Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО

Заведующий кафедрой

Межинститутская базовая кафедра "Прикладная физика и космические технологии" (ПФиКТ, МИБК)

наименование кафедры

подпись, инициалы, фамилия

«____» _____ 20__г.

институт, реализующий ОП ВО

УТВЕРЖДАЮ

Заведующий кафедрой

Межинститутская базовая кафедра "Прикладная физика и космические

наименование кафедры

Косенко В.Е.

подпись, инициалы, фамилия

«____» _____ 20__г.

институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дисциплина Б1.В.ДВ.02.02 Информационная безопасность

Направление подготовки / специальность 09.04.01 Информатика и вычислительная техника, пррограмма 09.04.01.03 Информационные системы космических

Направленность (профиль)

Форма обучения очная

Год набора 2020

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования с учетом профессиональных стандартов по укрупненной группе

090000 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

Направление подготовки /специальность (профиль/специализация)

Направление 09.04.01 Информатика и вычислительная техника,
пррограмма 09.04.01.03 Информационные системы космических аппаратов и центров управления полетами

Программу составили канд.техн.наук, доцент кафедры, Углев В.А.

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью изучения дисциплины - получение студентами знаний, умений и навыков в области обеспечения информационной безопасности

1.2 Задачи изучения дисциплины

Ведущими задачами изучения данной дисциплины являются:

- изучение средств и методов предотвращения несанкционированного доступа к информации;
- оценка уязвимостей в информационных системах.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

УК-1:Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	
Уровень 2	Знать: - виды и источники угроз при нарушении информационной безопасности (2) - методы предотвращения несанкциони-рованного доступа к информации (2)
Уровень 3	Знать: - возможности современных средств ИиВТ (3)
Уровень 3	Уметь: - брать на себя ответственность за при-нимаемые решения (3) - анализировать и структурировать ин-формацию (3)
Уровень 3	Владеть: - общенаучной и специальной терминологией
УК-2:Способен управлять проектом на всех этапах его жизненного цикла	
Уровень 3	Знать: - принципы системной инженерии (2) - виды и источники угроз при нарушении информационной безопасности (2)
Уровень 3	Уметь: - брать на себя ответственность за при-нимаемые решения (3)
Уровень 3	Владеть: - общенаучной и специальной терминологией

1.4 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационная безопасность» читается в третьем семестре, является дисциплиной по выбору.

Магистрант, начинающий изучение дисциплины «Информационная безопасность» должен знать такие дисциплины, изучаемые ранее, как: «Теория истсем и системный анализ» (1 сем.), «Вычислительные системы» (1 и 2 сем.).

Дисциплина «Информационная безопасность» может быть полезна при выполнении ВКР.

1.5 Особенности реализации дисциплины

Язык реализации дисциплины Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		3
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1 (36)**	**1 (36)**
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,5 (18)	0,5 (18)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
Самостоятельная работа обучающихся:	**2 (72)**	**2 (72)**
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Зачёт)		

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад.час)	Занятия семинарского типа		Самостоятельная работа, (акад.час)	Формируемые компетенции
			Семинары и/или Практические занятия (акад.час)	Лабораторные работы и/или Практикумы (акад.час)		
1	2	3	4	5	6	7
1	Информационная безопасность	18	18	0	72	УК-1 УК-2
Всего		18	18	0	72	

3.2 Занятия лекционного типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Тема 1. Введение (базовые понятия информационной безопасности) Информация и её свойства. Защита информации. Виды информации с позиции защиты. Нарушитель. Цели и задачи информационной защиты	2	0	0
2	1	Тема 2. Защита от НСД Уровни защиты. Организационный уровень. Аппаратный уровень. Программный уровень. Типовые решения и инструменты для каждого уровня	2	0	0

3	1	Тема 3. Модели безопасности ФЗ 152. Модель нарушителя. Модель угроз.	2	0	0
4	1	Тема 4. Стандарты в области ИБ. Стандартизация в области ИБ. ГОСТ Р 53114-2008. ГОСТы группы Р ИСО/МЭК 15408	2	0	0
5	1	Тема 5. Основы криптографии Кодирование и шифрование. Шифрование с открытым и закрытым ключом. Шифры Вижинера, Цезаря, PGP.	4	0	0
6	1	Тема 6. Организация безопасности в вычислительных сетях и рабочих местах Механизмы идентификации и аутентификации. Антивирусная защита. Политика безопасности. Профили пользователей и настройка их прав. Межсетевые экраны и сетевые сканеры.	2	0	0
7	1	Тема 7. Вопросы безопасности при разработке ПО Хакинг и фишинг. Декомпиляция и её предотвращение. Специфика работы с носителями информации и памятью. Тестирование на наличие недокументированных функций.	4	0	0
Всего			18	0	0

3.3 Занятия семинарского типа

			Объем в акад.часах

			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Тема 3. Разработка модели угроз и модели нарушителя	6	0	0
2	1	Тема 5. Шифрование с открытым ключом	6	0	0
3	1	Тема 5. Шифрование с закрытым ключом	6	0	0
Всего			18	0	0

3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
Всего					

5 Фонд оценочных средств для проведения промежуточной аттестации

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Косяков А.	Системная инженерия. Принципы и практика	Москва: ДМК Пресс, 2014
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Тарасенко Ф. П.	Прикладной системный анализ: учебное пособие по специальности "Государственное и муниципальное управление"	Москва: КноРус, 2010
Л2.2	Батоврин В. К.	Системная и программная инженерия	Москва: ДМК Пресс, 2010
Л2.3	Кузнецов В. А., Черепахин А. А.	Системный анализ, оптимизация и принятие решений.: учебник	Москва: ООО "КУРС", 2017

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Э1	Левенчук А.И. Системно-инженерное мышление	http://techinvestlab.ru/files/systems_engineering_thinking/systems_engine.
Э2	Перечень практических заданий и методических рекомендаций к выполнению практических и самостоятельных работ	https://e.sfu-kras.ru/course/view.php?id=16579

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Организация процесса работы по дисциплине «Информационная безопасность» направлена на обучение и контроль знаний магистрантов. В рамках реализации дисциплины предусмотрено:

- Самостоятельное теоретическое обучение – изучение учебной литературы, научных статей; знакомство с методологическими положениями по основным разделам дисциплины, периодическими статистическими изданиями и ежегодниками.
- практическое обучение – подготовка к практическим занятиям по теме, выполнение заданий преподавателя, подготовка отчетов с предоставлением презентационных материалов;
- зачет по завершению всего курса – проверка знаний при завершении изучения дисциплины.

Самостоятельная работа заключается в изучении отдельных тем курса по заданию преподавателя по рекомендуемой им учебной литературе, в проработке определенных задач и проблем, поставленных в ходе развертывания курса.

Результатами самостоятельной работы являются:

Формами текущего контроля по каждому модулю являются следующие виды работ:

- работа магистранта в аудитории;
- защита отчетов по практическим работам.

Формой итогового контроля является зачет, который проводится в устной форме.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

9.1 Перечень необходимого программного обеспечения

9.1.1	1.	ОС MSWindows
9.1.2	2.	MS Office
9.1.3	3.	Объектный паскаль (Delphi)
9.1.4		

9.2 Перечень необходимых информационных справочных систем

9.2.1	Не требуется

10 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Помещения для осуществления образовательного процесса представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Оборудование:

-проекционное оборудование;

-маркерная доска.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья в зависимости от нозологии, осуществляется с использованием средств обучения общего и специального назначения.