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 А.В. Фомина
« 09 » февраля 2023 г.

Рабочая программа дисциплины

К.М.07.04 Информационная безопасность
Код, название дисциплины

Направление подготовки
09.03.01 Информатика и вычислительная техника
Код, название направления

Направленность (профиль) подготовки
Автоматизированные системы обработки информации и управления

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Заочная

Год набора 2023

Новокузнецк 2023

СОДЕРЖАНИЕ

1 Цель дисциплины

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее ОПОП): ОПК-3.

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 *(универсальная, общепрофессиональная, профессиональная)*	Код и название компетенции
Общепрофессиональная	ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

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
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1. Формулирует профессиональные задачи в сфере проектирования, разработки, внедрения и эксплуатации средств вычислительной техники и информационных систем, управления их жизнен-ным циклом, к решению которых в рамках освое-ния программы бакалавриата могут готовиться выпускники. ОПК-3.2. Осуществляет поиск источников инфор-мации по заданной теме своей профессиональной области в электронных информационных ресурсах по различным типам запросов. ОПК-3.3. Осуществляет информационно-библиографический поиск по заданной теме своей профессиональной области в печатных информа-ционных ресурсах по различным типам запросов.	К.М.05 Современные информационные технологии и информационные системы К.М.05.02 Введение в профессиональную деятельность К.М.05.04 Операционные системы **К.М.05.05 Информационная безопасность** К.М.05.08 Сети и телекоммуникации К.М.05.14(У) Технологическая (проектно-технологическая) практика К.М.09 Государственная итоговая аттестация К.М.09.01(Д) Выполнение и защита выпускной квалификационной работы

	ОПК-3.4. Осуществляет информационный поиск по заданной теме своей профессиональной области с применением информационно-коммуникационных технологий в современных профессиональных базах данных и информационных справочных системах. ОПК-3.5. Выявляет угрозы информационной без-опасности; ОПК-3.6. Анализирует и выбирает методы и сред-ства обеспечения информационной безопасности в соответствии с заданием. ОПК-3.7. Эксплуатирует программно-аппаратные средства в сетевых структурах.	

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код компетенции	Формируемые компетенции	Дескрипторные характеристики компетенций
ОПК-3	ОПК-3.5. Выявляет угрозы информационной безопасности; ОПК-3.6. Анализирует и выбирает методы и средства обеспечения информационной безопасности в соответствии с заданием.	Знать: – базовые понятия информационной безопасности; – классификацию угроз уязвимостей; – нормативно-правовую базу в области защиты информации; – основные понятия и методы организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; – методики построения систем защиты информации. Уметь: – моделировать угрозы и уязвимости информационной безопасности; – выделять источники информации, объекты защищаемой информации; – формировать требования к построению безопасной системы; – определять функциональные задачи и требования. Владеть:

		– методами организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; – методами и методиками построения систем защиты информации; – программными продуктами для оценки риска информационной безопасности; – программными средствами обеспечения информационной безопасности; – протоколами аутентификации, распределения ключей, электронной подписи и финансовой криптографии.

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	ОЗФО	ЗФО
1 Общая трудоемкость дисциплины	180		
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	54		
Аудиторная работа (всего):	54		
в том числе:			
лекции	18		
практические занятия, семинары	36		
практикумы			
лабораторные работы			
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)	90		
4 Промежуточная аттестация обучающегося – экзамен – 5 семестр	36		

3 Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 5 - Учебно-тематический план очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	семинары, практические занятия		
1.	Введение в предмет. Угрозы информационной безопасности	16	2	6	7	Устный доклад; отчет по лабораторной работе.
2.	Основные понятия теории информационной безопасности	16	3	6	7	Устный доклад; Отчет по лабораторной работе.
3.	Программно-технические методы защиты	25	3	6	16	Устный доклад; Отчет по лабораторной работе.
4.	Криптографические методы защиты	25	3	6	16	Устный доклад; Отчет по лабораторной работе.
5.	Организационно правовые методы информационной безопасности	18	3	8	7	Устный доклад; Отчет по лабораторной работе.
6.	Роль стандартов в обеспечении информационной безопасности	18	3	8	7	Устный доклад; Отчет по лабораторной работе.
7.	Технологии построения защищенных систем	27	3	8	16	Устный доклад; Отчет по лабораторной работе
8.	Промежуточная аттестация -экзамен	36				
ИТОГО		**180**	**18**	**36**	**90**	

3.2 Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание
Содержание лекционного курса		
1	Введение в предмет. Угрозы информационной безопасности	Понятие информационной безопасности и защищенной системы. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.
2	Основные понятия теории информационной безопасности	Основные положения теории информационной безопасности информационных систем. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

№ п/п	Наименование раздела дисциплины	Содержание
3	Программно-технические методы защиты	Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.
4	Криптографические методы защиты	Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации. Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами). Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов нформациионной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

№ п/п	Наименование раздела дисциплины	Содержание
5	Организационно правовые методы информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
6	Роль стандартов в обеспечении информационной безопасности	Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности. Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем. Международные стандарты информационной безоапсности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.
7	Технологии построения защищенных систем	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем.

№ п/п	Наименование раздела дисциплины	Содержание
		Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности
Содержание лабораторных занятий		
1	Введение в предмет. Угрозы информационной безопасности	Построение матрицы рисков для выбранного предприятия.
2	Основные понятия теории информационной безопасности	Знакомство с основными направлениями работ в рамках федеральной программы «Электронная Россия», а также со сведениями о порядке использования и действующих алгоритмах постановки ЭЦП.
3	Программно-технические методы защиты	Исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.
4	Криптографические методы защиты	Методы современной криптографии на примере программирования одного из предложенных алгоритмов.
5	Организационно правовые методы информационной безопасности	Проведение анализ способов нарушений безопасности на прим.
6	Роль стандартов в обеспечении информационной безопасности	Изучение логики работы и формы предоставления информации сетевыми анализаторами; овладение приемов анализа сетевого трафика; получение базовых знаний для обнаружения и организации сетевых атак.
7	Технологии построения защищенных систем	Составление документа «Политика безопасности»

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)

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)	**80**	Лекционные занятия (конспект) (10 занятий)	**1 балл -** посещение 1 лекционного занятия и выполнение задания на 51-85%	0-10
		Практические занятия (24 занятий).	**24/50 балла -** посещение 1 лекционного занятия и выполнение задания на 51-85% **24/520 балла** - посещение 1 практического занятия и выполнение задания на 85.1-100%	0-50
Итого по текущей работе в семестре				0-60
Промежуточная аттестация (зачет с оценкой)	20	Теоретический вопрос 1	**2 балла** (пороговое значение) **10 баллов** (максимальное значение)	2 - 10
		Теоретический вопрос 2	**2 балла** (пороговое значение) **10 баллов** (максимальное значение)	2 - 10
Итого по промежуточной аттестации (зачет с оценкой)				4-20

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная литература

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах [Электронный ресурс] : Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ: НИЦ ИНФРА—М, 2013. — 592 с. – Режим доступа: http://www.znanium.com/bookread.php?book=402686

2. Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2008. - 432 с.: ил.; 60x90 1/16. - (Проф. обр.). (п) ISBN 978-5-91134-246-3 Режим доступа: http://znanium.com/bookread.php?book=167284

Дополнительная литература

1. Стратегия информационной безопасности и инновационной политики [Текст] / Под ред. Е. А. Олейникова. - М.: ВА им. Ф.Э. Дзержинского, 2003. - 271 с.

2. Экономическая безопасность: производство — финансы — банки/ Под ред. В. К. Сенчагова.- М.: ЗАО "Финстатинформ", 2000. - 621 с.

3. Ярочкин, В. И. Служба безопасности коммерческого предприятия [Текст] / В. И. Ярочкин. - М.: Ось-89, 1999. - 144 с.

4. Романец, Ю.В. Защита информации в компьютерных системах и сетях [Текст] / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – 2-е изд., перераб. и доп. – М.: радио и связь, 2001 г. – 376 с.

5. Вопросы инновационной политики и экономической безопасности деятельности предприятий [Текст] / Под ред. Е. А. Олейникова. - М.: РЭА им. Г. В. Плеханова, 1992. - 210 с.

6. Гончаренко, Л. П. Экономическая и информационная модели создания системы безопасности личности [Текст] / Л. П. Гончаренко // Проблемы национальной безопасности. - М.: Ун-т дружбы народов, 1998. - С. 62—69.

7. Илларионов, А.С. Критерии экономической безопасности [Текст] / А.С. Илларионов // Вопросы экономики. - 1998. №10. - С. 35—58.

8. Матвеев, Н.В. Анализ методов исследования экономической безопасности [Текст]: Учеб.-метод. пособие для дистанционного обучения / Н.В. Матвеев. - М.: Рос.экон. акад., 1998. - 29 с.

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы	Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом
710 Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа.	Классная доска, место преподавателя, компьютер, проектор, экран, посадочные места для обучающихся. Программное обеспечение - MSPowerPoint для демонстрации слайдов.	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
509 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - самостоятельной работы; - текущего контроля и промежуточной аттестации.	Компьютерный класс, оборудованный компьютерами (по количеству обучающихся в группе), объединенными в локальную сеть и имеющими выход в Интернет. Учебное программное обеспечение: MS PowerPoint, MS Excel, MS Word, MS Visio, Delphi, MS Visual Studio.	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

5.3 Современные профессиональные базы данных и информационные справочные системы.

- Электронная библиотека механико-математического факультета Московского государственного университета – www.lib.mexmat.ru/bookks/41
- Новая электронная библиотека – www.newlibrary.ru
- Российское образование (федеральный портал) – www.edu.ru
- Нехудожественная библиотека – www.nehudlit.ru
- Научная электронная библиотека www.e-library.ru
- Университетская информационная система www.uisrussia.ru

6 Иные сведения и (или) материалы.

6.1 Примерные темы письменных учебных работ

Письменные работы не предусмотрены.

6.2 Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 9 - Примерные теоретические вопросы и практические задания к экзамену

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания и (или) задачи
1. Введение в предмет. Угрозы информационной безопасности.	1. Что называется информационной безопасностью? 2. Какие данные называются критическими? 3. Какие вы знаете признаки компьютерных преступлений в интернет технологиях и какие основные технологии, и методы используются при совершении компьютерных преступлений? 4. Какие четыре уровня защиты компьютерных (интернет технологий) и информационных ресурсов вы можете назвать? 5. Перечислите признаки, свидетельствующие о наличии уязвимых мест в информационной безопасности?	*Задание 1.* Для одноалфавитного метода с задаваемым смешением выполнить шифрование с произвольным смещением.
2. Основные понятия теории информационной безопасности.	6. Перечислите меры защиты информационной безопасности? 7. Какие меры предпринимают по защите целостности информации? 8. Какие меры предпринимают по защите системных программ? 9. Дублирование информации и его классы.	*Задание 2.* Для одноалфавитного метода с задаваемым смешением выполнить дешифрование зашифрованный шифром Цезаря текст.

	10. Перечислите позиции административного уровня. 11. Назовите цель ОНРВ и его основные положения?	
3. Программно-технические методы защиты.	12. Что такое межсетевой экран и какая у него роль в защите. 13. Законодательная основа информационной безопасности, статьи и пр. 14. Что такое политика безопасности на административном уровне? 15. Основные принципы защиты информации на административном уровне? Средства Разграничения доступа. Что такое CGI процедуры, их назначения? Чем опасна программа, полученная из ненадежного источника, какие вы знаете средства контроля над такими программами? Как осуществляется защита WEB-серверов?	*Задание 3.* Проверить на простоту два произвольных целых числа разрядностью 5.
4. Криптографические методы защиты.	20. Криптография и криптоанализ. Назначение криптографии. 21. Перечислите известные алгоритмы шифрования. Цифровые деньги и их характеристики. 22. Симметричная и асимметричная методология	*Задание 4.* Задан интервал вида [*x, x + L*]. Вычислить количество *П(x, L*) простых чисел в интервале и сравнить с величиной *L/1n(x)*. При каких условиях *П(x, L)/L* близко к *1/1n(x)* при заданных *x* = 2000, *L* = 500, количество простых чисел для деления 5-15, количество оснований 1-2?

	шифрования. 23. Криптографические средства защиты. 24. Квантовая криптография и ККС.	
5. Организационно-правовые методы информационной безопасности.	25. Чем определяется концепция обеспечения безопасности АСОИ. 26. В чем состоит избирательная политика безопасности способом управления доступом. 27. Организационные меры безопасности АСОИ. 28. Матрица доступа в АСОИ. 29 Полномочное управление доступом. 30. Избирательное управление доступом.	*Задание 5.* Найти в интервале (1000, 1000 + 300) все простые числа. Пусть L(i) - разность между двумя соседними простыми числами. Построить гистограмму для *L(i)*. Вычислить выборочное среднее $L_{сред}$. Сравнить с величиной *1n(x)*, где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований 1-3.
6. Роль стандартов в обеспечении информационной безопасности.	31. Что такое универсальная операционная система? 32. Что такое компьютерный вирус. 33. Полиморфные вирусы. 34. Суррогатные платежные средства. 35. Файловые вирусы и алгоритм их работы. 36. Особенность макровирусов.	*Задание 6.* Для заданного набора чисел {*k*} оценить относительную погрешность формулы для *k*-го простого числа: *p(k) = k/ln(k), k= {10, 15, 20, 30, 35}.*
7. Технологии построения защищенных систем.	37. Полномочное управление доступом. 38. Избирательное управление доступом. 39. Отказоустойчивые компьютерные системы. 40. Что вы понимаете под технологией RAID. 41.Методы дублирования информации.	*Задание 7.* В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые к простых. Расчет производится для всех *k* <= 10.

Составитель (и): Зайцев В.Н., аспирант,
ведущий специалист отдела автоматизации расчета заработной платы, кадрового и производственного учета
ООО «Синерго Софт Системс»
(*фамилия, инициалы и должность преподавателя (ей)*)