МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт
Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан ФИМЭ
А.В. Фомина
«10» февраля 2023 г.

Рабочая программа дисциплины

К.М.09.06 Информационная безопасность образовательной организации

Направление подготовки

Прикладная информатика

Направленность (профиль) подготовки
09.03.03 Прикладная информатика в образовании

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Заочная

Год набора 2023

Новокузнецк 2023

Оглавление

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП):

Профессиональная компетенция ПК-1

1.1 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 1 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ПК-1 Способен внедрять и обеспечивать техническую поддержку информационных систем в образовательной сфере	ПК-1.2. Устанавливает и настраивает программное обеспечение в соответствии с требованиями образовательной организации ПК-1.3. Документирует процесс проектирования информационных систем образовательной организации ПК-1.4. Проектирует и осуществляет техническую поддержку электронной информационно-образовательной среды	Знать: - виды программного обеспечения, используемые в образовательных организациях; - этапы процедуры инсталляции и настройки программного обеспечения ИС; - нормативную техническую документацию; - структуру и требования к электронной информационно-образовательной среде организации. Уметь: - подбирать и обосновывать выбор информационного обеспечения для сопровождения прикладных процессов в образовательных организациях; - устанавливать и настраивать программное обеспечение в образовательных организациях; - определять параметры настройки программного обеспечения в образовательных организациях; - выполнять работы по документированию процесса проектирования информационных систем; Владеть навыками: - выбора оптимальных параметров установки и настройки программного обеспечения в образовательных

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
		организациях; - настройки программного обеспечения информационных систем с учетом их области приложения.

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 2 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения		
	ОФО	ОЗФО	ЗФО
1 Общая трудоемкость дисциплины			108
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)			12
Аудиторная работа (всего):			8
в том числе:			
лекции			2
практические занятия, семинары			
практикумы			
лабораторные работы			8
в интерактивной форме			
в электронной форме			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			
подготовка курсовой работы /контактная работа			
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)			
творческая работа (эссе)			
3 Самостоятельная работа обучающихся (всего)			96
4 Промежуточная аттестация обучающегося - экзамен и объём часов, выделенный на промежуточную аттестацию:		-	зачет 5 курс

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план заочной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)		Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО	ЗФО	

			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ.		лекц.	практ.		
Семестр 3									
	1. Основы информационной безопасности					4	0	48	
1	1.1 Основные понятия ИБ.					2		20	
2	1.2 Уровни обеспечения ИБ					2		28	Тест № 1
	2.Основные подходы к обеспечению информационной безопасности образовательной организации					0	12	179	
3	2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации						2	38	
4	2.2 Политика информационной безопасности ОО						2	35	Контрольная работа № 1
5	2.3 Механизмы и средства сетевой безопасности						2	33	
6	2.4 Криптографические средства защиты информации, электронная цифровая подпись						4	45	Реферат
7	2.5 Средства фильтрации Интернет-контента						2	28	
8	Промежуточная аттестация - *экзамен*								Итоговый тест
ИТОГО по семестру		252				4	12	227	

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Семестр 3	
	Содержание лекционного курса	
1	*Основы информационной безопасности*	
1.1	Основные понятия ИБ.	Информационная безопасность (ИБ) и защита информации. Понятия доступности, целостности и конфиденциальности в контексте ИБ. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Основные задачи обеспечения защиты информации. Источники, риски и формы атак на информацию. Международные стандарты информационного обмена.
1.2	Уровни обеспечения ИБ	Законодательный, административный, процедурный и программно-технический уровни обеспечения ИБ. Законодательство РФ об информации и защите информации.
	Содержание лабораторных занятий	
1	*Основные подходы к*	

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	обеспечению информационной безопасности образовательной организации	
1.1	Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Модель информационных процессов образовательной организации. Учет требований законодательства при размещении сведений об ОО на сайте.
1.2	Политика информационной безопасности ОО	Основные принципы разработки политики информационной безопасности с учетом специфики информационных процессов образовательной организации. Анализ угроз ИБ. Классификация видов угроз ИБ по различным признакам.
1.3	Механизмы и средства сетевой безопасности	Модели безопасности основных ОС. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Антивирусное ПО. Межсетевые экраны.
1.4	Криптографические средства защиты информации, электронная цифровая подпись	Основы криптографии. Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.
1.5	Средства фильтрации Интернет-контента	Управление правами доступа к ресурсам ОС, ИС и веб-сервисов. Настройка шлюза контентной фильтрации.
	Промежуточная аттестация - *экзамен*	

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 5.

Таблица 5 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**60**	Лекционные занятия (конспект) (2 занятий)	**5 баллов** посещение 1 лекционного занятия	5 – 10
		Лабораторные работы (отчет о выполнении лабораторной работы) (5 работ).	**3 балла** - посещение 1 лаб. раб. и выполнение работы на 51-65% **6 балла** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	15 - 30

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
		Контрольная работа (отчет о выполнении контрольной работы) (1 работа)	**от 5 до:** **6 баллов** (выполнено 51 - 65% заданий) **8 баллов** (выполнено 66 - 85% заданий) **10 баллов** (выполнено 86 - 100% заданий)	5 – 10
		Реферат (по разделу 2.4)	**6 баллов** (пороговое значение) **12 баллов** (максимальное значение)	6 – 10
Итого по текущей работе в семестре				31 - 60
Промежуточная аттестация (экзамен)	40 (100% /баллов приведенной шкалы)	Тест.	**20 балла** (пороговое значение) **40 баллов** (максимальное значение)	20 - 40
Итого по промежуточной аттестации (экзамену)				(51 – 100% по приведенной шкале) 20 – 40 б.
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации 51 – 100 б.				

Для обучающихся заочной формы обучения в текущей учебной работе в семестре (по графику – в период ТО) планируется выполнение контрольной работы, за которую назначаются баллы, включаемые в общий объем баллов за текущую работу в семестре (см. таблицу 7). Обучающемуся по ЗФО задание на контрольную работу выдается на установочной сессии. Примеры тем для контрольных работ приведены в п. 6.1 данной программы.

5 Учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная литература

1. Башлы П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. ISBN 978-5-369-01178-2. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=405000 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

2. Шаньгин В. Ф. Информационная безопасность. – М.: ДМК Пресс, 2014. – 702 с.: ил. ISBN 978-5-94074-768-0. – Текст : электронный // Лань : электронно-библиотечная система. - URL: http://e.lanbook.com/books/element.php?pl1_id=50578 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

Дополнительная учебная литература

1. Бабаш А. В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. ISBN 978-5-369-01304-5. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=432654 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

2. Баранова Е. К., Бабаш А. В. Моделирование системы защиты информации: Практикум: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. ISBN 978-5-369-01379-3. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=476047 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

3. Кнауб Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. ISBN 978-5-7638-2113-7. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=441493 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

4. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил. ISBN 978-5-91134-627-0. – Текст : электронный // Знаниум : электронно-библиотечная система. - URL: http://znanium.com/catalog.php?bookinfo=420047 (дата обращения 24.08.2019). – Режим доступа : для авториз. пользователей.

5.2 Материально-техническое и программное обеспечение дисциплины

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ:

Информационная безопасность образовательной организации	303 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения занятий: занятий лекционного типа; - занятий семинарского (практического) типа. - текущего контроля и промежуточной аттестации. Специализированная (учебная) мебель: доска маркерно-меловая, столы компьютерные, стулья. Оборудование для презентации учебного материала: стационарное - ноутбук преподавателя, экран, проектор. Оборудование: компьютеры для обучающихся (11 шт.). Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО),	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом.2

	Java (бесплатная версия), MicrosoftSQLServer 2008 (MicrosoftImaginePremium 3 yearпо сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), OpenProject (бесплатная версия), Яндекс.Браузер (отечественное свободно распространяемое ПО), UML-диаграммы (бесплатная версия), Denwer (свободно распространяемое ПО), Eclipse(свободно распространяемое ПО), Blender(свободно распространяемое ПО), Dia(свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	

5.3 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке - http://citforum.ru

2. Научная электронная библиотека eLIBRARY.RU – крупнейший российский информационный портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты - www.elibrary.ru

3. Единое окно доступа к образовательным ресурсам - http://window.edu.ru/

4. База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru

5. База данных правовых актов «КонсультантПлюс»: комп. справ. правовая система / компания «КонсультантПлюс»: http://base.consultant.ru .

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

Темы контрольной работы

1. Разработка политики информационной безопасности образовательной организации (по выбору обучающегося).

Темы рефератов

1. Вредоносное ПО: способы распространения, опасность, методы защиты.
2. Программные закладки: типы, способы внедрения и защиты.
3. Аппаратные средства защиты информации.
4. Сравнительный анализ средств защиты электронной почты.
5. Сравнительный анализ систем обнаружения атак.

6. Сравнительный анализ межсетевых экранов.

7. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.

8. Анализ методов нарушения безопасности сетевых ОС и методов противодействия им.

9. Применение биометрической информации для аутентификации пользователей компьютерных систем.

10. Стандарты безопасности компьютерных систем и информационных технологий.

11. Сравнительный анализ методов и программных средств защиты от спама.

12. Методы и программные средства перехвата и анализа контента.

13. Уязвимости симметричных и асимметричных криптографических систем.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Семестр 3

Таблица 8 - Примерные теоретические вопросы и практические задания к экзамену

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания
1. *Основы информационной безопасности*		
1.1 Основные понятия ИБ	1. Опишите основные угрозы целостности информации и способы противодействия им. 2. Опишите основные угрозы конфиденциальности информации и способы противодействия им.	
1.2 Уровни обеспечения ИБ	1. Укажите, к каким уровням ИБ относятся следующие средства: а) федеральный закон; б) антивирусное ПО; в) межсетевой экран; г) должностная инструкция сотрудника; д) распоряжение директора. 2. Каким образом необходимость защиты информации отражена в Конституции РФ?	
2. *Основные подходы к обеспечению информационной безопасности образовательной организации*		
2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	1. Укажите три основные угрозы для информации в человеко-компьютерных системах. 2. Выделите три наиболее эффективных метода защиты информации от ошибочных действий пользователей.	

2.2 Политика информационной безопасности ОО	1. Укажите основные требования к механизму авторизации пользователей в информационных системах организации.	1. Проанализируйте обоснованность положений предложенной политики ИБ, выработайте рекомендации по оптимизации Политики с учетом специфики организации.
2.3 Механизмы и средства сетевой безопасности	1. Укажите уровень эталонной модели OSI, в которые входит в функции шифрования.	1. Разработайте правила для сетевого фильтра, обеспечивающего работу протоколов Web, электронной почты, системы видеоконференций (по выбору) с учетом SSL-транспорта.
2.4 Криптографические средства защиты информации, электронная цифровая подпись	1. Опишите криптосистему, которая обладает следующими чертами: предусматривает использование открытого ключа для шифрования и закрытого для дешифрования данных.	1. Предложите безопасный алгоритм восстановления забытого пароля электронной почты. 2. Напишите программу, реализующую предложенный криптографический алгоритм.
2.5 Средства фильтрации Интернет-контента	1. Сформулируйте цели и принципы контентной фильтрации в образовательной организации	1. Разработайте систему контент-фильтрации на основе открытых программных средств. Оцените ее надежность для применения в образовательной организации.

Составитель (и): Читайло А. И., ст. преп. каф. ИОТД
(*фамилия, инициалы и должность преподавателя (ей)*)