



КГУ

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



КГУ

Подписан: ФГБОУ ВО «КГУ»,
КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ
ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
Владелец: Торкунова Юлия Владимировна,
Директор цифровых технологий и экономики,
Сертификат: 04637A9600B7AE93974C7182805C6B90EF
Действителен с 17.06.2022 по 17.06.2023

УТВЕРЖДАЮ
Директор ИЦТЭ

 Ю.В. Торкунова
«28» октября 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки

46.03.02 Документоведение и архивоведение

Направленность

Документоведение и документационное
обеспечение управления

Квалификация

Бакалавр

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО 3+ по направлению подготовки 46.03.02 Документоведение и архивоведение (уровень бакалавриата) (приказ Минобрнауки России от 06.03.2015 г. № 176)

Программу разработал:

доцент, к.пед.н.



С.М. Куценко.

Программа рассмотрена и одобрена на заседании кафедры-разработчика «Информатика и информационно-управляющие системы», протокол № 24 от 26.10.2020

Заведующий кафедрой ИИУС Ю.В. Торкунова



Программа рассмотрена и одобрена на заседании выпускающей кафедры «Менеджмент», протокол № 3 от 09.10.2020

Зав. кафедрой
«Менеджмент»

А.В. Махиянова

Программа одобрена на заседании методического совета ИЦТЭ, протокол № 2 от 26.10.2020

Зам. директора ИЦТЭ



/В.В.Косулин/

Программа принята решением Ученого совета ИЦТЭ, протокол № 2 от 26.10.2020

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 дескрипторами достижения компетенций:

Код и наименование компетенции	Запланированные результаты обучения по дисциплине (знать, уметь, владеть)
ПК-17 Владение методами защиты информации	знать: цели, задачи, принципы и основные направления обеспечения информационной безопасности личности, общества, государства(31) уметь: выявлять и классифицировать угрозы информационной безопасности и применять методы защиты (У1); владеть: навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем (В ₁).

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана по направлению подготовки бакалавров 46.03.02 Документоведение и архивоведение, направленность (профиль) Документоведение и документационное обеспечение управления.

Для освоения дисциплины обучающийся должен:

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
 - принципы автономной отладки и тестирования программ.
- уметь:
- разрабатывать алгоритмы решения;
 - программировать задачи обработки данных в предметной области;
 - выполнять тестирование и отладку программ.
- 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 зачетные единицы (ЗЕ), всего 108 часов, из которых 53 часа составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 16 час., практические занятия 16 час., лабораторные работы 16 час, консультации 2 час., контактные часы во время промежуточной аттестации (КПА) - 1 час., контроль самостоятельной работы (КСР) 2 часа, самостоятельная работа обучающегося 20 час. Практическая подготовка по виду профессиональной деятельности составляет 32 час.

Вид учебной работы	Всего зачетных единиц	Всего часов	семестр
			3
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ, в т.ч. по РУП:	3	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ	-	53	53
Лекции (Лк)	-	16	16
Практические занятия (ПР)		16	16
Лабораторные занятия (ЛЗ)	-	16	16
КПА		1	1
Контроль самостоятельной работы (КСР)		2	2
Консультации (К)		2	2
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	-	20	20
ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ (Э – экзамен)	-	35	Э

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	Групповые консультации	Самостоятельная работа студента	Контроль самостоятельной работы (КСР)	подготовка к промежуточной аттестации	Сдача зачета / экзамена	Итого					
1	2	3	4	5	6	7		8	9	10	11	12	13	14	15
Раздел 1. Теоретические аспекты информационной безопасности Лекция «Основные понятия информационной безопасности» Лабораторная работа «Шифр Цезаря»	3	2				4				6	31	10, 1д	Тест		15
Раздел 2. Информационные угрозы и их виды Лекции «Экономическая информация как товар и объект безопасности. Коммерческая тайна» «Информационные угрозы и их классификация» Лабораторная работа «Шифр Цезаря» Практические занятия « Доктрина информационной безопасности » «Риски информационной	3	4	4	4		4				16	31, У1, В1	10, 20, 2д	Тест		15

безопасности»															
Раздел 3. Принципы построения системы информационной безопасности Лекции « Вредоносные программы» «Компьютерные преступления и наказания. Субъекты и предпосылки компьютерных преступлений» «Государственное регулирование информационной безопасности» Лабораторные занятия «Аддитивные шифры» «Требования по обеспечению информационной безопасности организации» Практические занятия «Применение алгоритмов шифрования» (4 часа) «Обеспечение и обработка безопасности персональных данных» (4 часа)	3	6	8	8	4				26	31, у1,В1	1о, 2о, 1д	Тест		15	
Раздел 4. Организация системы защиты информации организации Лекции «Организационно-техническое обеспечение компьютерной безопасности» «Методы шифрования. Электронная	3	4	4	4	8	2			22	31, у1,В1	1о, 2о, 1д. 2д	Рфр		15	

подпись» Лабораторная работа « Анализ рисков выбранной организации» Практические занятия «Оценка ущерба от реализации угроз»															
Экзамен	3				2			35	1	38		1о, 2о, 1,2 д		Э	40
Итого	3	16	16	16	2	20	2	35	1	108					100

4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями, 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: групповые дискуссии, анализ ситуаций. При реализации дисциплины применяются электронное обучение и дистанционные образовательные технологии. В образовательном процессе используются электронные образовательные ресурсы (ЭОР), размещенные в личных кабинетах студентов Электронного университета КГЭУ, URL: <http://e.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: индивидуальный и групповой опрос (устный или письменный), защиты лабораторных работ; 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 (дескрипторы 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	<i>Уровень знаний ниже минимальных требований, имеют место грубые ошибки</i>	<i>Минимально допустимый уровень знаний, имеет место много негрубых ошибок</i>	<i>Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок</i>	<i>Уровень знаний в объеме, соответствующем программе подготовки, без ошибок</i>
Наличие умений	<i>При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки</i>	<i>Продemonстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме</i>	<i>Продemonстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами</i>	<i>Продemonстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме</i>
Наличие навыков (владение опытом)	<i>При решении стандартных задач не продемонстрированы базовые навыки, имеют место грубые ошибки</i>	<i>Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами</i>	<i>Продemonстрированы базовые навыки при решении стандартных задач с некоторыми недочетами</i>	<i>Продemonстрированы навыки при решении нестандартных задач без ошибок и недочетов</i>
Характеристика сформированности компетенции	<i>Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач</i>	<i>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</i>	<i>Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач</i>	<i>Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач</i>
Уровень сформированности компетенции	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код 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
ПК-5	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
	Уметь:				
	выявлять и классифицировать угрозы информационной безопасности и применять методы защиты (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
	Владеть:				
	навыками формальной постановки и решения задачи обеспечения информационной безопасности организации (В ₁)	Продемонстрированы навыки формальной постановки и решения задачи обеспечения информационной безопасности организации	Продемонстрированы базовые навыки формальной постановки и решения задачи обеспечения информационной безопасности организации, Допущен ряд мелких ошибок.	Имеет минимальный набор навыков использования навыков формальной постановки и решения задачи обеспечения информационной безопасности организации	Не продемонстрированы базовые навыки формальной постановки и решения задачи обеспечения 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 электронного ресурса	Кол-во экз. в библиотеке 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 электронного ресурса	Кол-во экз. в библиотеке 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/	
2	Куняев Н.Н.	Конфиденциальное делопроизводство и защищенный электронный документооборот	Учебник	М.: Логос	2013	URL: https://ibooks.ru/reading.php?productid=29403	

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№	Наименование электронных и интернет-ресурсов	Ссылка
---	--	--------

п/п		
1	<i>Электронно-библиотечная система «Лань»</i>	https://e.lanbook.com/
2	<i>Электронно-библиотечная система «ibooks.ru»</i>	https://ibooks.ru/

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
1	<i>Официальный интернет-портал правовой информации</i>	http://pravo.gov.ru	
2	<i>Справочно-правовая система по законодательству РФ</i>	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	
2	Российская государственная библиотека	http://www.rsl.ru	

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	описание	Реквизиты подтверждающих документов
1	Windows 7 Профессиональная (Pro)	лицензионное	Договор № 2011.25486 от 28.11.2011, ЗАО «Софт Лайн Трейд». Неискл. право. Бессрочно
2	Операционная система Windows 7 Профессиональная (сертифицированная ФСТЭК).	лицензионное	Договор ПО ЛИЦ № 0000/20, ЗАО «ТаксНет Сервис». Неискл. право. Бессрочно.
3	Программное обеспечение: Windows 10	лицензионное	Договор № Tr096148 от 29.09.2020, ООО "Софтлайн трейд". Неискл. право. До 14.09.2021
4	Office Standard 2007 Russian OLP NL AcademicEdition+	лицензионное	Договор №21/2010 от 04.05.2010, ЗАО «Софт Лайн Трейд». Неискл. право. Бессрочно.
5	Office Professional Plus 2007 Russian OLP NL AcademicEdition	лицензионное	Договор №21/2010 от 04.05.2010, ЗАО «Софт Лайн Трейд». Неискл. право. Бессрочно.
6	LMS Moodle	свободно	Свободная лицензия. Неискл. право. Бессрочно.
7	Браузер Chrome	свободно	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, экран на штативе, проектор, компьютер в комплекте с монитором (8 шт.)
2	Практические занятия	Учебная аудитория для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Доска аудиторная, экран на штативе, проектор, компьютер в комплекте с монитором (8 шт.)
3	Лабораторные работы	Учебная лаборатория	Доска аудиторная, экран на штативе, проектор, компьютер в комплекте с монитором (8 шт.)

4	Самостоятельная работа обучающегося	Компьютерный класс с выходом в Интернет В-600а	Моноблок (30 шт.), система видеонаблюдения (6 видеокамер), проектор, экран
		Читальный зал библиотеки	Проектор, переносной экран, тонкие клиенты (13 шт.), компьютеры (5 шт.)

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 для заочной формы обучения

Вид учебной работы	Всего зачетных единиц	Всего часов	Курс
			2
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ, в т.ч. по РУП:	3	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ	-	19	19
Лекции (Лк)	-	6	6
Практические занятия (ПР)		4	4
Лабораторные занятия (Лаб)	-	4	4
Контроль промежуточной аттестации (КПА)		1	1
Контроль самостоятельной работы и иная контактная работа(КСР)		4	4
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	-	81	81
Подготовка к промежуточной аттестации в форме: экзамен	-	8	8
ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ		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 «____» _____
20__г., протокол № _____

Зав. кафедрой _____

Подпись, дата

Ю.В.Торкунова

Программа одобрена методическим советом института _____
«____» _____ 20____г., протокол № _____

Зам. директора по УМР _____

Подпись, дата

В.В.Косулин

Согласовано:

Руководитель ОПОП _____

Подпись, дата

Железнякова Ю.Е

*Приложение к рабочей
программе дисциплины*



КГУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «КГУ»)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Информационная безопасность

Направление
подготовки

46.03.02 Документоведение и архивоведение

Направленность
управления

Документоведение и документационное обеспечение

Квалификация

Бакалавр

г. Казань, 2020

Фонд оценочных средств по дисциплине «Информационная безопасность» - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие достижения компетенции: ПК-17 Владение методами защиты информации.

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

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 дис- циплины	Вид СРС	Наимено- вание оценочного средства	Заплани- рованные компетенции 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 теоретичес- кого материала	Тест	ПК-5	<7	7-9	10-11	12-15
2	Изучение теоретичес- кого материала	Тест	ПК-5	<7	7-10	10-12	12-15
3	Изучение теоретичес- кого материала	Тест	ПК-5	<8	8-10	10-13	13-15
4	Изучение теоретичес- кого материала	Тест Рфр	ПК-5	<8	8-10	10-13	13-15
Всего баллов				менее 30	30-39	40-49	50-60
Промежуточная аттестация							
	Подготовка к экзамену	Задания к	ПК-5	менее 25	25-29	30-34	35-40

		экзамену					
Итого баллов				0-54	55-69	70-84	85-100

2. Перечень оценочных средств

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

3. Фонд оценочных средств 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: - Информация – это - сведения, поступающие от СМИ; - только документированные сведения о лицах, предметах, фактах, событиях; - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления; - только сведения, содержащиеся в электронных базах данных. - Информации свойственно - не исчезать при потреблении; - становиться доступной, если она содержится на материальном носителе; - подвергаться только "моральному износу"; - всё выше перечисленное. - Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных – это - защита информации; - компьютерная безопасность; - защищенность информации; - безопасность данных. - Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрепятствования доступа к ним – это - информационная война; - информационное оружие; - информационное превосходство. - 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: <table> <tr> <td>Количество правильных ответов</td><td>Баллы</td></tr> <tr> <td>8-10</td><td>15</td></tr> <tr> <td>6-7</td><td>10</td></tr> <tr> <td>4-5</td><td>5</td></tr> <tr> <td>Менее 4</td><td>0</td></tr> </table> Максимальное количество баллов - 15	Количество правильных ответов	Баллы	8-10	15	6-7	10	4-5	5	Менее 4	0
Количество правильных ответов	Баллы										
8-10	15										
6-7	10										
4-5	5										
Менее 4	0										
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	При оценке тестовых заданий учитываются следующие критерии: <table> <tr> <td>Количество правильных ответов</td><td>Баллы</td></tr> <tr> <td>8-10</td><td>15</td></tr> </table>	Количество правильных ответов	Баллы	8-10	15						
Количество правильных ответов	Баллы										
8-10	15										

шкала оценивания в баллах	6-710 4-55 Менее 40 Максимальное количество баллов - 15												
Представление и содержание оценочных материалов	Тестовые задания по разделу 3 «Принципы построения системы информационной безопасности». Примеры тестовых заданий: - 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. - 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. - 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: <table> <tr> <td>Количество правильных ответов</td> <td>Баллы</td> </tr> <tr> <td>8-10</td> <td>15</td> </tr> <tr> <td>6-7</td> <td>10</td> </tr> <tr> <td>4-5</td> <td>5</td> </tr> <tr> <td>Менее 4</td> <td>0</td> </tr> <tr> <td colspan="2">Максимальное количество баллов - 15</td> </tr> </table>	Количество правильных ответов	Баллы	8-10	15	6-7	10	4-5	5	Менее 4	0	Максимальное количество баллов - 15	
Количество правильных ответов	Баллы												
8-10	15												
6-7	10												
4-5	5												
Менее 4	0												
Максимальное количество баллов - 15													
Представление и содержание оценочных материалов	Тестовые задания по разделу 4 «Организация системы защиты информации в организации». Примеры тестовых заданий: - Какие средства защиты информации в ПК наиболее распространены? а) применение различных методов шифрования, не зависящих от контекста информации; б) средства защиты от копирования коммерческих программных продуктов; в) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя; г) защита от компьютерных вирусов и создание архивов; д) все вышеперечисленные - Выберите правильные утверждения: а) должно быть относительно легко создавать цифровую подпись; б) должно быть относительно трудно создавать цифровую подпись; в) должно быть относительно легко проверять цифровую подпись; г) нет верного утверждения. - Выходом хэш-функции является: а) сообщение той же длины, что и входное сообщение; б) сообщение фиксированной длины; в) сообщение меньшей длины; г) нет верного ответа. - Хэш-функции предназначены для:												

	а) сжатия сообщения; б) получения «отпечатков пальцев» сообщения; в) шифрования сообщения; г) нет верного ответа.										
Критерии оценки и шкала оценивания в баллах	При оценке тестовых заданий учитываются следующие критерии: <table> <tr> <td>Количество правильных ответов</td><td>Баллы</td></tr> <tr> <td>8-10</td><td>15</td></tr> <tr> <td>6-7</td><td>10</td></tr> <tr> <td>4-5</td><td>5</td></tr> <tr> <td>Менее 4</td><td>0</td></tr> </table> Максимальное количество баллов - 15	Количество правильных ответов	Баллы	8-10	15	6-7	10	4-5	5	Менее 4	0
Количество правильных ответов	Баллы										
8-10	15										
6-7	10										
4-5	5										
Менее 4	0										
Наименование оценочного средства	Практическое занятие										
Представление и содержание оценочных материалов	Комплект заданий к разделу 3 «Информационные угрозы и их виды» Дать обоснование необходимости анализа рисков для организации и указать: кто принимает решение о проведении анализа рисков? кто проводит анализ рисков, с какой периодичностью? в какой форме представлена оценка рисков? если данный анализ не проводится, то по каким причинам?										
Наименование оценочного средства	Реферат										
Представление и содержание оценочных материалов	Темы рефератов: 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 – 3 балла; ☐ содержание материала раскрыто неполно, показано общее понимание вопроса, достаточное для дальнейшего изучения программного материала – 2 балл; ☐ не раскрыто основное содержание учебного материала – 0 баллов; 2. Последовательность изложения ☐ содержание материала раскрыто последовательно, достаточно хорошо продумано – 2 балла; ☐ последовательность изложения материала недостаточно продумана – 1 балл; ☐ путаница в изложении материала – 0 баллов; 3. Применение конкретных примеров ☐ показано умение иллюстрировать материал конкретными примерами – 2 балла; ☐ приведение примеров вызывает затруднение – 1 балл; ☐ неумение приводить примеры при объяснении материала – 0 баллов; Количество баллов: максимум –9										

4. Фонд оценочных средств промежуточной аттестации

Дается характеристика всех оценочных материалов промежуточной аттестации обучающихся в соответствии с технологической картой дисциплины

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 Гронсфелда»
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

РЕЦЕНЗИЯ

на фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине **Информационная безопасность**

Содержание ФОС соответствует требованиям федерального государственного стандарта высшего образования по направлению подготовки 46.03.02 Документоведение и архивоведение и учебному плану.

ФОС соответствует требованиям, предъявляемым к структуре, содержанию ФОС по дисциплине, а именно:

1. Перечень формируемых компетенций, которыми должен овладеть обучающийся в результате освоения дисциплины, соответствует ФГОС ВО и профстандарту, будущей профессиональной деятельности выпускника.

2. Показатели и критерии оценивания компетенций, а также шкалы оценивания обеспечивают возможность проведения всесторонней оценки результаты обучения, уровней сформированности компетенций.

3. Контрольные задания и иные материалы оценки результатов освоения разработаны на основе принципов оценивания: валидности, определённости, однозначности, надёжности, а также соответствуют требованиям к составу и взаимосвязи оценочных средств, полноте по количественному составу оценочных средств и позволяют объективно оценить результаты обучения, уровни сформированности компетенций.

4. Методические материалы ФОС содержат чётко сформулированные рекомендации по проведению процедуры оценивания результатов обучения и сформированности компетенций.

5. Направленность ФОС по дисциплине соответствует целям ОПОП ВО по направлению по направлению подготовки 46.03.02 Документоведение и архивоведение и профессиональным стандартам специалиста по управлению документацией организации №416н от 10.05.2017; специалиста по организационному и документационному обеспечению управления организацией №333н от 17.07.2020.

6. Объём ФОС соответствует учебному плану подготовки.

7. Качество ФОС в целом обеспечивают объективность и достоверность результатов при проведении оценивания с различными целями.

Заключение. На основании проведенной экспертизы можно сделать заключение, что ФОС по дисциплине соответствует требованиям ФГОС ВО, профессионального стандарта, современным требованиям рынка труда и рекомендуются для использования в учебном процессе. Следует отметить, что созданы условия для максимального приближения системы оценки и контроля компетенций обучающихся к условиям их будущей профессиональной деятельности.

Рассмотрено на заседании методического совета Института цифровых технологий и экономики «26» октября 2020 г., протокол № 2.

Председатель методического совета ИЦТЭ


подпись

Торкунова Юлия Владимировна

Начальник отдела документационного обеспечения АО «Татэнергосбыт»


подпись

Сибгатуллина Фания Ярулловна

