МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

К Г Э У

АКТУАЛИЗИРОВАНО
Решением Ученого совета ИЦТЭ КГЭУ
Протокол №7 от 19.03.2024

УТВЕРЖДАЮ
Директор Института цифровых технологий и экономики

_____
Ю.В.Торкунова
«26» октября 2020 г.

КГЭУ
Подписан: ФГБОУ ВО «КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
Владелец: Беляев Эдуард Ирекович
Директор Института цифровых технологий и экономики
Сертификат: 01E4B4530091B044A4464D6B8C379A8EBA
Действителен с 04.10.2023 по 04.10.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки 42.03.01 Реклама и связи с общественностью

Направленность (профиль) Реклама и связи с общественностью в коммерческой сфере

Бакалавр

Квалификация

г. Казань, 2020

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО бакалавриат по направлению подготовки 42.03.01 Реклама и связи с общественностью (приказ Минобрнауки России от 08.06.2017 г. № 512)

Программу разработала:

доц., к.п.н. _____ Куценко С.М.

(дата, подпись)

Программа рассмотрена и одобрена на заседании кафедры-разработчика Информатика и информационно-управляющие системы,

протокол № _24___ от _26.10.2020

Заведующий кафедрой _____ Ю.В. Торкунова

(подпись)

Программа рассмотрена и одобрена на заседании выпускающей кафедры философии и медиакоммуникаций,
протокол № _15_ от 26.10.2020

Заведующий кафедрой _____ Э.Б. Миннулина

(подпись)

Программа одобрена на заседании методического совета института
_ЦТЭ_____протокол № 2 от 26.10.2020

Зам. директора института ЦТЭ _____ Косулин В.В.

(подпись)

Программа принята решением Ученого совета института ЦТЭ
протокол № № 2 от 26.10.2020

Согласовано:

Руководитель ОПОП _____ Э.Б. Миннулина

(подпись, дата)

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины «Информационная безопасность организации» является развитие творческих подходов при решении сложных научно-технических задач, связанных с обеспечением информационной безопасности личности, общества и государства.

Задачами дисциплины являются: дать знания по вопросам: обеспечение информационной безопасности личности, общества и государства; методологии создания систем защиты информации и систем защиты от информации; методов и средств информационного противоборства; оценки защищенности и обеспечения информационной безопасности компьютерных систем; политики информационной безопасности компании; стандартов и нормативных документов в области информационной безопасности.

Компетенции, формируемые у обучающихся, запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
Общепрофессиональные компетенции (ОПК)		
ОПК- 6 Способен использовать в профессиональной деятельности современные технические средства и информационно-коммуникационные технологии	ОПК 6.1 Отбирает для осуществления профессиональной деятельности необходимое техническое оборудование и программное обеспечение	знать: - цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства (З1) - программное обеспечение для защиты информации вычислительных устройствах и сетях (З2); уметь: - выявлять и классифицировать угрозы информационной безопасности (У1) - применять программное обеспечение с целью защиты информации (У2) владеть: - навыками использования технического оборудования и программного обеспечения для защиты информации (В1).

2. Место дисциплины в структуре ОПОП

Дисциплина Информационная безопасность относится к обязательной части учебного плана по направлению подготовки 42.03.01 Реклама и связи с общественностью

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др.[1]

ОПК 6.2;	Информатика	
УК-3.1; УК-3.2; УК-3.3; УК-3.4; ПК-1.1; ПК-1.2; ПК-1.3; ПК-1.4; ПК-1.5; ПК-3.3; ПК-3.4		Производственная практика (технологическая)
УК-7.1; УК-7.2; УК-7.3; УК-8.1; УК-8.2; УК-8.3; ПК-1.1; ПК-1.2; ПК-1.3; ПК-1.4; ПК-1.5		Производственная практика (преддипломная)

Знать: – основные положения теории информации;

– принципы функционирования аппаратных средств вычислительных систем;

– форматы представления данных в ЭВМ;

– основные приемы алгоритмизации и программирования на языке высокого уровня

Уметь:

– разрабатывать алгоритмы решения;

– программировать задачи обработки данных в предметной области;

Владеть:

- навыками работы с персональным компьютером на высоком пользовательском уровне;

– основами работы с научно-технической литературой и технической документацией по программному обеспечению.

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единицы (ЗЕ), всего 108 часов, из которых 53 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 16 час., занятия семинарского типа (практические, лабораторные работы) - 32 час., групповые и индивидуальные консультации 2 час., прием экзамена (КПА) - 1 час., самостоятельная работа обучающегося 20 час, контроль самостоятельной работы (КСР) - 2 час.

Вид учебной работы	Всего часов	Семестр
		3
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	53	53
Лекции (Лек)	16	16
Практические (семинарские) занятия (Пр)	16	16
Лабораторные работы (Лаб)	16	16
Контроль самостоятельной работы и иная контактная работа (КСР	2	2
Консультации (Конс)	2	2
Контактные часы во время аттестации (КПА)	1	1
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ (СРС), в том числе:	20	20
Подготовка к промежуточной аттестации в форме: (экзамен)	35	35
ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (За – зачет, ЗО – зачет с оценкой, Э – экзамен)	Эк	Эк

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	**Семестр**	**Распределение трудоемкости (в часах) по видам учебной работы, включая СРС**									**Формируемые результаты обучения (знания, умения, навыки)**	**Литература**	**Формы текущего контроля успеваемости**	**Формы промежуточной аттестации**	**Максимальное количество баллов по балльно - рейтинговой системе**
		Занятия лекционного типа	Занятия практического / семинарского типа	Лабораторные работы	Г	Самостоятельная работа студента, в	Контроль самостоятельной работы	*подготовка к промежуточной аттестации*	Сдача зачета / экзамена	**Итого**					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Раздел 1. Теоретические аспекты информационной безопасности	3	2				4				6	ОПК 6.1-31,	Л1.1, Л2.1	Тест		15

Раздел 2 Информационные угрозы и их виды	3	4	4	4		4				16	ОПК 6.1-З1, ОПК 6.1-З2 ОПК 6.1-У1, ОПК 6.1- ОПК 6.1-У2, ОПК 6.1-В1	Л1.1, Л1.2	Тест		15
Раздел 3. Принципы построения системы информационной безопасности	3	6	8	8		4				26	ОПК 6.1-З1, ОПК 6.1-З2 ОПК 6.1-У1, ОПК 6.1-У2, ОПК 6.1-В1	Л1.1, Л1.2	Тест		15
Раздел 4. Организация системы защиты информации организации	3	4	4	4		8	2			22	ОПК 6.1-З1, ОПК 6.1-З2 ОПК 6.1-У1, ОПК 6.1-У2, ОПК 6.1-В1	Л1.1, Л1.2	Рфр		15
Промежуточная аттестация	3				2			35	1	38	ОПК 6.1-З1, ОПК 6.1-З2 ОПК 6.1-У1, ОПК 6.1-У2, ОПК 6.1-В1	Л1.1, Л1.2		Э	40
Итого	3	**16**	**16**	**16**	**2**	**20**	**2**	**35**	**1**	**108**					**100**

3.3. Тематический план лекционных занятий

№ п/п	Темы лекционных занятий	Трудоемкость, час.
1	Основные понятия информационной безопасности	2
2	Экономическая информация как товар и объект безопасности. Коммерческая тайна	2
3	Информационные угрозы и их классификация.	2
4	Компьютерные вирусы, их классификация. Антивирусные программы, их классификация. Вредоносные программы.	2
5	Компьютерные преступления и наказания. Субъекты и предпосылки компьютерных преступлений.	2

6	Государственное регулирование информационной безопасности. Подходы, принципы, методы и средства обеспечения безопасности	2
7	Организационно-техническое обеспечение компьютерной безопасности.	2
8	Методы шифрования. Электронная подпись.	2
	Всего	**16**

3.4. Тематический план практических занятий

№ п/п	Темы практических занятий	Трудоемкость, час.
1	Доктрина информационной безопасности	2
2	Риски информационной безопасности	2
3	Применение алгоритмов шифрования	4
4	Парольная защита	2
5	Обеспечение и обработка безопасности персональных данных в организации	4
6	Оценка ущерба от реализации угроз	2
	Всего	**16**

3.5. Тематический план лабораторных работ

№ п/п	Темы лабораторных работ	Трудоемкость, час.
1	Шифр Цезаря	4
2	Аддитивные шифры	4
3	Требования по обеспечению информационной безопасности организации	4
4	Анализ рисков выбранной организации	4
	Всего	**16**

3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудоемкость, час
1	Изучение теоретического материала, подготовка к практическому занятию	Изучение основных понятий информационной безопасности, изучение Доктрины информационной безопасности. Подготовка к тестированию	5
2	Изучение теоретического материала, выполнение теста	Изучение Постановления № 35 «О перечне сведений, которые не могут составлять коммерческую тайну. Изучение действий и событий, нарушающих информационную безопасность	5
3	Изучение теоретического материала, подготовка к практическому занятию	Изучение методических, организационных и реализационных принципов информационной безопасности, подготовка к тестированию.	5
4	Изучение теоретического материала, подготовка к практическому занятию	Изучение особенностей применения цифровой подписи. Изучение механизмов защиты корпоративных сетей. Подготовка к тестированию	5
	Итого:		20

4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями, семинарами и с лабораторными работами, самостоятельное изучение определённых разделов) и современные образовательные технологии, направленные на обеспечение развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств: интерактивные лекции, групповые дискуссии, анализ ситуаций.

При реализации дисциплины "Информационная безопасность" по образовательной программе направления подготовки бакалавриата 42.03.01 "Реклама и связи с общественностью" применяются электронные образовательные технологии.

В процессе обучения используются:

- электронные образовательные ресурсы (ЭОР), размещенные в личных кабинетах студентов Электронного университета КГЭУ, URL: http://lms.kgeu.ru

5. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Текущий контроль успеваемости осуществляется в течение семестра, включает: защиты рефератов, проведение компьютерного тестирования.

Итоговой оценкой результатов освоения дисциплины является оценка, выставленная во время промежуточной аттестации обучающегося (экзамен) с учетом результатов текущего контроля успеваемости. На экзамен выносятся теоретические и практические задания, проработанные в течение семестра на учебных занятиях и в процессе самостоятельной работы обучающихся. Экзаменационные билеты содержат 2 теоретических заданий и 1 задание практического характера.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (индикатора достижения компетенции) по итогам освоения дисциплины:

Планируемые результаты обучения	Обобщенные критерии и шкала оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
Полнота знаний	*Уровень знаний ниже минимальных требований, имеют место грубые ошибки*	*Минимально допустимый уровень знаний, имеет место много негрубых ошибок*	*Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок*	*Уровень знаний в объеме, соответствующем программе подготовки, без ошибок*
Наличие умений	*При решении*	*Продемонстрированы основные*	*Продемонстрированы все основные умения,*	*Продемонстриро-*

	стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки	*умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме*	*решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами*	*ваны все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме*
Наличие навыков (владение опытом)	*При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки*	*Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами*	*Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами*	*Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов*
Характеристика сформированности компетенции (индикатора достижения компетенции)	*Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач*	*Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач*	*Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач*	*Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач*
Уровень сформированности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено			не зачтено
ОПК-6		*Знать:*				

		цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства ($З_1$)	Свободно и в полном объеме описывает все цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства	Достаточно полно знает цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства, допускает неточности	Плохо описывает цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства, допускает много ошибок	Не знает цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства
		программное обеспечение для защиты информации вычислительных устройствах и сетях ($З_2$)	Свободно и в полном объеме знает программное обеспечение для защиты информации вычислительных устройствах и сетях	Достаточно полно знает программное обеспечение для защиты информации вычислительных устройствах и сетях	Плохо знает программное обеспечение для защиты информации вычислительных устройствах и сетях	Не знает программное обеспечение для защиты информации вычислительных устройствах и сетях
		Уметь:				
	ОПК-6.1	выявлять и классифицировать угрозы информационной безопасности ($У_1$)	Свободно выявляет и классифицирует угрозы информационной безопасности	Умеет выявлять и классифицировать угрозы информационной безопасности, допускает незначительные ошибки	Слабо ориентируется в классификации угроз информационной безопасности	Не умеет выявлять и классифицировать угрозы информационной безопасности
		- применять программное обеспечение с целью защиты информации ($У_2$)	Свободно применяет программное обеспечение	Умеет применять программное обеспечение, допускает незначительные ошибки	Имеет минимальный набор навыков применения программного обеспечения	Не умеет применять программное обеспечение
		Владеть:				
		навыками формальной постановки и решения задачи обеспечения информационной безопасности организации ($В_1$)	Продемонтрированы навыки формальной постановки и решения задачи обеспечения информационной безопасности организации	Продемонстрированы базовые навыки формальной постановки и решения задачи обеспечения информацион	Имеет минимальный набор навыков использования навыков формальной постановки и решения задачи	Не продемонстрированы базовые навыки формальной постановки и решения задачи обеспечения

				ной безопасности организации, Допущен ряд мелких ошибок.	обеспечения информационной безопасности организации	информационной безопасности организации

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины. Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре-разработчике в бумажном и электронном виде.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Основная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электрон-ного ресурса	Кол-во экз. в библио-теке КГЭУ
1	Мельников В. П., Куприянов А. И., Васильева Т. Ю	Информационная безопасность	учебник	М.: Кнорус	2018	https://www.book.ru/book/9 29884	
2	Шаньгин В. Ф.	Информационная безопасность	учебник	М.: ДМК Пресс	2014	http://ibooks.ru/reading.php?productid=344097.	

Дополнительная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие, др.)	Место издания, издательство	Год издания	Адрес электрон-ного ресурса	Кол-во экз. в библио-теке КГЭУ
1	Бабаш А. В., Баранова Е. К., Мельников Ю. Н..	Информационная безопасность. Лабораторный практикум (+CD)	учебное пособие	М.: Кнорус	2016	https://www.book.ru/book/9 18700/	

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка

1	*Электронно-библиотечная система «Лань»*	https://e.lanbook.com/
2	*Электронно-библиотечная система «ibooks.ru»*	https://ibooks.ru/

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	*Официальный интернет-портал правовой информации*	http://pravo.gov.ru	http://pravo.gov.ru
2	*Справочно-правовая система по законодательству РФ*	http://garant.ru	http://garant.ru

6.2.3. Информационно-справочные системы

№ п/п	Наименование информационно-справочных систем	Адрес	Режим доступа
1	*Научная электронная библиотека*	http://elibrary.ru	http://elibrary.ru
2	*Российская государственная библиотека*	http://www.rsl.ru	http://www.rsl.ru

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Описание	Реквизиты подтверждающих документов
1	Браузер Chrome	Система поиска информации в сети интернет	Свободная лицензия Неискл. право. Бессрочно
2	Браузер Firefox	Система поиска информации в сети интернет	Свободная лицензия Неискл. право. Бессрочно
3	OpenOffice	Пакет офисных приложений	Свободная лицензия Неискл. право. Бессрочно
4	LMS Moodle	ПО для эффективного онлайн-взаимодействия преподавателя и студента	Свободная лицензия Неискл. право. Бессрочно

7. Материально-техническое обеспечение дисциплины

№ п/п	Вид учебной работы	Наименование специальных помещений и помещений для СРС	Оснащенность специальных помещений и помещений для СРС
1	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа	доска аудиторная, акустическая система, проектор, усилитель-микшер для систем громкой связи, экран, микрофон, миникомпьютер, монитор
2	Практические занятия	Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	доска аудиторная, персональный компьютер (25 шт.)

		Компьютерный класс с выходом в Интернет	доска аудиторная, персональный компьютер (25 шт.)
3	Лабораторные работы	Учебная лаборатория	доска аудиторная, персональный компьютер (25 шт.)
4	Самостоятель-ная работа обучающегося	Компьютерный класс с выходом в Интернет В-600а	моноблок (30 шт.), система виденаблюдения (6 видеокамер), проектор, экран

8. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению

подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;

- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;

- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;

- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;

- обеспечивается необходимый уровень освещенности помещений;

- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

Структура дисциплины по заочной форме обучения

Вид учебной работы	Всего часов	Курс
		2
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ, в т.ч. по РУП:	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ	21	21
Лекции (Лк)	6	6
Практические занятия (ПР)	6	6
Лабораторные занятия (Лаб)	4	4
Контроль промежуточной аттестации (КПА)	1	1
Контроль самостоятельной работы и иная контактная работа(КСР)	4	4
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	79	79
Подготовка к промежуточной аттестации в форме: экзамен	8	8
ФОРМА ПРОМЕЖУТОЧНОЙАТТЕСТАЦИИ	Эк	Эк

Лист внесения изменений

Дополнения и изменения в рабочей программе дисциплины на 20___ /20____ учебный год

В программу вносятся следующие изменения:

1. _____

2. _____

3. _____

Указываются номера страниц, на которых внесены изменения, и кратко дается характеристика этих изменений

Программа одобрена на заседании кафедры –разработчика Информатика и информационно-управляющие системы, , протокол № _24___ от _26.10.2020

Заведующий кафедрой _____ Ю.В. Торкунова

Программа одобрена на заседании методического совета института _ЦТЭ_____протокол № 2 от 26.10.2020

Зам. директора института ЦТЭ _____ Косулин В.В.
(подпись)

Согласовано:

Руководитель ОПОП _____ Э.Б. Миннулина
Подпись, дата

Приложение к
рабочей
программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

КГЭУ

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по дисциплине

Информационная безопасность

Направление подготовки — 42.03.01 Реклама и связи с общественностью

Направленность (профиль) — Реклама и связи с общественностью в коммерческой сфере

Квалификация — Бакалавр

г. Казань, 2020

Оценочные материалы по дисциплине Информационная безопасность - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенции:
ОПК 6.1 Отбирает для осуществления профессиональной деятельности необходимое техническое оборудование и программное обеспечение

Текущий контроль успеваемости обеспечивает оценивание процесса обучения по дисциплине. При текущем контроле успеваемости используются следующие оценочные средства: защита практических работ; презентаций рефератов, тестирование с использованием компьютера. Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 2 курс 3 семестр. Форма промежуточной аттестации - экзамен.

Оценочные материалы включают задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с рабочей программой дисциплины.

1.Технологическая карта

Семестр _3__

Номер раздела/ темы дисциплины	Вид СРС	Наименование оценочного средства	Запланированные дескрипторы освоения дисциплине	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачтено	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
1	Изучение теоретического материала	Тест	ОПК 6.1	<7	7-9	10-11	12-15
2	Изучение теоретического материала	Тест	ОПК 6.1	<7	7-10	10-12	12-15
3	Изучение теоретического материала	Тест	ОПК 6.1	<8	8-10	10-13	13-15
4	Изучение теоретического материала	Рфр	ОПК 6.1	<8	8-10	10-13	13-15
Всего баллов				менее 30	30-39	40-49	50-60

Промежуточная аттестация							
	Подготовка к экзамену	Задания к экзамену	ОПК 6.1	менее 25	25-29	30-34	35-40
Итого баллов				**0-54**	**55-69**	**70-84**	**85-100**

2. Перечень оценочных средств[2]

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Реферат (Рфр)	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее	Темы рефератов
Тест (Тест)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Комплект тестовых заданий
Экзамен (Экз)	Средство контроля усвоения учебного материала разделов дисциплины, организованное в виде письменной работы и последующего собеседования преподавателя с обучающимся	Экзаменационные билеты по темам/разделам дисциплины

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	Тест
Представление и содержание оценочных материалов	Тестовые задания по разделу 1 «Теоретические аспекты информационной безопасности». Примеры тестовых заданий: 1. Информация – это а) сведения, поступающие от СМИ; б) только документированные сведения о лицах, предметах, фактах, событиях; в) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; г) только сведения, содержащиеся в электронных базах данных. 2. Информации свойственно а) не исчезать при потреблении; б) становиться доступной, если она содержится на материальном носителе; в) подвергаться только "моральному износу"; г) всё выше перечисленное. 3. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных – это

	а) защита информации; б) компьютерная безопасность; в) защищенность информации; г) безопасность данных. 4. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним – это а) информационная война; б) информационное оружие; в) информационное превосходство. 5. Что называют источником конфиденциальной информации? а) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников; б) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе; в) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники; г) это защищаемые предприятием сведения в области производства и коммерческой деятельности; д) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации. 6. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации? а) получить, изменить, а затем передать ее конкурентам; б) размножить или уничтожить ее; в) получить, изменить или уничтожить; г) изменить и уничтожить ее; д) изменить, повредить или ее уничтожить
Критерии оценки и шкала оценивания в баллах	При оценке тестовых заданий учитываются следующие критерии: Количество правильных ответов Баллы 8-10 15 6-7 11 4-5 7 Менее 4 0 Максимальное количество баллов - 15
Представление и содержание оценочных материалов	Тестовые задания по разделу 2 «Информационные угрозы и их виды». Примеры тестовых заданий: 1. Главная причина существования многочисленных угроз информационной безопасности – это а) просчеты при администрировании информационных систем; б) действия злоумышленников и хакеров; в) необходимость постоянной модификации информационных систем; г) любопытство и происки недоброжелателей; д) сложность современных информационных систем. 2. Окно опасности появляется в случае, когда а) становится известно о средствах использования уязвимости; б) появляется возможность использовать уязвимость; в) устанавливается программное обеспечение. 3. К случайным не относится угроза а) ошибка персонала; б) форс- мажор; в) ошибка автоматизированных систем; г) программы закладки. 4. Атака называется безусловной в случае, когда а) пользователь принес вирус на дискете; б) пользователь открыл зараженное письмо, которое парализовало работу на компьютере; в) злоумышленник открыто похитил диск с информацией, оставленный без присмотра; г) на ПК обнаружен вирус, передающий информацию в интернет.

	5. Незадокументированная возможность, содержащаяся в полезной программе, называется а) троянец; б) червь; в) программа-шутка; г) программа закладка.
Критерии оценки и шкала оценивания в баллах	При оценке тестовых заданий учитываются следующие критерии: Количество правильных ответов Баллы 8-10 15 6-7 12 4-5 10 Менее 4 0 Максимальное количество баллов - 15
Представление и содержание оценочных материалов	Тестовые задания по разделу 3 «Принципы построения системы информационной безопасности». Примеры тестовых заданий: 1. Какие средства использует инженерно-техническая защита (по функциональному назначению)? а) программные, аппаратные, криптографические, технические; б) программные, физические, шифровальные, криптографические; в) программные, аппаратные, криптографические физические; г) физические, аппаратные, материальные, криптографические; д) аппаратные, физические, программные, материальные. 2. Что включают в себя технические мероприятия по защите информации? а) поиск и уничтожение технических средств разведки; б) кодирование информации или передаваемого сигнала; в) подавление технических средств постановкой помехи; г) применение детекторов лжи; д) все вышеперечисленное. 3. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете? а) недопущение нарушителя к вычислительной среде; б) защита вычислительной среды; в) использование специальных средств защиты информации ПК от несанкционированного доступа; г) все вышеперечисленные; д) правильного ответа нет.
Критерии оценки и шкала оценивания в баллах	При оценке тестовых заданий учитываются следующие критерии: Количество правильных ответов Баллы 8-10 15 6-7 13 4-5 10 Менее 4 0 Максимальное количество баллов - 15
Наименование оценочного средства	Реферат
Представление и содержание оценочных материалов	Темы рефератов к 4 разделу: 1. Субъекты компьютерных преступлений. 2. Предпосылки компьютерных преступлений. 3. Государственное регулирование информационной безопасности. 4. Методологические принципы информационной безопасности. 5. Организационные принципы информационной безопасности. 6. Реализационные принципы информационной безопасности.

Критерии оценки и шкала оценивания в баллах	1. Знание материала содержание материала раскрыто в полном объеме, предусмотренном программой дисциплины – 5 балла; содержание материала раскрыто неполно, показано общее понимание вопроса, достаточное для дальнейшего изучения программного материала – 3 балл; не раскрыто основное содержание учебного материала – 0 баллов; 2. Последовательность изложения содержание материала раскрыто последовательно, достаточно хорошо продумано – 5 балла; последовательность изложения материала недостаточно продумана – 3 балл; путаница в изложении материала – 0 баллов; 3. Применение конкретных примеров показано умение иллюстрировать материал конкретными примерами – 5 балла; приведение примеров вызывает затруднение – 3 балл; неумение приводить примеры при объяснении материала – 0 баллов; Количество баллов: максимум –15

4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	**Экзамен**
Представление и содержание оценочных материалов	Оценочные материалы, вынесенные на экзамен, состоят из экзаменационных билетов. Билет содержит два вопроса по теоретическому материалу и задание практического характера для проверки практических умений. Всего 25 экзаменационных билетов. Пример экзаменационных билетов: Билет 1. 1. Сведения, относящиеся к конфиденциальной информации. 2. Электронная цифровая подпись. 3. Зашифровать свою фамилию и имя, применяя алгоритм «Полибианский квадрат» Билет 2. 1. Защита от компьютерных вирусов. 2. Государственное регулирование информационной безопасности. 3. Зашифровать свою фамилию и имя, применяя алгоритм «Шифр Гронсфельда»
Критерии оценки и шкала оценивания в баллах	Число баллов, которое может получить обучающийся за экзамен, составляет от 20 до 40. При выставлении баллов за ответы на вопросы и задание в билете учитываются следующие критерии: При выставлении баллов за ответы на вопросы учитываются следующие критерии: *1.* Знание понятий, категорий *2.* Владение методами и технологиями, запланированными в РПД *3.* Владение специальными терминами и использование их при ответе. *4.* Умение объяснять, делать выводы и обобщения, давать аргументированные ответы *5.* Логичность и последовательность ответа Ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа – **29-32** баллов. Ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение

	терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна – две неточности в ответе – **24-28** балла. Ответ не полный, с недостаточной глубиной и полнотой раскрытия – **20-23** баллов. При выставлении баллов за задание в билете учитываются правильность выполнения практического задания Задание выполнено полностью – **8** балла Задание выполнено с ошибками – **4-7** балла Много ошибок – **1-3** Не выполнено – **0** баллов **Максимальное количество баллов за экзамен – 40 баллов**