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

Б1.В.ДВ.02.02 Информационная безопасность

Направление подготовки – 09.04.03 «Прикладная информатика»
Направленность (профиль) – Прикладная информатика в управлении организационными системами
Квалификация – магистр
Количество зачетных единиц (*часов*) – 4 (144)

Екатеринбург 2021

Разработчики: к.с.-х.н., доцент Е.В. Анянова
старший преподаватель Г.Л. Нохрина

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

Дисциплина «Информационная безопасность» относится к блоку Б1, дисциплинам по выбору части учебного плана, формируемой участниками образовательных отношений, входящего в состав основной профессиональной образовательной программы высшего образования направления подготовки 09.04.03 «Прикладная информатика», направленность (профиль) «Прикладная информатика в управлении организационными системами».

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;
- Учебные планы образовательной программы высшего образования направления 09.04.03 – Прикладная информатика (профиль – Прикладная информатика в управлении организационными системами) подготовки магистров по очной и заочной формам обучения, одобренного Ученым советом УГЛТУ (Протокол № 2 от 25.02.2020) и утвержденного ректором УГЛТУ;
- Приказ Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 896н с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. N 727н, об утверждении профессионального стандарта 06.015 «Специалист по информационным системам».
- Приказ Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. N 893н с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. N 727н об утверждении профессионального стандарта 06.016 «Руководитель проектов в области информационных систем».
- Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 09.04.03 «Прикладная информатика» (уровень высшего образования магистратура), утвержденный приказом Министерства образования и науки Российской Федерации от 19 сентября 2017 г. N 916.

Обучение по образовательной программе 09.04.03 – Прикладная информатика (профиль – Прикладная информатика в управлении организационными системами) 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.

Целью дисциплины является ознакомление обучающихся с угрозами информационной безопасности, методами и средствами защиты информации в процессе эксплуатации прикладных ИС.

Задачи дисциплины:

- формирование у обучающихся системы знаний по основным положениям теории информации, информационной безопасности и стандартами шифрования в процессе эксплуатации прикладных ИС;
- 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 при управлении ИТ-проектами, стратегией ИТ в условиях неопределенности и риска;

- формирование представлений об информационной безопасности, включая аппаратную часть и математическое обеспечение в процессе эксплуатации прикладных ИС.

Процесс изучения дисциплины направлен на формирование следующих компетенции:

ПК-1. Способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС;

ПК-8. Способен принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.

В результате освоения дисциплины обучающийся должен:

знать: основные виды угроз безопасности информации; правила защиты информации; методы и средства защиты информации; основы шифрования и криптографии, методы и модели оценки эффективности и информационной безопасности ИС в процессе эксплуатации прикладных ИС;

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, формировать систему показателей оценки эффективности информационной безопасности ИТ;

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 в процессе эксплуатации прикладных ИС в условиях неопределенности и риска.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» реализуется в рамках блока Б1.В.ДВ дисциплин по выбору части учебного плана, формируемой участниками образовательных отношений, что означает формирование в процессе обучения у магистра 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. 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
–	Проектный менеджмент. Системный анализ. Методы анализа больших наборов данных.	Правовое регулирование в информационной сфере
		Выпускная квалификационная работа

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 4 зачетные единицы (144 академических часа).

Виды учебной работы	Академические часы	
	очная форма	заочная форма
Контактная работа с преподавателем*:	**18,25**	**12,4**
в том числе: – занятия лекционного типа (Л)	6	6
– занятия семинарского типа (лабораторные работы) (ЛР)	12	6
– промежуточная аттестация (ПА)	0,25	0,4
Самостоятельная работа обучающихся	**125,75**	**131,6**
в том числе: – изучение теоретического курса	98	98
– подготовка к текущему контролю	11,75	11,6
– контрольная работа	-	6
– подготовка к промежуточной аттестации	16	16
Вид промежуточной аттестации	зачет с оценкой	
Общая трудоемкость дисциплины	**144**	

* 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	Л	ЛР	Всего контактной работы	Самостоятельная работа
1	Раздел 1. Основные составляющие информационной безопасности				
1.1	Тема 1. Понятие информационной безопасности, ее основные составляющие	0,5		0,5	4
1.2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	0,5		0,5	4
2	Раздел 2. Уровни информационной безопасности				
2.1	Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	0,5		0,5	4
2.2	Тема 4. Административный уровень информационной безопасности	0,5		0,5	4
2.3	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	0,5		0,5	4
3	Раздел 3. Программно-технические меры				
3.1	Тема 6. Основные программно-технические меры	0,5		0,5	8

№ п/п	Наименование раздела (темы) дисциплины	Л	ЛР	Всего контактной работы	Самостоятельная работа
3.2	Тема 7. Идентификация и аутентификация, управление доступом	0,5	2	2,5	10
3.3	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	0,5	2	2,5	10
3.4	Тема 9. Экранирование, анализ защищенности.	0,5	2	2,5	10
3.5	Тема 10. Обеспечение высокой доступности	0,5	2	2,5	10
3.6	Тема 11. Туннелирование и управление	0,5	2	2,5	10
3.7	Тема 12. Криптографические методы защиты информации	0,5	2	2,5	36
Итого по разделам		**6**	**12**	**18**	**109,75**
Промежуточная аттестация				0,25	16
Всего часов				**144**	

заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	Л	ЛР	Всего контактной работы	Самостоятельная работа
1	Раздел 1. Основные составляющие информационной безопасности				
1.1	Тема 1. Понятие информационной безопасности, ее основные составляющие	0,5		0,5	4
1.2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	0,5		0,5	4
2	Раздел 2. Уровни информационной безопасности				
2.1	Тема 3. Законодательный уровень информационной безопасности. Стандарты и спецификации в области информационной безопасности	0,5		0,5	4
2.2	Тема 4. Административный уровень информационной безопасности	0,5		0,5	4
2.3	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	0,5		0,5	4
3	Раздел 3. Программно-технические меры				
3.1	Тема 6. Основные программно-технические меры	0,5		0,5	8
3.2	Тема 7. Идентификация и аутентификация, управление доступом	0,5	1	1,5	10
3.3	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	0,5	1	1,5	10
3.4	Тема 9. Экранирование, анализ защищенности.	0,5	1	1,5	10
3.5	Тема 10. Обеспечение высокой доступности	0,5	1	1,5	10
3.6	Тема 11. Туннелирование и управление	0,5	1	1,5	10
3.7	Тема 12. Криптографические методы защиты информации	0,5	1	1,5	42
Итого по разделам		6	6	12	109,6
Контрольная работа				0,15	6
Промежуточная аттестация				0,25	16
Всего часов				**144**	

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 занятия.

№ п/п	Наименование занятий семинарского типа	Форма проведения занятия	Трудоёмкость, час.	
			очная	заочная
1	Тема 7. Идентификация и аутентификация, управление доступом. Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.	Лабораторная	2	1
2	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит.	Лабораторная	2	1
3	Тема 9. Экранирование, анализ защищенности.	Лабораторная	2	1
4	Тема 10. Обеспечение высокой доступности.	Лабораторная	2	1
5	Тема 11. Туннелирование и управление.	Лабораторная	2	1
6	Тема 12. Криптографические методы защиты информации.	Лабораторная	2	1
Всего часов			**12**	**6**

5.4. Детализация самостоятельной работы

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.	
			очная форма обучения	заочная форма обучения
Раздел 1. Основные составляющие информационной безопасности			**8**	**8**
1	Тема 1. Понятие информационной безопасности, ее основные составляющие	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	2	2
2	Тема 2. Распространение объектно-ориентированного подхода на информационную безопасность	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	2	2
Раздел 2. Уровни информационной безопасности			**12**	**12**
3	Тема 3. Законодательный уровень информационной безопас-	Изучение теоретического курса	2	2

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.	
			очная форма обучения	заочная форма обучения
	ности. Стандарты и спецификации в области информационной безопасности	Подготовка к текущему контролю	2	2
4	Тема 4. Административный уровень информационной безопасности	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	2	2
5	Тема 5. Процедурный уровень информационной безопасности. Управление рисками	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	2	2
Раздел 3. Программно-технические меры			**94**	**100**
6	Тема 6. Основные программно-технические меры	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	6	6
7	Тема 7. Идентификация и аутентификация, управление доступом	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	8	8
8	Тема 8. Моделирование и аудит, шифрование, контроль целостности. Протоколирование и аудит	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	8	8
9	Тема 9. Экранирование, анализ защищенности	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	8	8
10	Тема 10. Обеспечение высокой доступности	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	8	8
11	Тема 11. Туннелирование и управление	Изучение теоретического курса	2	2
		Подготовка к текущему контролю	8	8
12	Тема 12. Криптографические методы защиты информации	Изучение теоретического курса	2	6
		Подготовка к текущему контролю	34	36
Итого по разделам			**109,75**	**115,6**
Промежуточная аттестация			16	16
Всего часов			**125,75**	**131,60**

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 госу-	2019	Полнотекстовый доступ при входе

№ п/п	Реквизиты источника	Год издания	Примечание
	дарственный 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.		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. – Библиогр. в кн. – Текст: электронный.	2019	Полнотекстовый доступ при входе по логину и паролю*
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: http://www.consultant.ru/
2. Информационно-правовой портал Гарант.Ру.- Режим доступа: http://www.garant.ru/
3. «Система Главбух» - справочная система – Режим доступа: http://www.1gl.ru/
4. Программа поддержки образования «Системы Главбух». – Режим доступа: http://student.1gl.ru/

Профессиональные базы данных

1. Elibrary.ru: электронная библиотечная система: база данных содержит сведения об отечественных книгах и периодических изданиях по науке, технологии, медицине и образованию / Рос.информ. портал. – Москва, 2000– . – Режим доступа: http://elibrary.ru/
2. База данных Scopus компании Elsevier B.V. - Режим доступа: https://www.scopus.com/

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации (часть первая). Федеральный закон от 30.11.1994 № 51-ФЗ [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. http://www.consultant.ru/document/cons_doc_LAW_5142/.
2. Гражданский кодекс Российской Федерации (часть вторая). Федеральный закон от 26.01.1996 № 14-ФЗ. [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. http://www.consultant.ru/document/cons_doc_LAW_9027/.
3. Гражданский кодекс Российской Федерации (часть третья). Федеральный закон от 26.11.2001 № 146-ФЗ. [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. http://www.consultant.ru/document/cons_doc_LAW_34154/.
4. Гражданский кодекс Российской Федерации (часть четвертая). Федеральный закон от 18.12.2006 № 230-ФЗ. [Электронный ресурс] // КонсультантПлюс: справ.-правовая система. http://www.consultant.ru/document/cons_doc_LAW_64629/.
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

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 использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	**Промежуточный контроль**: контрольные вопросы к зачету с оценкой. **Текущий контроль**: опрос, тестирование, выполнение лабораторных заданий, контрольная работа для заочной формы обучения.
ПК-8. Способен принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.	**Промежуточный контроль**: контрольные вопросы к зачету с оценкой. **Текущий контроль**: опрос, тестирование, выполнение лабораторных заданий, контрольная работа для заочной формы обучения.

Этапы формирования компетенций – занятия лекционного типа, лабораторные занятия, самостоятельная работа, подготовка и защита рефератов, отчетов по лабораторным работам, контрольной работы для заочной формы обучения, подготовка и сдача экзамена, отчетов по производственным практикам, подготовка и защита ВКР.

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-1, ПК-8):

«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 магистрантом 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.

«зачтено» (удовлетворительно) – 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-1, ПК-8):

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 лабораторных заданий (текущий контроль формирования компетенций ПК-1, ПК-8):

«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 контрольной работы для заочной формы обучения (текущий контроль формирования компетенций ПК-3, ПК-8):

Контрольная работа считается зачтённой в случае получения обучающимся правильного качественного или численного ответа и её уверенной защиты (дан полный, развернутый ответ на поставленный в контрольной работе вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах изучаемой дисциплины. Могут быть допущены незначительные ошибки или недочеты, исправленные магистрантом с помощью «наводящих» вопросов). В противном случае работа не засчитывается и отправляется на доработку или на повторную защиту.

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

Контрольные вопросы для проведения опроса (текущий 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.

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

1. Информационная безопасность и ее основные компоненты.
2. Основные положения доктрины информационной безопасности в области защиты информации.
3. Стандарты в области информационной безопасности
4. Задачи обеспечения информационной безопасности на государственном уровне.
5. Классификация атак, уровни безопасности.
6. Уязвимости и политика информационной безопасности.
7. Основные угрозы и способы обеспечения безопасности
8. Основные аспекты проблемы кодирования.
9. Коды обнаруживающие и исправляющие ошибки.
10. Концепция информационной безопасности.
11. Типы кодов, примеры.
12. Основные компоненты и их назначение в стандарте шифрования данных DES.
13. Достоинства и недостатки аппаратной и программной реализации шифров.
14. Блочные системы шифрования, примеры.
15. Поточные системы шифрования. Примеры.
16. Криптоаналитические атаки и их виды.
17. Методы генерации псевдослучайных последовательностей на базе ЛРС.
18. Модели и критерии распознавания открытых текстов.
19. Понятие шифра, типы шифров их сильные и слабые стороны.
20. Принципы криптографической защиты информации. Симметричные и асимметричные криптосистемы.
21. Принципы разработки вычислительно стойких шифров.

22. Принципы построения криптосистем с открытым ключом.
23. Проблемы защиты информации в компьютерных сетях и пути их решения.
24. Проблемы идентификации и проверки подлинности.
25. Требования к шифрам и «правило Керкгоффса»
26. Управление криптографическими ключами: проблемы и методы их решения.
27. Хэш-функции и их применение.
28. Шифрование методом гаммирования. Пример.
29. Шифры замены. Примеры
30. Шифры перестановки. Примеры.
31. Электронная цифровая подпись. Правовой и технический аспекты.
32. Отличительные особенности AES от DES.
33. Межсетевые экраны и их предназначение.
34. Вирусные атаки и защита от них.
35. Виды нарушений информационной системы.
36. Целостность данных и аутентификация сообщений.
37. Административный и процедурный уровни информационной безопасности.
38. Основные положения теории информационной безопасности информационных систем.
39. Обеспечение информационной безопасности в ОС
40. Проблемы надежности шифров.
41. Классы моделей политики безопасности.
42. Политика информационной безопасности.
43. Проблемы защиты информации в глобальных компьютерных сетях.
44. Обеспечение безопасности в приложениях MS Word и MS Excel.
45. Защита информации в БД на примере MS Access.

Пример задания для контрольной работы заочной формы обучения (текущий контроль)

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 балльной 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. Обучающийся способен самостоятельно использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. Обучающийся способен самостоятельно принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.
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. Обучающийся способен с незначительными наставлениями использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. Обучающийся способен с незначительными наставлениями принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.
Пороговый	зачтено (удовлетворительно)	Теоретическое содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Обучающийся способен под руководством использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. Обучающийся способен под руководством принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.
Низкий	не 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.

Уровень сформированности компетенций	Оценка	Пояснение
		Обучающийся не способен использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС. Обучающийся не способен принимать эффективные управленческие решения по управлению ИТ-проектами, стратегией ИТ в условиях неопределенности и риска.

8. Методические указания для самостоятельной работы обучающихся

Вид учебных занятий	Организация деятельности обучающегося
Занятия лекционного типа	В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на выполнение самостоятельной работы. В ходе лекций студентам рекомендуется: - вести конспектирование учебного материала; - обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации по их применению; - задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. В рабочих конспектах желательно оставлять поля, на которых во внеаудиторное время можно сделать пометки из рекомендованной литературы, дополняющей материал прослушанной лекции, а также пометки, подчеркивающие особую важность тех или иных теоретических положений. Для успешного овладения курсом необходимо посещать все лекции, так как тематический материал взаимосвязан между собой. В случаях пропуска занятия студенту необходимо самостоятельно изучить материал и ответить на контрольные вопросы по пропущенной теме во время индивидуальных консультаций.
Занятия семинарского типа (лабораторные занятия)	Семинарские (практические занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения лабораторных занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в компьютерных классах. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса. Практические занятия – это активная форма учебного процесса. При подготовке к занятиям студенту необходимо изучить основную литературу, ознакомиться с дополнительной литературой, нормативными документами, учесть рекомендации преподавателя. Большая часть тем дисциплины предполагает выполнение заданий.
Самостоятельная работа (изучение теоретического курса, подготовка к практическим занятиям)	Самостоятельная работа – это процесс активного, целенаправленного приобретения обучающимися новых знаний, умений без непосредственного участия преподавателя, характеризующийся предметной направленностью, эффективным контролем и оценкой результатов деятельности. Самостоятельная работа, связанная с текущей проработкой курса, включает чтение и обобщение лекционного материала, а также учебной и научной литературы. Основная функция учебников – ориентировать обучающегося в системе знаний, умений и навыков, которые должны быть усвоены по данной дисциплине. Подготовка к практическим занятиям предполагает изучение лекционного материала и литературных источников по заданной тематике. Закрепле-

Вид учебных занятий	Организация деятельности обучающегося
	нию умений и навыков, формированию профессиональных компетенций по дисциплине способствует выполнение домашних заданий по указанию преподавателя, а также практических заданий для самостоятельной работы, аналогичных предлагаемым на занятиях. Перед выполнением обучающимися внеаудиторной самостоятельной работы преподаватель проводит инструктаж по выполнению задания, который включает информирование о цели и содержании задания, сроках его выполнения, ориентировочном объеме работы, основных требованиях к результатам работы и критериях оценки, возможных типичных ошибках при выполнении. Инструктаж проводится за счет объема времени, отведенного на изучение дисциплины. Контроль результатов внеаудиторной самостоятельной работы студентов может проходить в письменной, устной или смешанной форме.
Подготовка к зачету	Подготовка к зачету предполагает: - изучение рекомендуемой литературы; - изучение конспектов лекций; - участие в проводимых контрольных опросах; - тестирование по темам; - выполнение заданий. Оценка за зачет выставляется в соответствии с критериями, представленными в пункте 7.2.

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

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, лабораторное занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно-иллюстративное изложение) и лабораторно-практических методов обучения (выполнение лабораторных работ).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

- семейство коммерческих операционных систем семейства Microsoft Windows;
- офисный пакет приложений Microsoft Office;
- информационная среда 1С:Предприятие 8.3;

– программная система для обнаружения текстовых заимствований в учебных и научных работах "Антиплагиат.ВУЗ";

– Kaspersky Endpoint Security для бизнеса- Стандартный Russian Edition. 250-499 Node 2 year Educational Renewal License.

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

Реализация учебного процесса осуществляется в учебных аудиториях университета, предназначенных для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации обучающимся. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.

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

Есть помещения для хранения и профилактического обслуживания учебного оборудования.

Оснащенность аудиторий и помещений

Наименование аудиторий и специальных помещений	Оснащенность аудиторий и специальных помещений
Аудитории для занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущей и промежуточной аттестации	Учебная мебель (столы, стулья или лавки, доски), проекционное оборудование
Помещение для лабораторных занятий обучающихся	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет. Доступ к электронной информационно-образовательной среде УГЛТУ
Помещение для самостоятельной работы обучающихся	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет. Доступ к электронной информационно-образовательной среде УГЛТУ
Помещение для хранения и профилактического обслуживания учебного оборудования	Шкафы. Наглядные пособия. Плакаты. Раздаточный материал.