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.08.07 Информационная безопасность

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 / прикладного бакалавриата / (далее — ОПОП):

ОПК 3 – Разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы.

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**
ОПК 3 – Разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы	ОПК 3.1 - моделирование угрозы и уязвимости информационной безопасности; ОПК 3.2 - выделение источника информации или объекты защищаемой информации; ОПК 3.3 - формирование требования к построению безопасной системы;	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 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**
	ЗФО
1 Общая трудоемкость дисциплины	180
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	23
Аудиторная работа (всего):	14
в том числе:	
лекции	4
практические занятия, семинары	10
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[1]	
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем*)*	
творческая работа (эссе)	
3 Самостоятельная работа обучающихся (всего)	157
4 Промежуточная аттестация обучающегося	экзамен 3 курс

3 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Учебно-тематический план

Таблица 35 — 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
			ЗФО			
			Аудиторн. занятия		СРС	
			лекц	пр.		
Раздел 1. Введение в надежность и безопасность программного обеспечения						
1.1	Виды программного обеспечения		1		10	УО
1.2	Надежность и отказобезопасность программного обеспечения в информационных системах		1		10	УО

[1] УО - устный опрос, УО-1 - собеседование, УО-2 - коллоквиум, УО-3 - зачет, УО-4 – экзамен, ПР - письменная работа, ПР-1 - тест, ПР-2 - контрольная работа, ПР-3 эссе, ПР-4 - реферат, ПР-5 - курсовая работа, ПР-6 - научно-учебный отчет по практике, ПР-7 - отчет по НИРС, ИЗ –индивидуальное задание; ТС - контроль с применением технических средств, ТС-1 - компьютерное тестирование, ТС-2 - учебные задачи, ТС-3 - комплексные ситуационные задачи

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ЗФО			
			Аудиторн. занятия		СРС	
			лекц	пр.		
Раздел 2. Угрозы надежности и безопасности программного обеспечения						
2.1	Угрозы надежности и безопасности программного обеспечения		2		10	УО
Раздел 3. Построение надежного программного обеспечения						
3.1	Качество программного обеспечения		2		10	УО
3.2	Правила и этапы построения надежного программного обеспечения			2	20	УО -1, ПР-4
Раздел 4. Разработка надежного программного обеспечения						
4.1	Технологии разработки надежного программного обеспечения			2	20	УО -1, ПР-4
4.2	Методы и технологии обеспечения безопасности программного обеспечения			2	20	УО -1, ПР-4
Раздел 5. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения						
5.1	Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения			2	21	УО -1, ПР-4
	Промежуточная аттестация (экзамен)				**9**	**УО-4**
ИТОГО по курсу (4 курс)			**6**	**8**	**130**	

3.2 Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
Содержание лекционного курса		
Раздел 1. Введение в надежность и безопасность программного обеспечения		
1.1	Виды программного обеспечения	Системное (базовое) программное обеспечение. Прикладное программное обеспечение. Программы встроенных систем.
1.2	Надежность и отказобезопасность программного обеспечения в информационных системах	Функциональная надежность программного обеспечения в информационных системах. Понятие общей надежности информационной системы. Отказобезопасность и кибербезопасность информационных систем. Отказобезопасность информационной системы. Кибербезопасность информационной системы. Взаимосвязь функциональной и информационной безопасности критически важных систем.
Раздел 2. Угрозы надежности и безопасности программного обеспечения		
2.1	Угрозы надежности и безопасности программного обеспечения	Уязвимости программного обеспечения. Ошибки в программном обеспечении. Характерные недостатки эксплуатируемых программ. Вредоносные программы
Раздел 3. Построение надежного программного обеспечения		
3.1	Качество программного обеспечения	Модели качества программного обеспечения. Метрики качества программного обеспечения. Некоторые общие замечания по стратегии и тактике обеспечения надежности и безопасности различных видов программного обеспечения. Обеспечение надежности и безопасности программного обеспечения на различных

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
		этапах его жизненного цикла.
Содержание практических занятий		
Раздел 3. Построение надежного программного обеспечения		
3.1	Качество программного обеспечения	Модели качества программного обеспечения. Метрики качества программного обеспечения. Некоторые общие замечания по стратегии и тактике обеспечения надежности и безопасности различных видов программного обеспечения. Обеспечение надежности и безопасности программного обеспечения на различных этапах его жизненного цикла.
3.2	Правила и этапы построения надежного программного обеспечения	Маршрутная карта обеспечения функциональной надежности программного обеспечения. Модели надежности программного обеспечения. Показатели функциональной надежности и функциональной безопасности ПО. Пример расчета функциональной надежности программы.
Раздел 4. Разработка надежного программного обеспечения		
4.1	Технологии разработки надежного программного обеспечения	Рекомендации по разработке спецификации требований. Технология разработки архитектуры надежной программы. Проектирование надежного программного обеспечения и его реализация. Интеграция программного обеспечения с аппаратными средствами. Обеспечение надежности программного обеспечения в процессе подтверждения соответствия, эксплуатации и сопровождения. Требования к функциональной надежности и архитектуре программного обеспечения критически важных систем.
4.2	Методы и технологии обеспечения безопасности программного обеспечения	Методы доказательства правильности программ: Общие положения; Предусловия и постусловия в доказательствах правильности; Правила вывода (доказательства); Применение правил вывода; Пример доказательства правильности программы для алгоритма дискретного экспоненцирования. Методы создания самотестирующихся и самокорректирующихся программ. Криптографические методы защиты от вредоносных программ. Технологии защиты от вредоносных программ. Технологии тестирования программного обеспечения на его защищенность. Методы защиты программ от несанкционированного исследования
Раздел 5. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения		
5.1	Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения	Федеральный закон РФ «Об информации, информационных технологиях и о защите информации». ГОСТ Р ИСО/МЭК 15408—2013 ГОСТ Р ИСО/МЭК 18045—2013 ГОСТ Р МЭК 61508—2012 Приказ ФСТЭК России от 14 марта 2014 г. № 31 Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» Требования к средствам антивирусной защиты (информационное сообщение ФСТЭК России от 30 июля 2012 г. № 240/24/3095)
	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 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** (100% /баллов приведенной шкалы)	Лекционные занятия (конспект) (3 занятия)	**0,5 балл —** посещение 1-го лекционного занятия **1 балл** - полный конспект 1-го лекционного занятия	1.5 – 3
		Лабораторные работы (отчет о выполнении лабораторной работы) (4 работы).	**1 балл —** посещение 1 практического занятия и выполнение работы на 51-65% **2 балла** — посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	2 - 4
		Реферат (по разделу 3)	**5,5 балла** (пороговое значение) **11 баллов** (максимальное значение)	10 – 18
		Реферат (по разделу 4)	**5,5 балла** (пороговое значение) **11 баллов** (максимальное значение)	10 – 18
		Реферат (по разделу 5)	**5,5 балла** (пороговое значение) **11 баллов** (максимальное значение)	10 – 18
Итого по текущей работе в семестре				31 – 60
Итого по промежуточной аттестации (экзамен)				20 – 40
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации 51 – 100				

5 УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.

5.1 Учебная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/454453

5.2 Материально-техническое и программное обеспечение дисциплины

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ:

Информационная безопасность	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), Яндекс.Браузер (отечественное свободно распространяемое ПО),), AdobeReaderXI(свободно распространяемое ПО), WinDjView(свободно распространяемое ПО), Интернет с обеспечением доступа в ЭИОС.	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом.2

5.3 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» - http://www.window.edu.ru

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

6 ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

6.1 Примерные темы письменных учебных работ

Раздел 1. Введение в надежность и безопасность программного обеспечения.

1. Объект исследования функциональной надежности ПО.
2. Принципиальное отличие между надежностью программ и надежностью технических средств.
3. Трактовка понятия «киберзащищенность ИС». Угрозы и категории киберзащищенности для ИС.
4. Стадии информационной атаки, в чем они заключаются.
5. Типы компьютерных атак на ИС, поражающих ПО.
6. Суть DoS-атак.

7. Взаимосвязь функциональной и информационной безопасности критически важных систем.

Раздел 2. Угрозы надежности и безопасности программного обеспечения.

1. Модель процессов возникновения уязвимостей и ошибок в ходе разработки ПО.
2. Группы проявления программных ошибок.
3. Случаи, когда ошибки оператора приводят к серьезным негативным последствиям.
4. Примеры характерных недостатков эксплуатируемых программ.
5. Назначение троянских программ. Приведите примеры.
6. Назначение основных вредоносных программ.

Раздел 3. Построение надежного программного обеспечения.

1. Уровни представления модели качества ПО.
2. Атрибуты функциональных возможностей ПО.
3. Классификация метрик качества ПО.
4. Стратегия и тактика обеспечения надежности и безопасности различных видов ПО.
5. Основные этапы жизненного цикла современного ПО.
6. Функциональная надежность ПО на различных этапах его жизненного цикла.
7. Как обеспечивается безопасность ПО на различных этапах его жизненного цикла.
8. Маршрутная карта функциональной надежности ПО?
9. Модели надежности ПО. Дайте основные определения этих моделей.
10. Опишите одну из измерительных моделей Коркорэна, Пальчуна, Нельсона.
11. Как производится оценка безопасности ПО на базе модели Нельсона?
12. Охарактеризуйте основные группы показателей функциональной надежности и функциональной безопасности ПО.
13. Связь показателей и свойств надежности ПО.

Раздел 4. Разработка надежного программного обеспечения.

1. Какими рекомендациями следует руководствоваться при разработке спецификации требований к программам?
2. В чем суть защитного программирования?
3. Опишите способы многоверсионного программирования.
4. Охарактеризуйте методы и способы создания проекта надежного ПО.
5. Изложите способы обеспечения надежности системы при интеграции программных и аппаратных средств.
7. Процесс эксплуатации, сопровождения и конфигурации программных средств.
8. Требования к функциональной надежности и архитектуре ПО критически важных систем.
9. Средства и системы тестирования программного обеспечения при испытаниях его на технологическую безопасность вам известны.
10. Обобщенные способы анализа программных средств на предмет наличия (отсутствия) недекларированных возможностей.
11. Основные этапы построения программно-аппаратных комплексов для контроля технологической безопасности программ.
12. Средства и комплексы защиты программ от компьютерных вирусов.
13. Типы обфускаторов программ вам известны.

14. Средства обеспечения целостности и достоверности используемого программного кода.
15. Средства защиты программ от несанкционированного копирования.

Раздел 5. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения.
1. Характеристика ГОСТ Р ИСО/МЭК 61508—2012.
2. Характеристика ГОСТ Р ИСО/МЭК 15408—2013 и каждой из его трех частей.
3. Характеристика ГОСТ Р ИСО/МЭК 18045—2013.
4. Основные этапы сертификации и эксплуатации ПО СЗИ в соответствии с положениями Руководящего документа ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей»?
5. Характеристика «Требованиям к средствам антивирусной защиты, содержащимся в информационном сообщении ФСТЭК России от 30 июля 2012 г. №240/24/3095».

6.2 Примерные вопросы и задания / задачи для промежуточной аттестации

Курс 4

Таблица 9 - Примерные теоретические вопросы и практические задания / задачи к зачету

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания / задачи
Раздел 1. Введение в надежность и безопасность программного обеспечения		
1.1 Виды программного обеспечения	– Системное (базовое) программное обеспечение. – Прикладное программное обеспечение. – Программы встроенных систем.	
1.2 Надежность и отказобезопасность программного обеспечения в информационных системах	– Функциональная надежность программного обеспечения в информационных системах. – Понятие общей надежности информационной системы. – Отказобезопасность и кибербезопасность информационных систем. – Отказобезопасность информационной системы. – Кибербезопасность информационной системы. – Взаимосвязь функциональной и информационной безопасности критически важных систем.	
Раздел 2. Угрозы надежности и безопасности программного обеспечения		
2.1 Угрозы надежности и безопасности программного обеспечения	– Уязвимости программного обеспечения. – Ошибки в программном обеспечении. – Характерные недостатки эксплуатируемых программ. – Вредоносные программы	– Приведите свою таксономию вредоносных программ. - Приведите примеры характерных недостатков эксплуатируемых программ. – Приведите примеры назначение троянских программ. Приведите примеры.

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания / задачи
		– Приведите примеры назначение основных вредоносных программ.
Раздел 3. Построение надежного программного обеспечения		
3.1 Качество программного обеспечения	– Модели качества программного обеспечения. – Метрики качества программного обеспечения. – Некоторые общие замечания по стратегии и тактике обеспечения надежности и безопасности различных видов программного обеспечения. – Обеспечение надежности и безопасности программного обеспечения на различных этапах его жизненного цикла.	– Опишите четыре уровня представления модели качества ПО. – Опишите оценочную модель Джелинского — Моранды; – Опишите оценочную модель Шика — Волвертона, Литтлвуда, Шумана. - Опишите измерительную модель Коркорэна. – Опишите измерительную модель Пальчуна. – Опишите измерительную модель Нельсона. – Приведите пример расчета функциональной надежности программы.
3.2 Правила и этапы построения надежного программного обеспечения	– Маршрутная карта обеспечения функциональной надежности программного обеспечения. – Модели надежности программного обеспечения. – Показатели функциональной надежности и функциональной безопасности ПО.	
Раздел 4 Разработка надежного программного обеспечения		
4.1 Технологии разработки надежного программного обеспечения	– Рекомендации по разработке спецификации требований. - Технология разработки архитектуры надежной программы. – Проектирование надежного программного обеспечения и его реализация. – Интеграция программного обеспечения с аппаратными средствами. – Обеспечение надежности программного обеспечения в процессе подтверждения соответствия, эксплуатации и сопровождения. – Требования к функциональной надежности и архитектуре программного обеспечения критически важных систем.	
4.2 Методы и технологии обеспечения безопасности программного обеспечения	– Методы доказательства правильности программ: общие положения; – Методы доказательства правильности программ: предусловия и постусловия в доказательствах правильности; – Методы доказательства правильности программ: правила вывода (доказательства); – Методы доказательства правильности программ: применение правил вывода;	

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания / задачи
	– Методы доказательства правильности программ: пример доказательства правильности программы для алгоритма дискретного экспоненцирования. – Методы создания самотестирующихся и самокорректирующихся программ. – Криптографические методы защиты от вредоносных программ. – Технологии защиты от вредоносных программ. – Технологии тестирования программного обеспечения на его защищенность. – Методы защиты программ от несанкционированного исследования	
Раздел 5. Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения		
5.1 Отечественные нормативные акты, регламентирующие деятельность в области обеспечения надежности и безопасности программного обеспечения	– Федеральный закон РФ «Об информации, информационных технологиях и о защите информации». – ГОСТ Р ИСО/МЭК 15408—2013 – ГОСТ Р ИСО/МЭК 18045—2013 – ГОСТ Р МЭК 61508—2012 – Приказ ФСТЭК России от 14 марта 2014 г. № 31 – Руководящий документ ФСТЭК России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» – Требования к средствам антивирусной защиты (информационное сообщение ФСТЭК России от 30 июля 2012 г. № 240/24/3095)	– Приведите примеры существующих на отечественном рынке средств обеспечения целостности и достоверности используемого программного кода и средств защиты программ от несанкционированного копирования, их основные достоинства и недостатки. – Приведите примеры существующих на отечественном рынке антивирусных комплексов, их основные достоинства и недостатки. – Охарактеризуйте показатели качества ПО разных уровней (ПО называет преподаватель). – Приведите последовательность операций при выборе номенклатуры показателей качества ПО (ПО называет преподаватель). – Дайте оценку значений показателей качества ПО (ПО называет преподаватель).

Составитель: О. А. Кравцова, к.техн.наук, доцент кафедры информатики и общетехнических дисциплин.