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
Кафедра информатики и общетехнических дисциплин

«УТВЕРЖДАЮ»
Декан ФИМЭ
А.В. Фомина
«08» февраля 2024 г.

Рабочая программа дисциплины

Б1.В.06 Информационная безопасность

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) подготовки
«Математика и Информатика»

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
очная

Год набора 2020

Новокузнецк 2024

Оглавление

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы академического бакалавриата (далее - ОПОП): ПК-2

Содержание компетенций как планируемых результатов обучения по дисциплине см. таблицы 1 и 2.

1.1 Формируемые компетенции

Таблица 1 - Формируемые дисциплиной компетенции

Наименование вида компетенции	Наименование категории (группы) компетенций	Код и название компетенции
профессиональная		ПК – 2 Способен осуществлять разработку и реализацию образовательных программ основного и среднего общего образования по математике на основе специальных научных знаний в предметной области “Информатика”

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ПК – 2 Способен осуществлять разработку и реализацию образовательных программ основного и среднего общего образования по математике на основе специальных научных знаний в предметной области “Информатика”	ПК 2.1 Проектирует элементы образовательной программы и рабочую программу по информатике, формулирует дидактические цели и задачи обучения информатике и реализовывает их в учебном процессе, моделирует и реализовывает различные организационные формы обучения информатике (урок, экскурсию, домашнюю, внеклассную и внеурочную работу), планирует и комплексно применяет различные средства обучения информатике в системе основного и среднего общего образования ПК 2.2 Использует педагогические технологии для достижения личностных, предметных и метапредметных результатов обучающихся в предметной области “Информатика”	Б1.В.03 Оценивание и мониторинг образовательных результатов обучающегося по информатике Б1.В.04 Операционные системы Б1.В.06 Информационная безопасность Б1.В.07 Информатизация управления образовательным процессом Б1.В.ДВ.01.01 Организация проектной деятельности обучающихся в предметной области "Математика и информатика" Б1.В.ДВ.01.02 Организация учебно-исследовательской деятельности обучающихся в предметной области "Математика и информатика" Б2.В.01(П)Производственная практика. Профильная практика ФТД.02 Видеомонтаж

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
	ПК 2.3 Демонстрирует владение методикой преподавания по предмету “Информатика” различных категорий обучающихся в соответствии с основной образовательной программой на основе деятельностного подхода и владения современными педагогическими техно-логиями ПК 2.4 Демонстрирует владение специальными научными знаниями в предметной области “Информатика”, позволяющими осуществлять образовательный процесс в данной предметной области в системе основного и среднего общего образования	

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ПК – 2 Способен осуществлять разработку и реализацию образовательных программ основного и среднего общего образования по математике на основе специальных научных знаний в предметной области “Информатика”	ПК 2.4 Демонстрирует владение специальными научными знаниями в предметной области “Информатика”, позволяющими осуществлять образовательный процесс в данной предметной области в системе основного и среднего общего образования	Знать: - виды и источники угроз безопасности информации; - основные требования информационной безопасности; - основные элементы информационной поддержки решения задачи защиты информации Уметь: - выбирать методы и разрабатывать средства защиты информации; Владеть: - навыками применения современных средств информационной безопасности - способами анализа и отбора методов и средств обеспечения информационной безопасности при работе в электронной среде обучения

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

Таблица 4 – 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
1 Общая трудоемкость дисциплины	144
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	46
Аудиторная работа (всего):	30
в том числе:	
лекции	10
практические занятия, семинары	
практикумы	20
лабораторные работы	
в интерактивной форме	
в электронной форме	
Внеаудиторная работа (всего):	78
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)	78
4 Промежуточная аттестация обучающегося	Экзамен (36 ч) 9 семестр

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 5 - Учебно-тематический план очной 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				
			Аудиторн. занятия			СРС	
			лекц.	практ.	лаб		
Семестр _9__							
	1. Основы информационной безопасности						ТС-2
1	1.1 Основные понятия ИБ.	18	2	4		12	ТС-2
2	1.2 Уровни обеспечения ИБ	18	2	4		12	ТС-2
	2.Основные подходы к обеспечению информационной безопасности образовательной организации						ТС-2
3	2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	18	2	4		12	ТС-2
4	2.2 Политика информационной безопасности ОО	15	1	2		12	ТС-2

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.) ОФО				Формы текущего контроля и промежуточной аттестации успеваемости
			Аудиторн. занятия			СРС	
			лекц.	практ.	лаб		
Семестр _9__							
5	2.3 Механизмы и средства сетевой безопасности	13	1	2		10	ТС-2
6	2.4 Криптографические средства защиты информации, электронная цифровая подпись	13	1	2		10	ТС-2
7	2.5 Средства фильтрации Интернет-контента	13	1	2		10	ТС-2
8	Промежуточная аттестация - *экзамен*	36					УО-3
ИТОГО по семестру		**144**	**10**	**20**		**78**	

ТС-2 (учебные задачи); УО-3 (Зачет)

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Семестр 9	
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 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 7.

Таблица 7 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

9 семестр				
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) (9 занятий)	**1 балл** посещение 1 лекционного занятия	1 – 9
		Лабораторные работы (отчет о выполнении лабораторной работы) (14 работ).	**3,5 балла** - посещение 1 практического занятия и выполнение работы на 51-65% **6,5 баллов** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	50 – 91
Итого по текущей работе в семестре				51 - 100
Промежуточная аттестация (зачет)	**40**	Теоретический вопрос	**5 баллов** (пороговое значение) **10 баллов** (максимальное значение)	5 - 10
		Практическое задание	**5 баллов** (пороговое значение) **10 баллов** (максимальное значение)	5– 10
Итого по промежуточной аттестации (экзамен)				(51 – 100% по приведенной шкале) 10 – 20 б.
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации				51 – 100 б.

5 Материально-техническое, программное и 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	508 Компьютерный класс Учебная аудитория для проведения занятий лекционного типа, занятий практического типа, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная (учебная) мебель: доска меловая, кафедра, столы, стулья Оборудование для презентации учебного материала: компьютер преподавателя, проектор, экран, 18 компьютеров Лабораторное оборудование: стационарное – компьютеры для обучающихся (18 шт.). Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), Яндекс.Браузер (отечественное свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Opera 12 (свободно распространяемое ПО),LibreOffice (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), XAMPP (свободно распространяемое ПО), Denwer (свободно распространяемое ПО), MicrosoftVisualStudio (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), Антивирусное ПО ESET Endpoint Security, лицензия №EAV-0267348511 до 30.12.2022.. Интернет с обеспечением доступа в ЭИОС	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

5.3.2 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. Федеральный портал «Российское образование» - http://www.edu.ru. Доступ свободный

2. Информационная система «Единое окно доступа к образовательным ресурсам» - http://www.window.edu.ru.

3. Федеральный центр информационно-образовательных ресурсов - http://fcior.edu.ru. Доступ свободный.

4. Федеральный портал "Информационно-коммуникационные технологии в образовании" - http://www.ict.edu.ru/.

5. Сайт Министерства образования и науки РФ. - Режим доступа: http://www.mon.gov.ru. Доступ свободный.

6. Единая коллекция цифровых образовательных ресурсов.- Режим доступа: http://school-collection.edu.ru/

7. Единое окно доступа к образовательным ресурсам. Раздел Образование в области техники и технологий – http://window.edu.ru/?p_rubr=2.2.75

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

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

Таблица 9 - Примерные теоретические вопросы и практические задания к *зачету*

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.