, ПК-3)

«Зачтено» (отлично) - дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки, показана способность быстро реагировать на уточняющие вопросы;

«Зачтено» (хорошо) - дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные обучающимся с помощью «наводящих» вопросов;

«Зачтено» (удовлетворительно) - дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении

сущности раскрываемых понятий, теорий, явлений, вследствие непонимания обучающимся их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции;

«Не зачтено» (неудовлетворительно) – обучающийся демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

Критерии оценивания практических заданий (текущий контроль формирования компетенции ПК-4):

«отлично» – выполнены все задания, обучающийся четко и без ошибок ответил на все контрольные вопросы;

«хорошо» – выполнены все задания, обучающийся без с небольшими ошибками ответил на все контрольные вопросы;

«удовлетворительно» – выполнены все задания с замечаниями, обучающийся ответил на все контрольные вопросы с замечаниями;

«неудовлетворительно» – обучающийся не выполнил или выполнил неправильно задания, ответил на контрольные вопросы с ошибками или не ответил на конкретные вопросы.

Критерии оценивания тестовых заданий (текущий контроль формирования компетенции ПК-4):

«5» (отлично) – даны верные ответы на 86-100% тестовых заданий;

«4» (хорошо) – даны верные ответы на 71-85% тестовых заданий;

«3» (удовлетворительно) – даны верные ответы на 51-70% тестовых заданий;

«2» (неудовлетворительно) – даны верные ответы менее, чем на 51% тестовых заданий.

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

7.3.1. Контрольные вопросы к зачету с оценкой (промежуточный контроль)

1. Какие вы знаете методы криптографической защиты файлов?
2. В чем преимущества и недостатки одноалфавитных методов?
3. Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из одноалфавитных, вы выберете? Обоснуйте свой выбор.
4. Целесообразно ли повторно применять для уже зашифрованного текста: а) метод многоалфавитного шифрования? б) метод Цезаря?
5. Чем отличается "псевдооткрытый" текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?
6. Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины "вероятного" слова?
7. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
8. В чем недостатки метода дешифрования с использованием протяжки вероятного слова?
9. Сравните основные характеристики алгоритмов *Rijndael* и ГОСТ 28147-89.
10. Сравните выработку ключевой информации в алгоритмах *Rijndael* и ГОСТ 28147-89.

11. Сравните основные характеристики алгоритмов *Rijndael* и *DES.*
12. Опишите структуру сети Фейстеля.
13. Сравните алгоримы *Rijndael* и ГОСТ 28147-89 по показателям диффузии.
14. Сравните алгоримы *Rijndael* и ГОСТ 28147-89 по показателям стойкости.

7.3.2. Примерные практические задания (текущий контроль)

1. Для одноалфавитного метода с фиксированным смещением определить установленное в программе смещение.

   Для этого:

- просмотреть предварительно созданный с помощью редактора свой текстовый файл;
- выполнить для этого файла шифрование;
- просмотреть в редакторе зашифрованный файл;
- просмотреть гистограммы исходного и зашифрованного текстов,
- описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование;
- расшифровать зашифрованный текст:
  1) с помощью программы, после чего проверить в редакторе правильность расшифрования;
  2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

2. Для одноалфавитного метода с задаваемым смещением (шифр Цезаря):
   - для своего исходного текста выполнить шифрование с произвольным смещением;
   - просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов;
   - расшифровать текст с помощью программы;
   - имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.
3. Для метода перестановки символов дешифровать зашифрованный файл.

Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

1) вручную (объясните ваши действия);
2) с помощью программы.

4. Для инверсного кодирования (по дополнению до 255):
   - для своего произвольного файла выполните шифрование;
   - просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов;
   - дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.
5. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе.

Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

6. Для многоалфавитного шифрования с ключом фиксированной длины:
   - для файла, состоящего из строки одинаковых символов выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ;
   - для файла произвольного текста произвести шифрование и расшифрование;
   - просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.

7. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п.6.

7.3.3. Примерные задания в тестовой форме (текущий контроль)

1. Согласно закону "Об информации, информатизации и защите информации", риск, связанный с использованием информации, полученной из несертифицированного источника, лежит на:
   а) потребителе информации
   б) владельце этой системы
   в) собственнике документов
2. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:
   а) предоставление услуг в области шифрования информации
   б) деятельность по технической защите конфиденциальной информации
   в) образовательную деятельность в области защиты информации
3. Согласно Закону "О лицензировании отдельных видов деятельности", лицензия - это:
   а) документ, гарантирующий безопасность программного продукта
   б) специальное разрешение на осуществление конкретного вида деятельности
   в) удостоверение, подтверждающее высокое качество изделия
4. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
   а) верифицируемой безопасностью
   б) произвольным управлением доступом
   в) принудительным управлением доступом 10 вопрос:
5. Уголовный кодекс РФ не предусматривает наказания за:
   а) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
   б) создание, использование и распространение вредоносных программ
   в) ведение личной корреспонденции на производственной технической базе
6. Согласно закону "Об информации, информатизации и защите информации", персональные данные - это:
   а) данные, находящиеся в чьей-либо персональной собственности
   б) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие
   в) идентифицировать его личность
   г) данные, хранящиеся в персональном компьютере
7. В число возможных стратегий нейтрализации рисков входят:
   а) переадресация риска
   б) уменьшение риска
   в) афиширование риска
   г) декомпозиция риска
8. Первый шаг в анализе угроз - это:
   а) ликвидация угроз
   б) идентификация угроз
   в) аутентификация угроз
9. После идентификации угрозы необходимо оценить:
   а) вероятность её осуществления
   б) ущерб от её осуществления
   в) частоту её осуществления
10. Политика безопасности строится на основе:
    а) анализа рисков
    б) общих представлений об ИС организации
    в) изучения политик родственных организаций
11. В число целей политики безопасности верхнего уровня входят:
    а) выбор методов аутентификации пользователей

б) формулировка целей, которые преследует организация в области ИБ
в) обеспечение конфиденциальности почтовых сообщений
г) формулировка административных решений по важнейшим аспектам реализации программы безопасности
д) обеспечение базы для соблюдения законов и правил

12. В число этапов жизненного цикла информационного сервиса входят:
    а) выведение из эксплуатации
    б) закупка
    в) продажа
13. Главная цель мер, предпринимаемых на административном уровне:
    а) сформировать программу безопасности и обеспечить её выполнение
    б) выполнить положения действующего законодательства
    в) отчитаться перед вышестоящими инстанциями
14. В число принципов физической защиты входят:
    а) минимизация защитных средств
    б) беспощадный отпор
    в) непрерывность защиты в пространстве и времени
15. В число принципов управления персоналом входят:
    а) инкапсуляция наследования
    б) минимизация привилегий
    в) минимизация зарплаты
    г) "разделяй и властвуй"
    д) разделение обязанностей

7.4. Соответствие шкалы оценок и уровней сформированных компетенций

Уровень сформированных компетенций	Количество баллов (оценка)	Пояснения
Высокий	«зачтено (отлично)»	Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены без замечаний. Компетенции сформирована на высоком уровне.
Хороший	«зачтено (хорошо)»	Теоретическое содержание дисциплины освоено полностью, все поставленные в ней цели и задачи достигнуты, все предусмотренные программой обучения учебные задания выполнены с отдельными незначительными замечаниями. Компетенции сформированы на базовом уровне.
Средний	«зачтено (удовлетворительно)»	Теоретическое содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Компетенции сформированы на пороговом уровне.
Низкий	«зачтено (неудовлетворительно)»	Теоретическое содержание дисциплины не освоено, компетенции не сформирована, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий.

8. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа – планируемая учебная, производственная, технологическая работа обучающихся, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль в контроле за работой обучающихся).

Самостоятельная работа обучающихся в вузе является важным видом их учебной и производственной деятельности. Самостоятельная работа играет значительную роль в рейтинговой технологии обучения. В связи с этим, обучение в вузе включает в себя две, практически одинаковые по взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой обучающихся.

Формы самостоятельной работы обучающихся разнообразны. Они включают в себя:

- чтение основной и дополнительной литературы по выполняемому заданию;
- участие в работе конференций, комплексных научных исследованиях;

В процессе изучения дисциплины «Информационная безопасность» обучающимся направления 09.03.03 *основными видами самостоятельной работы* являются:

– подготовка к аудиторным занятиям (лекциям и лабораторным работам) и выполнение соответствующих заданий;

– самостоятельная работа над отдельными темами учебной дисциплины в соответствии с учебно-тематическим планом;

- выполнение тестовых заданий;
- подготовка к зачету с оценкой.

Самостоятельное выполнение *тестовых заданий* по всем разделам дисциплины сформированы в фонде оценочных средств (ФОС)

Тестовые задания рассчитаны на самостоятельную работу без использования вспомогательных материалов. То есть при их выполнении не следует пользоваться учебной и другими видами литературы.

Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать индекс (цифровое обозначение), соответствующий правильному ответу.

На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста. Как правило, время выполнения тестового задания определяется из расчета 45-60 секунд на один вопрос.

Содержание тестов по дисциплине ориентировано на подготовку обучающихся по основным вопросам курса. Уровень выполнения теста позволяет преподавателям судить о ходе самостоятельной работы обучающихся в межсессионный период и о степени их подготовки к зачету с оценкой.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

– при проведении лекций используются презентации учебного материала, подготовленные в программе MicrosoftOffice (PowerPoint), демонстрация работы изучаемых программных продуктов (см. список ниже);

– лабораторные работы по дисциплине проводятся с использованием платформы LMS MOODLE, используются изучаемые программные продукты (см. список ниже).

Университет обеспечен необходимым комплектом лицензионного либо свободно распространяемого программного обеспечения:

– операционная система Windows 7, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок действия - бессрочно;

– пакет прикладных программ Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок действия – бессрочно;

– антивирусная программа Kaspersky Endpoint Security для бизнеса- Стандартный Russian Edition. 250-499 Node 2 year Educational Renewal License. Лицензионный сертификат: № лицензии 1B08-201001-083025-257-1457. PN: KL4863RATFQ. Срок с 01.10.2020 г. по 09.10.2022 г.;

– система управления обучением LMS Mirapolis. Договор №41/02/22/0148/22-ЕП-223-06 от 11.03.2022. Срок: с 01.04.2022 по 01.04.2023;

– – система управления обучением LMS Pruffme. Договор 2576620/0119/22-ЕП-223-03 от 09.03.2022. Срок действия: 09.03.2022-09.03.2023;

– система управления обучением LMS Moodle – программное обеспечение с открытым кодом, распространяется по лицензии GNU Public License (rus);

– браузер Яндекс (https://yandex.ru/) – программное обеспечение на условиях простой (неисключительной) лицензии;

– электронно-библиотечная система «Лань». Договор №0018/22-ЕЛ–44-06 от 24.03.2022 г. Срок действия: 09.04.2022-09.04.2023;

– электронно-библиотечная система «Университетская библиотека онлайн». Договор №8505/20220046/22-ЕП-44-06 от 27.05.2022 г. Срок действия: 27.06.2022-26.06.2023;

– программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат. ВУЗ» (URL: https://www.antiplagiat.ru/). Договор № 4831/0104/22-ЕП–223-03 от 03.03.2022 года. Срок с 03.03.2022 г по 03.03.2023 г.;

– справочная правовая система «КонсультантПлюс» (URL: http://www.consultant.ru/). Договор оказания услуг по адаптации и сопровождению экземпляров СПС КонсультантПлюс №0557/ЗК от 10.01.2022. Срок с 01.01.2022 г по 31.12.2022 г.

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Реализация учебного процесса осуществляется в специальных учебных аудиториях университета для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории университета оснащены учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Мультимедийный лекционный зал, так же оборудован системой интерактивной прямой проекции SMART Board 480iv со встроенным проектором SMARTV25 и компьютерами: Эсти ПС dx17-3770/4Gb 500Gb – 10 шт.; Pentium4 2005 CPU 2,2 GHz, DDR 256 Mb, HDD 32 Gb – 7 шт. Имеется выход в сеть Интернет.

Лабораторные занятия проводятся в компьютерных классах, оборудованными учебной мебелью (15-20 рабочих мест каждый) и компьютерами: Pentium4 2004 CPU 2,8 GHz, DDR 256 Mb, HDD 40 Gb – 20 шт., Pentium3 2003 CPU 1,2 GHz, DDR 128 Mb, HDD 10 Gb – 20 шт., Pentium4 2004 CPU 2,8 GHz, DDR 512 Mb, HDD 40 Gb – 14 шт. Имеется выход в сеть Интернет.

Обучающиеся с ограниченными возможностями здоровья, и обучающиеся инвалиды обеспечены печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия, материалы для самостоятельной работы и т. д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УГЛТУ.

Есть помещение для хранения и профилактического обслуживания учебного оборудования

Требования к оснащенности аудиторий

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Помещение для лекционных занятий	Интерактивная доска или экран, проектор; ноутбук или компьютер; комплект электронных учебно-наглядных материалов (презентаций) на флеш-носителях, обеспечивающих тематические иллюстрации. Учебная мебель.
Помещение для занятий семинарского типа (лабораторных работ), групповых и индивидуальных консультаций, текущей и промежуточной аттестации	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационную образовательную среду университета. Проектор, экран или интерактивная доска
Помещения для самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационную образовательную среду университета.