Министерство науки и высшего образования РФ

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

Адаптированная образовательная программа

Б1.В.16 Информационная безопасность

Направление подготовки 09.03.03 «Прикладная информатика»
Направленность (профиль) Цифровая экономика
Квалификация – бакалавр
Количество зачетных единиц (*часов*) – 5 (180)

Екатеринбург, 2021

Разработчик: старший преподаватель Г.Л. Нохрина

к.с.-х.н., доцент Е.В. Анянова

Рабочая программа утверждена на заседании кафедры
интеллектуальных систем
(протокол № 5 от «04» февраля 2021 года)

Заведующий кафедрой В.В. Побединский

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией социально-экономического института

(протокол № 2 от «25» февраля 2021 года)

Председатель методической комиссии СЭИ А.В. Чевардин

Рабочая программа утверждена директором социально-экономического института

Директор СЭИ Ю.А. Капустина

«26» февраля 2021 года

Оглавление

1. Общие положения 4
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
3. Место дисциплины в структуре образовательной программы 5
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 5
5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий 6
5.1. Трудоёмкость разделов дисциплины 6
Очная форма обучения 6
5.2. Содержание занятий лекционного типа 6
5.4. Детализация самостоятельной работы 9
6. Перечень учебно-методического обеспечения по дисциплине 10
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 11
7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы 11
7.2. Описание показателей и критериев оценивания компетенций при изучении дисциплины, описание шкал оценивания 12
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 12
7.4. Соответствие шкалы оценок и уровней сформированности компетенций 15
8. Методические указания для обучающихся по освоению дисциплины 16
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине 17

1. Общие положения

Дисциплина «Информационная безопасность» относится к обязательной части (блоку Б1) учебного плана, входящего в состав основной профессиональной образовательной программы высшего образования (ОПОП ВО) направления подготовки 09.03.03 «Прикладная информатика», направленность (профиль) «Цифровая экономика».

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

- Федеральный закон РФ от 29 декабря 2012 г. N 273-ФЗ «Об образовании в Российской Федерации» с изменениями;
- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.03.03 «Прикладная информатика» (уровень высшего образования бакалавриат), утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 922;
- Федеральный закон «О социальной защите инвалидов в Российской Федерации (с изменениями, редакция, действующая с 18 марта 2018 года);
- Федеральным законом РФ от 24.11.1995 г. № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- Учебный план адаптированной образовательной программы высшего образования направления 09.03.03 – Прикладная информатика (профиль – Цифровая экономика) подготовки бакалавров по очной и заочной формам обучения, одобренного Ученым советом УГЛТУ (Протокол № 2 от 25.02.2020).

Обучение по адаптированной образовательной программе 09.03.03 – Прикладная информатика (профиль – Цифровая экономика) осуществляется на русском языке.

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

Целью изучения дисциплины является реализация требований, установленных в Федеральном государственном образовательном стандарте высшего образования. Преподавание строится исходя из требуемого уровня подготовки студентов, обучающихся по данному направлению подготовки. 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.

Целью дисциплины является ознакомление обучающихся с угрозами информационной безопасности, методами и средствами защиты информации.

Задачи 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 компетенции:

- ***общепрофессиональных:***

ПК-3 – Кодирование на языках программирования;

ПК-4 – Модульное и интеграционное тестирование ИС (верификация).

В результате освоения дисциплины обучающийся 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» реализуется в рамках блока Б1.В «Дисциплины (модули)» части, формируемой участниками образовательных отношений учебного плана, что означает формирование в процессе обучения у бакалавра основных профессиональных знаний и компетенций в рамках выбранного направления подготовки. Освоение дисциплины «Информационная безопасность» опирается на знания, умения и компетенции, приобретённые в процессе изучения обеспечивающих дисциплин. В свою очередь, освоение дисциплины «Информационная безопасность» позволяет обучающимся быть подготовленными к изучению обеспечиваемых дисциплин (см. табл.). 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.

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие	Сопутствующие	Обеспечиваемые
Имитационное моделирование в экономике; Серверные вычислительные системы	Экспертные системы и системы искусственного интеллекта	Производственная практика (преддипломная); Выполнение и защита выпускной квалификационной работы

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 составляет 5 зачетных единиц (180 академических часов).

Виды учебной работы	Академические часы
	Очная форма
Контактная работа с преподавателем*:	34,25
в том числе: – занятия лекционного типа (ЛЗ)	12
– занятия семинарского типа (лабораторные работы) (ЛР)	22
– промежуточная аттестация (ПА)	0,25
Самостоятельная работа обучающихся (СР)	145,75
в том числе: – изучение теоретического курса (ТО)	121
– подготовка к текущему контролю (ТК)	13
– подготовка к промежуточной аттестации (ПА)	11,75
Вид промежуточной аттестации	Зачет с оценкой
Общая трудоемкость дисциплины	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 и видов учебных занятий

5.1. Трудоёмкость разделов дисциплины

Очная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	ЛЗ	ЛР	Всего контактной работы	Самостоя-тельная 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	0,25	11,75
Всего часов		**180**			

По дисциплине разработан курс с применением дистанционных образовательных технологий для лиц с ограниченными возможностями здоровья. Все виды учебной нагрузки (лекции, практические занятия) в полном объеме представлены на сайте ЭИОС УГЛТУ.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, текущего контроля и промежуточной аттестации, для лиц с ограниченными возможностями здоровья предусмотрена возможность выбрать режим ПЭВМ, удобный для обучающегося. Для обеспечения доступа в аудиторию лиц с нарушениями опорно-двигательного аппарата предусмотрена возможность перемещения с помощью пандуса раскладного переносного.

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 (лабораторные работы)

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

5.4. Детализация самостоятельной работы

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.
			очная форма обучения
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 задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	14
2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	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 задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	14
4	Тема 4. Административный уровень информационной безопасности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	14
5	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	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 задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	10
7	Тема 7. Идентификация и аутентификация, управление доступом	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	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 задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	10
9	Тема 9. Экранирование, анализ защищенности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в	10

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.
			очная форма обучения
		тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	
10	Тема 10. Обеспечение высокой доступности	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	10
11	Тема 11. Туннелирование и управление	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	10
12	Тема 12. Криптографические методы защиты информации	Изучение теоретического курса (чтение конспекта лекций, специальной литературы) Подготовка к текущему контролю задания в тестовой форме в дистанционном режиме в ЭИОС или видеоконференцсвязь	14
Итого по разделам			134
Промежуточная аттестация			11,75
Всего часов			145,75

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная учебная литература

№ п/п	Реквизиты источника	Год издания	Примечание
Основная учебная литература			
1	Моргунов, А. В. Информационная безопасность: учебно-методическое пособие / А. В. Моргунов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726. – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст: электронный.	2019	Полнотекстовый доступ при входе по логину и паролю*
2	Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с.: ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст: электронный.	2018	Полнотекстовый доступ при входе по логину и паролю*
Дополнительная учебная литература			
3	Информационная безопасность в цифровом обществе: учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова; Башкирский государственный университет. – Уфа: Башкирский государственный университет, 2019. – 128 с.: табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=611084. –	2019	Полнотекстовый доступ при входе по логину и паролю*

№ п/п	Реквизиты источника	Год издания	Примечание
	Библиогр. в кн. – Текст: электронный.		
4	Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.: схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485. – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст: электронный.	2020	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. Режим доступа: http://www.garant.ru/
3. База данных Scopus компании Elsevier B.V. https://www.scopus.com/

Профессиональные базы данных

1. Федеральная служба государственной статистики. Официальная статистика - Режим доступа: http://www.gks.ru/
2. Научная электронная библиотека elibrary. Режим доступа: http://elibrary.ru/ .
3. Экономический портал (https://institutiones.com/);
4. Информационная система РБК (https://ekb.rbc.ru/;

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации от 30 ноября 1994 года N 51-ФЗ
2. Профессиональный стандарт 06.015 - " Специалист по информационным системам", утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 17 сентября 2014 г. N 645н.

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-3 – Кодирование на языках программирования;	**Промежуточный контроль:** контрольные вопросы к зачету с оценкой; **Текущий контроль:** практические задания, задания в тестовой форме.
ПК-4 – Модульное и интеграционное тестирование ИС (верификация).	**Промежуточный контроль:** контрольные вопросы к зачету с оценкой; **Текущий контроль:** практические задания, задания в тестовой форме.

7.2. Описание показателей и критериев оценивания компетенций при изучении дисциплины, описание шкал оценивания

Критерии оценивания устного ответа на контрольные вопросы к зачету с оценкой (промежуточный контроль формирования компетенций ПК-3, ПК-4)

«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 выполнения заданий в тестовой форме (текущий контроль формирования компетенций ПК-3, ПК-4)

По итогам выполнения тестовых заданий оценка производится по шкале. При правильных ответах на:

86-100% заданий – оценка *«отлично»;*

71-85% заданий – оценка *«хорошо»;*

51-70% заданий – оценка *«удовлетворительно»;*

менее 51% - оценка *«неудовлетворительно».*

Критерии оценивания выполнения практических заданий (текущий контроль формирования компетенций ПК-3, ПК-4):

«отлично» - выполнены все задания, обучающийся четко и без ошибок ответил на все контрольные вопросы. Обучающийся:

«хорошо» - выполнены все задания, обучающийся без с небольшими ошибками ответил на все контрольные вопросы. Обучающийся:

«удовлетворительно» - выполнены все задания с замечаниями, обучающийся ответил на все контрольные вопросы с замечаниями. Обучающийся:

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

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

1. Контрольные вопросы для подготовки к зачету с оценкой (промежуточная аттестация)

2. Какие вы знаете методы криптографической защиты файлов?
3. В чем преимущества и недостатки одноалфавитных методов?

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

Контрольные вопросы для подготовки к зачету с оценкой (промежуточная аттестация)

Практические задания для текущего контроля (фрагмент)

Задание

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.

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

Тестовые задания для текущего контроля (фрагмент)

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 сформированности компетенций

По каждой компетенции в зависимости от уровня освоения преподаватель выставляет следующие оценки: «зачтено», «не зачтено». Итоговая оценка по промежуточной аттестации определяется как среднеарифметическая по оценкам компетенций, основываясь на правилах математического округления.

Соответствие шкалы оценок и уровней сформированных компетенций

Уровень сформированности компетенций	Оценка	Пояснение
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.
Базовый	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.
Пороговый	зачтено/удовлетворительно	Теоретическое содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Компетенции сформированы на пороговом уровне.
Низкий	не	Теоретическое содержание дисциплины не освоено,

Уровень сформированности компетенций	Оценка	Пояснение
	зачтено/Неудовлетворительно	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 обучающихся по освоению дисциплины

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)

Данные тесты могут использоваться:

- обучающимися при подготовке к зачету с оценкой в форме самопроверки знаний;
- преподавателями для проверки знаний в качестве формы промежуточного контроля на практических занятиях;
- для проверки остаточных знаний обучающихся, изучивших данный курс.

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 материала в программе Microsoft Office (PowerPoint), выход на профессиональные сайты, использование видеоматериалов различных интернет-ресурсов.

– лабораторные работы по дисциплине проводятся с использованием платформы MOODLE, справочной правовой системы «Консультант Плюс».

Лабораторные работы по дисциплине проводятся с использованием электронных вариантов методических указаний.

В процессе изучения дисциплины учебными целями являются первичное восприятие учебной информации о теоретических основах и принципах работы информационных ресурсов общества, как экономической категории; знать основы современных информационных технологий переработки информации и их влияние на успех в профессиональной деятельности; о современном состоянии уровня и направлений развития вычислительной техники и программных средств;

Для достижения этих целей используются в основном традиционные информативно-развивающие технологии обучения с учетом различного сочетания пассивных форм (лекция, практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно-иллюстративное изложение) и лабораторно-практических методов обучения (выполнение практических работ).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

- семейство коммерческих операционных систем семейства Microsoft Windows;
- офисный пакет приложений Microsoft Office;
- программная система для обнаружения текстовых заимствований в учебных и научных работах "Антиплагиат.ВУЗ";
- Kaspersky Endpoint Security для бизнеса- Стандартный Russian Edition.

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. Аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.

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 аудиториям

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Помещение для лекционных и практических занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации.	Мультимедийная, цветная, интерактивная доска со спецпроцессором, монитором и проектором; ноутбук; комплект электронных учебно-наглядных материалов (презентаций) на флеш-носителях, обеспечивающих тематические иллюстрации. Учебная мебель.
Помещения для самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, электронную информационную образовательную среду университета.
Помещение для хранения и профилактического обслуживания учебного оборудования	Учебно-наглядные материалы (презентации).