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.О.25 Информационная безопасность

Направление подготовки 38.03.01 «Экономика»
Направленность (профиль) «Бухгалтерский учет, анализ и аудит»
Квалификация – бакалавр
Количество зачетных единиц (*часов*) – 4 (144)

Екатеринбург 2021

Разработчик: 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

Дисциплина «Информационная безопасность» относится к обязательной части (блоку Б1) учебного плана, входящего в состав основной профессиональной образовательной программы высшего образования (ОПОП ВО) направления подготовки 38.03.01 «Экономика», направленность (профиль) «Бухгалтерский учет, анализ и аудит».

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

- Федеральный закон «Об образовании в Российской Федерации», утвержденный приказом Минобрнауки РФ № 273-ФЗ от 29.12.2012;
- Приказ Минобрнауки России № 301 от 05.04.2017 г. «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;
- Приказ Министерства труда и социальной защиты Российской Федерации от 21.02.2019 № 103н «Об утверждении профессионального стандарта «Бухгалтер»;
- Приказ Министерства труда и социальной защиты Российской Федерации от 24 июня 2015 г. № 398н «Об утверждении профессионального стандарта «Внутренний аудитор»;
- Приказ Министерства труда и социальной защиты Российской Федерации от 19 октября 2015 г. № 728н «Об утверждении профессионального стандарта «Аудитор»;
- Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) – бакалавриат по направлению подготовки 38.03.01 «Экономика», утвержденный приказом Минобрнауки России от 12.08.2020 № 954;
- Учебные планы ОПОП ВО 38.03.01 «Экономика» направленность (профиль) «Бухгалтерский учет, анализ и аудит» по очной и заочной формам обучения, одобренные Ученым советом УГЛТУ (протокол № 12 от 24.12.2020) и утвержденные ректором УГЛТУ (24.12.2020).

Обучение по образовательной программе 38.03.01 «Экономика» направленность (профиль) «Бухгалтерский учет, анализ и аудит» 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 формирование у обучающихся системных знаний и практических навыков защиты информации, освоение эффективных и функциональных средств защиты информации.

Задачи дисциплины:

- овладение теорией и методологией защиты информации;
- ознакомление с законодательством Российской Федерации в области информационной безопасности, формирование знаний и умений, необходимых для использования нормативно-правовых документов, международных и отечественных стандартов в области информационной безопасности,
- приобретение знаний и умений по организационному обеспечению информационной безопасности;
- приобретение навыков решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности.

Процесс изучения дисциплины направлен на формирование следующих компетенции:

- общепрофессиональных:

ОПК-5. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;

ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;

В результате освоения дисциплины обучающийся должен:

знать: принципы, методы, средства информационной безопасности; основные виды угроз безопасности информации; правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности; организационное обеспечение информационной безопасности; основные программные средства защиты информации; криптографические методы и средства обеспечения информационной безопасности;

уметь: оценивать состояние информационной безопасности; определять рациональные меры по обеспечению информационной безопасности при решении профессиональных задач; организовать работу персонала с конфиденциальной информацией; оперативно реагировать на угрозы информационной безопасности;

владеть: методами защиты информации и выявления угроз информационной безопасности; способами обеспечения режима конфиденциальности.

3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» реализуется в рамках блока Б1.О «Дисциплины (модули)» обязательной части 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
Информатика Пакеты прикладных программ Информационные системы в экономике	Бухгалтерский финансовый учет Налоги и налогообложение Административное право Методы принятия управленческих решений	Лабораторный практикум по финансовому и управленческому учету Оценка рисков

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*:	52,25	12,25
в том числе: – занятия лекционного типа (ЛЗ)	18	4
– занятия семинарского типа (практические занятия) (ПЗ)	34	8

Виды учебной работы	Академические часы	
	Очная форма	Заочная форма
– промежуточная аттестация (ПА)	0,25	0,25
Самостоятельная работа обучающихся (СР)	91,75	131,75
в том числе: – изучение теоретического курса (ТО)	66	114
– подготовка к текущему контролю (ТК)	14	14
– подготовка к промежуточной аттестации (ПА)	11,75	3,75
Вид промежуточной аттестации	Зачет	Зачет
Общая трудоемкость дисциплины	144	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	ЛЗ	ПЗ	Всего контактной работы	Самостоя-тельная работа
1	Основные цели и задачи курса	2	4	6	10
2	Угрозы информационной безопасности на предприятии	2	6	8	10
3	Основные программные средства защиты информации	6	10	16	30
4	Организационное обеспечение информационной безопасности	4	6	10	20
5	Правовые аспекты информационной безопасности	4	8	12	10
Итого по разделам		18	34	52	80
Промежуточная аттестация		x	x	0,25	11,75
Всего часов		**144**			

Заочная форма обучения

№ п/п	Наименование раздела (темы) дисциплины	ЛЗ	ПЗ	Всего контактной работы	Самостоя-тельная работа
1	Основные цели и задачи курса	0,5	1	1,5	16
1.1	Угрозы информационной безопасности на предприятии	0,5	1	1,5	16
1.2	Основные программные средства защиты информации	2	2	4	50
2	Организационное обеспечение информационной безопасности	0,5	2	2,5	30
2.1	Правовые аспекты информационной безопасности	0,5	2	2,5	16
Итого по разделам		4	8	12	128
Промежуточная аттестация		x	x	0,25	3,75
Всего часов		**144**			

5.2. Содержание занятий лекционного типа

Тема 1. Основные цели и задачи курса

Актуальность информационной безопасности. Основные цели и задачи системы защиты. Источники угроз и атак. Основные классификации атак. Системы критериев оценки защищенности среды.

Тема 2. Угрозы информационной безопасности на предприятии

Виды угроз информационной безопасности и их характеристика. Модели нарушителей информационной безопасности на предприятии. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на предприятии.

Тема 3. Основные программные средства защиты информации

Программные средства защиты информации. Задачи обеспечения конфиденциальности, целостности и задачи обеспечения наблюдаемости, решаемые программными средствами защиты информации. Изучение основных технологий в области аутентификации данных, криптографии и обеспечении целостности данных. Управление доступом к ресурсам автоматизированной системы.

Технические мероприятия, призванные обеспечить физическую и информационную безопасность. Технические средства для реализации мероприятий данной группы.

Обеспечение безопасности электронного документооборота. Электронная подпись. Методы и средства защиты информации при работе с удаленными базами данных. Стеганография. Компьютерные вирусы и программы типа «Троянский конь». Средства обнаружения и уничтожения компьютерных вирусов.

Тема 4. Организационное обеспечение информационной безопасности

Корпоративная политика норм и требований, предъявляемых к сотрудникам на предприятии в отношении защиты корпоративной информации. Подходы к реализации мероприятий по обеспечению информационной безопасности. Построение модели защищенной системы. Обеспечение целостности и конфиденциальности. Примеры реализации политик безопасности информации на различных предприятиях.

Тема 5. Правовые аспекты информационной безопасности

Требования к защите информации, изложенные в соответствующих Законах РФ, стандартах и нормативных документах. Сравнение с нормативными документами о защите информации и мер наказания нарушителей законов о защите информации в развитых странах.

5.3. Темы и формы занятий семинарского типа (практических занятий)

№ п/п	Наименование занятий семинарского типа (практических занятий)	Форма проведения занятия	Трудоёмкость, час.	
			очная форма обучения	заочная форма обучения
1	Основные цели и задачи курса	Решение практических заданий	4	1
2	Угрозы информационной безопасности на предприятии	Решение практических заданий	6	1
3	Основные программные средства защиты информации	Решение практических заданий	10	2
4	Организационное обеспечение информационной безопасности	Решение практических заданий	6	2
5	Правовые аспекты информационной безопасности	Решение практических заданий	8	2
Всего часов			34	8

5.4. Детализация самостоятельной работы

№ п/п	Наименование занятий семинарского типа (практических занятий)	Вид самостоятельной работы	Трудоёмкость, час.	
			очная форма обучения	заочная форма обучения
1	Основные цели и задачи курса	Изучение теоретического курса	8	14
		Подготовка к текущему контролю	2	2
2	Угрозы информационной безопасности на предприятии	Изучение теоретического курса	8	14
		Подготовка к текущему контролю	2	2
3	Основные программные средства защиты информации	Изучение теоретического курса	24	44
		Подготовка к текущему контролю	6	6
4	Организационное обеспечение информационной безопасности	Изучение теоретического курса	18	28
		Подготовка к текущему контролю	2	2
5	Правовые аспекты информационной безопасности	Изучение теоретического курса	8	14
		Подготовка к текущему контролю	2	2
Итого по разделам			80	128
Промежуточная аттестация			11,75	3,75
Всего часов			91,75	131,75

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:	2019	Полнотекстовый доступ при входе по логину и паролю*

№ п/п	Реквизиты источника	Год издания	Примечание
	https://biblioclub.ru/index.php?page=book&id=611084. – 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. Договоры с ЭБС заключаются университетом ежегодно.

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	Семестр очная форма обучения (курс - заочная)
ОПК-5. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	**Текущий контроль**: тестирование, выполнение практических заданий **Промежуточный контроль**: контрольные вопросы к зачету	5 (4)
ОПК-6. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	**Текущий контроль**: тестирование, выполнение практических заданий **Промежуточный контроль**: контрольные вопросы к зачету	5 (4)

Этапы формирования компетенций:

ОПК-5, ОПК-6 – второй (проведение занятий лекционного типа, проведение занятий семинарского типа, самостоятельная работа обучающихся, подготовка к зачету и сдача зачета).

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

Показатели и критерии оценивания устного ответа на контрольные вопросы к зачету (промежуточный контроль формирования компетенций ОПК-5, ОПК-6)

Показатель: совокупность проявленных знаний, умений, навыков. *Критерии* оценивания:

- знание принципов, методов, средств информационной безопасности;
- знание основных видов угроз безопасности информации;
- знание правового обеспечения информационной безопасности, законодательной базы, системы государственного контроля и управления в области информационной безопасности;
- знание организационного обеспечения информационной безопасности;
- знание основных программных средств защиты информации;
- знание криптографических методов и средств обеспечения информационной безопасности;
- умение оценивать состояние информационной безопасности;
- умение определять рациональные меры по обеспечению информационной безопасности при решении профессиональных задач;
- умение организовать работу персонала с конфиденциальной информацией;
- умение оперативно реагировать на угрозы информационной безопасности;
- владение методами защиты информации и выявления угроз информационной безопасности;
- владение способами обеспечения режима конфиденциальности.

«зачтено» - 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. Обучающийся:

- *на высоком уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на высоком уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

«зачтено» - 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. Обучающийся:

- *на базовом уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на базовом уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

«зачтено» - 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. Обучающийся:

- *на пороговом уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на пороговом уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

«не зачтено» – 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. Обучающийся:

- *на низком уровне* способен или неспособен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на низком уровне* способен или неспособен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6).

Показатели и критерии оценивания выполнения заданий в тестовой форме (текущий контроль формирования компетенций ОПК-5, ОПК-6)

Показатель: количество правильных ответов.

Критерии оценивания:

- знание принципов, методов, средств информационной безопасности;

- знание основных видов угроз безопасности информации;

- знание правового обеспечения информационной безопасности, законодательной базы, системы государственного контроля и управления в области информационной безопасности;

- знание организационного обеспечения информационной безопасности;

- знание основных программных средств защиты информации;

- знание криптографических методов и средств обеспечения информационной безопасности;

- владение методами защиты информации и выявления угроз информационной безопасности;

- владение способами обеспечения режима конфиденциальности.

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».*

Показатели и критерии оценивания выполнения практических заданий (текущий контроль формирования компетенций ОПК-5, ОПК-6)

Показатели: выполнение всех заданий; уровень ответа на контрольные вопросы при защите заданий. *Критерии* оценивания:

- знание принципов, методов, средств информационной безопасности;

- знание основных видов угроз безопасности информации;

- знание правового обеспечения информационной безопасности, законодательной базы, системы государственного контроля и управления в области информационной безопасности;

- знание организационного обеспечения информационной безопасности;

- знание основных программных средств защиты информации;

- знание криптографических методов и средств обеспечения информационной безопасности;

- умение оценивать состояние информационной безопасности;

- умение определять рациональные меры по обеспечению информационной безопасности при решении профессиональных задач;

- умение организовать работу персонала с конфиденциальной информацией;

- умение оперативно реагировать на угрозы информационной безопасности;

- владение методами защиты информации и выявления угроз информационной безопасности;

- владение способами обеспечения режима конфиденциальности.

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

- *на высоком уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на высоком уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

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

- *на базовом уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на базовом уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

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

- *на пороговом уровне* способен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на пороговом уровне* способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6);

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

- *на низком уровне* способен или неспособен использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-5);

- *на низком уровне* способен или неспособен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-6).

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 подготовки к зачету (промежуточная аттестация)

1. Основные понятия информационной безопасности. Задачи. Объекты защиты информации.
2. Вирусная атака. Классификация вирусов. Антивирусная защита. Виды антивирусных программ.
3. Фильтрация трафика. Обзор персональных программных межсетевых экранов
4. Технология виртуальных частных сетей.
5. Шифрование с несимметричными ключами, обзор.
6. Шифрование с симметричным ключом, обзор.
7. Защита баз данных.
8. Организационные меры по обеспечению безопасности на предприятии.
9. Защита от форс-мажор факторов.
10. Законодательство РФ в области информационной безопасности
11. Средства аутентификации: программные, физические и биологические.
12. Защита информации в операционных системах
13. Электронная цифровая подпись, принципы и примеры использования
14. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
16. Программные средства защиты.
17. Оценка качества безопасности продукции и услуг.
18. Стандарты в области информационной безопасности.

Практические задания для текущего контроля (фрагмент)

Задание 1

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

   Для этого:

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

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

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

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

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

Дешифруйте файл:

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

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

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

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

Задание 2. Исследование основных методов криптографической зашиты информации

На языке VBA или C++ написать программу шифрования и дешифрования текстового файла методом, указанным преподавателем.

Описание. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, которая определяется степенью защищенности и устойчивости как компьютерных систем в целом, так и отдельных программ.

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем

безопасности является использование криптографии и криптоподобных преобразований информации.

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 информационной системе 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 информационной безопасности
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
16. Дополните. … - это защищенность информации, информационных ресурсов и систем от случайных или преднамеренных воздействий, которые могут нанести ущерб субъектам информационных отношений.
17. Укажите основные задачи информационной безопасности:
    а) обеспечение подлинности и сохранности информации
    б) обеспечение разграничения доступа к информации и ресурсам системы
    в) обеспечение функционирования системы
    г) обеспечение централизованного сбора информации
18. Вид атаки по цели воздействия:
    а) активная атака
    б) безусловная атака
    в) атака с обратной связью
    г) атака на нарушение целостности информации
19. Основная функция брандмауэра:
    а) деление сети на подсети
    б) увеличение количества хостов в каждой подключенной подсети
    в) контроль трафика
    г) контроль учетных записей
20. Определите отличие идентификации от аутентификации:
    а) идентификация задает права доступа к объекту, аутентификация – проверку подлинности объекта прав доступа
    б) процедура идентификации описывает объект; аутентификация обеспечивает подлинность объекта
    в) идентификация – успешная попытка представить объект не тем, чем он является; аутентификация – неуспешная попытка
    г) аутентификация – процедура обмена шифрованными ключами для опознания объекта; идентификация – процедура проверки подлинности ключей
21. К внутренним источникам угроз безопасности относятся:

а) программное обеспечение, в том числе и разработанное на предприятии
б) каналы связи: Internet, модемная связь, телефонные линии, факс
в) оборудование, коммуникации, системы водоснабжения
г) форс-мажор факторы
д) персонал предприятия, в том числе временные и бывшие работники
е) всё выше перечисленное

22. Дополните. … - это набор факторов, приводящих к сбоям или неработоспособности системы, а также наносящих урон целостности информации.
23. Дополните. … - это специально написанная программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, вычислительные с целью выполнения несанкционированных действий на несущем компьютере или сети.
24. Определите возможности Пользователя, являющегося членом группы с правом чтения папки и имеющего личное разрешение на запись для той же папки:
    а) читать и записывать в эту папку
    б) читать содержимое папки
    в) только входить в папку без возможности получения списка содержимого
    г) осуществлять полный доступ к папке и ее содержимому
25. Укажите меры, необходимые для защиты от троянских программ:
    а) проверять наличие цифровой подписи
    б) никогда не устанавливать на сетевых служебных компьютерах непроверенное программное обеспечение
    в) запрашивать разрешение на прием того или иного активного объекта.
    г) использовать протокол SSL
26. ШИФРОВАНИЕ, использующее один и тот же ключ как для зашифровки, так и для расшифровки данных, называется:
    а) однонаправленным шифрованием
    б) шифрованием на симметричном ключе
    в) «закрытым» шифрованием
    г) шифрованием на ассиметричном ключе
27. Мониторинг трафика включает в себя:
    а) проверку интенсивности трафика
    б) фильтрацию трафика
    в) проверку направленности трафика
    г) проверку целостности журналов трафика
    д) проверку содержания трафика
    е) проверку действий пользователя
28. Дополните. … подтверждает правильность и подлинность информации о фирме или индивидуальном программисте.
29. В области создания средств защиты информации действуют следующие нормативные акты:
    а) документы ФСБ о информационной безопасности
    б) документы ФАПСИ (Федеральное агентство правительственной связи и информации при Президенте РФ) о разработке и сертификации средств криптографической защиты информации
    в) документы Федеральной службы по техническому и экспортному контролю о лицензировании и сертификации деятельности и средств в области защиты информации
    г) ГОСТы
30. По назначению выделяют следующие виды антивирусных программ:
    а) ревизоры
    б) иммунизаторы
    в) резидентные мониторы

г) цензоры
д) сканеры

31. Политики паролей не позволяют:
    а) задавать минимальную длину пароля
    б) устанавливать алгоритм шифрования пароля
    в) требовать неповторяемости паролей
    г) задавать срок действия пароля
32. Укажите государственные органы, обеспечивающие информационную безопасность в России:
    а) Межведомственная комиссия по государственной тайне
    б) Федеральное агентство правительственной связи и информации при Президенте РФ
    в) Федеральное агентство правительственной связи и информации при Президенте РФ
    г) Министерство внутренних дел
    д) Федеральная служба безопасности
    е) Служба внешней разведки

7.4. Соответствие шкалы оценок и уровней сформированности компетенций

По каждой компетенции в зависимости от уровня освоения преподаватель выставляет следующие оценки: «зачтено», «не зачтено».

Соответствие балльной шкалы оценок и уровней сформированных компетенций

Уровень сформированности компетенций	Оценка	Пояснение
Высокий	«зачтено»	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»	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»	Содержание дисциплины освоено частично, предусмотренные программой обучения учебные задания выполнены с замечаниями. Компетенции сформированы на пороговом уровне.
Низкий	«не зачтено»	Содержание дисциплины не освоено, компетенции не сформирована, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий.

8. Методические указания для обучающихся по освоению дисциплины

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

Вид учебных занятий	Организация деятельности обучающегося
	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 (практические занятия)	Семинарские (практические занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях. 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. Закреплению 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; - тестирование по темам; - выполнение заданий.

Вид учебных занятий	Организация деятельности обучающегося
	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;

– практические занятия по дисциплине проводятся с использованием платформы MOODLE, справочной правовой системы «Консультант Плюс», бухгалтерской справочной системы Главбух (установленные информационные банки: нормативные документы, нормативно-справочная литература, справочная информация, рекомендации, разъяснения экспертов по вопросам финансово-хозяйственной деятельности предприятия, аналитические статьи из печатных изданий, видеоматериалы и т.п.).

Для достижения цели и задач дисциплины 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 практических методов обучения (выполнение расчетных работ, практических заданий, анализ практических ситуаций).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

– семейство коммерческих операционных систем Microsoft Windows;
– офисный пакет приложений Microsoft Office;
– программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ».

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, текущего контроля и промежуточной аттестации	Учебная мебель (столы, стулья или лавки, доски), проекционное оборудование
Помещения 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.

ЛИСТ ДОПОЛНЕНИЙ И ИЗМЕНЕНИЙ РАБОЧЕЙ ПРОГРАММЫ
на 2022 - 2023 учебный год

Внести в рабочую программу Информационная безопасность
(наименование дисциплины)
для направления (специальности) 38.03.01 «Экономика»
(код направления и наименование)
направленность (профиль) программы «Бухгалтерский учет, анализ и аудит»
следующие дополнения и изменения:

№ протокола заседания кафедры	дата заседания кафедры	Раздел РПД, в который вносятся изменения	Вносимые изменения	Подпись разработчика
6	12.01.22	9	**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 Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно (PowerPoint). • Практические занятие по дисциплине проводятся с применением необходимого методического материала (методические указания, дидактический материал и т.п.) • В случае дистанционного изучения дисциплины и самостоятельной работы используется система управления обучением LMS Moodle – программное обеспечение с открытым кодом, распространяется по лицензии GNU Public License (rus)); Лекции проводятся в обычных аудиториях. Практические занятия проводятся или в обычных аудиториях, или в компьютерном классе. При проведении практических занятий студенты используют учебно-методическую литературу, при необходимости выдается раздаточный материал: задания. Тестовый контроль знаний может проводиться в обычной аудитории и в компьютерном классе. Информативно-развивающие технологии обучения используются в основном с учетом различного сочетания традиционных форм (лекция, и практическое занятие, консультация, самостоятельная работа). Университет обеспечен необходимым комплектом лицензионного программного обеспечения: - операционная система Windows 7, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно; - пакет прикладных программ Office Professional Plus 2010, License 49013351 УГЛТУ Russia 2011-09-06, OPEN 68975925ZZE1309. Срок: бессрочно; • - программная система для обнаружения текстовых	

			заимствований в учебных и научных работах «Антиплагиат.ВУЗ» (URL: https://www.antiplagiat.ru/). Astra Linux (Orel 2.12.42), Libre office, Веб-браузер.	

Дополнения и изменения согласованы:

Зав. кафедрой ИС, профессор, д-р. техн. наук _____ В.В. Побединский

Председатель учебно-методической комиссии
Социально-экономический институт
доцент, канд. ист. наук _____ А.В. Чевардин

Протокол заседания учебно-методической комиссии
Социально-экономического института
№3 от «17» февраля 2022 г.