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
Фомина А.В.
«9» февраля 2023 г.

Рабочая программа дисциплины

К.М.08.01.11 Информационная безопасность
Код, название дисциплины /модуля

Направление подготовки / *специальность*
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) программы / специализация
«Математика и Информатика»

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
очная, заочная

Год набора 2023

Новокузнецк 2023

Оглавление

1 Цель дисциплины. 3
1.1 Формируемые компетенции ..... **Ошибка! Закладка не определена.**
1.2 Индикаторы достижения компетенций 3
1.3 Знания, умения, навыки (ЗУВ) по дисциплине ..... **Ошибка! Закладка не определена.**
2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации. 3
3. Учебно-тематический план и содержание дисциплины. 4
3.1 Учебно-тематический план 4
3.2. Содержание занятий по видам учебной работы ..... **Ошибка! Закладка не определена.**
4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации. 4
5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины. 5
5.1 Учебная литература 5
5.2 Материально-техническое и программное обеспечение дисциплины. 6
5.3 Современные профессиональные базы данных и информационные справочные системы. 6
6 Иные сведения и (или) материалы. 7
6.1.Примерные темы письменных учебных работ 7
6.2. Примерные вопросы и задания / задачи для промежуточной аттестации . 7

1 Цель дисциплины.

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

Формируемые компетенции, индикаторы достижения компетенций, знания, умения, навыки

Таблица 1 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ПК-2 Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области по профилю "Информатика" при решении профессиональных задач	ПК-2.1 Знает структуру, состав и дидактические единицы предметной области "Информатика" (преподаваемого предмета) ПК-2.2 Умеет осуществлять отбор учебного содержания предметной области "Информатика" для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО ПК-2.3 Демонстрирует умение разрабатывать по предметной области "Информатика" различные формы учебных занятий, применять методы, приемы и технологии обучения, в том числе информационные	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 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]
1 Общая трудоемкость дисциплины	144		144
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)			
Аудиторная работа (всего):	44		8
в том числе:			
лекции	18		4
практические занятия, семинары			
практикумы	26		4
лабораторные работы			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			

подготовка курсовой работы (проекта) /контактная работа[2]			
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)			
творческая работа (эссе)			
3 Самостоятельная работа обучающихся (всего)	64		127
4 Промежуточная аттестация обучающегося - экзамен	Экзамен 9 4 з.е.		Экзамен 6 4 з.е.

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план очной / заочной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)									Формы текущ. контроля и промежуточной аттестации
			ОФО			ОЗФО			ЗФО			
			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ		лекц.	практ		лекц.	практ		
Семестр ___9__												
1.	1. Основы информационной безопасности											
1	1.1 Основные понятия ИБ.	14	2	4	8				2		18	
2	1.2 Уровни обеспечения ИБ	14	2	4	8						18	
2.	2.Основные подходы к обеспечению информационной безопасности образовательной организации											
3	2.1 Типовые информационные процессы ОО, оценка рисков и принципы защиты информации	14	2	4	8				2		18	
4	2.2 Политика информационной безопасности ОО	16	2	4	10						18	
5	2.3 Механизмы и средства сетевой безопасности	16	2	4	10					2	18	
6	2.4 Криптографические средства защиты информации, электронная цифровая подпись	18	4	4	10					2	18	
7	2.5 Средства фильтрации Интернет-контента	16	4	2	10						19	
8	Промежуточная аттестация - *экзамен*	36										
ИТОГО по семестру 9		144	18	26	64						127	
	Всего по учебному плану:											

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 4.

Таблица 4 - 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) (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.

Обучающемуся по ЗФО задание на самостоятельную работу и контрольную работу выдается на установочной сессии.

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 КГПИ 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 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.

6.1.2 Контрольные работы/ рефераты/ индивидуальные задания обучающемуся.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Форма промежуточной аттестации зачет

Таблица 5 – Типовые (примерные) контрольные вопросы и задания

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания
Семестр _9_ Экзамен		
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.
2.5 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.
Компетенции		
ПК-2		1. Напишите программу, реализующую криптографический алгоритм шифрования сообщения.

Составитель (и): _____

(*фамилия, инициалы и должность преподавателя (ей)*)