

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

**СОГЛАСОВАНО**

**Заведующий кафедрой**

**Кафедра цифровых технологий  
управления**

наименование кафедры

подпись, инициалы, фамилия

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

институт, реализующий ОП ВО

**УТВЕРЖДАЮ**

**Заведующий кафедрой**

**Кафедра цифровых технологий  
управления**

наименование кафедры

**А.А. Ступина**

подпись, инициалы, фамилия

«\_\_\_» \_\_\_\_\_ 20\_\_ г.

институт, реализующий дисциплину

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ  
ИНФОРМАЦИОННАЯ  
БЕЗОПАСНОСТЬ**

Дисциплина Б1.В.ДВ.02.01 Информационная безопасность

Направление подготовки /  
специальность

Направленность  
(профиль)

Форма обучения

Год набора

очная

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)

09.04.03 Прикладная информатика программа магистратуры 09.04.03.07

Информационное обеспечение финансового мониторинга

---

Программу  
составили

PhD, Казаковцев Л.А.

---

## 1 Цели и задачи изучения дисциплины

### 1.1 Цель преподавания дисциплины

Курс посвящен основным аспектам защиты информации и ориентирован на студентов направлений подготовки, не связанных с защитой информации, но связанных с компьютерными науками, информационными технологиями.

В результате курса студенты ознакомятся с основными принципами обеспечения защиты информации, категориями мер защиты информации, принципами построения моделей угроз и нарушителей по методике ФСТЭК, а также оценки безопасности информационных технологий по ГОСТ Р ИСО/МЭК 15408.

### 1.2 Задачи изучения дисциплины

Понимание основных проблем в вопросах безопасности информации.

Формирование терминологической компетентности.

Понимание основных принципов обеспечения защиты информации.

Ознакомление с категориями мер защиты информации, принципами разработки политики безопасности организации.

Понимание принципов построения модели угроз по методике ФСТЭК.

Понимание принципов построения модели нарушителя по методике ФСТЭК.

Понимание принципов оценки безопасности информационных технологий по ГОСТ Р ИСО/МЭК 15408.

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

<b>ОПК-6:Способен исследовать современные проблемы и методы прикладной информатики и развития информационного общества;</b>	
Уровень 1	проблемы и тенденции развития в области информационной безопасности; состояние законодательной базы информационной безопасности; правила защиты информации
Уровень 1	использовать возможности современных методов и средств, включая программные, по обеспечению информационной безопасности в

	профессиональной деятельности
Уровень 1	основной терминологией области безопасности информации
<b>ПК-3:Способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы по финансовому мониторингу (Росфинмониторинг), Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</b>	
Уровень 1	основные положения государственной системы правового обеспечения защиты информации в Российской Федерации; виды технических средств и программных продуктов по защите информации; способы и средства защиты информации
Уровень 1	определять источники и содержание угроз в информационной сфере; использовать технические средства и программные продукты по защите информации
Уровень 1	программно-аппаратными и техническими методами и средствами защиты информации; основными технологиями построения защищенных систем

1.4 Место дисциплины (модуля) в структуре образовательной программы

Информационное общество и проблемы прикладной информатики

Методология и технология проектирования информационных систем

ИТ-инфраструктура цифрового предприятия

выполнение и защита выпускной квалификационной работы

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
<b>Общая трудоемкость дисциплины</b>	<b>4 (144)</b>	<b>4 (144)</b>
<b>Контактная работа с преподавателем:</b>	<b>0,89 (32)</b>	<b>0,89 (32)</b>
занятия лекционного типа	0,22 (8)	0,22 (8)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,67 (24)	0,67 (24)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
<b>Самостоятельная работа обучающихся:</b>	<b>3,11 (112)</b>	<b>3,11 (112)</b>
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
<b>Промежуточная аттестация (Зачёт)</b>		

### 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		8	24	0	112	ОПК-6 ПК-3
Всего		8	24	0	112	

#### 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	Основы информационной безопасности. Основы информационной безопасности. Основные понятия и определения	1	0	0
2	1	Угрозы и нарушители безопасности информации	1	0	0
3	1	Меры обеспечения защиты информации	1	0	0
4	1	Методы контроля и разграничения доступа	1	0	0
5	1	Исторический обзор криптографических методов защиты информации	1	0	0
6	1	Стеганографическая защита информации	1	0	0

7	1	Программно-технические меры защиты информации	1	0	0
8	1	Политика безопасности организации	1	0	0
Всего			2	0	0

### 3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в acad. часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Политика государства в области информационной безопасности	3	0	0
2	1	Модель угроз безопасности информации	3	0	0
3	1	Организационные меры защиты информации	3	0	0
4	1	Разработка плана мероприятий по мерам защиты на предприятии	3	0	0
5	1	Криптографические методы защиты информации	3	0	0
6	1	Техническая защита информации	3	0	0
7	1	Программно-технические меры защиты информации	3	0	0
8	1	Системы обнаружения и предотвращения компьютерных атак	3	0	0
Всего			24	0	0

### 3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в acad. 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	Ступина А. А., Корпачева Л. Н.	Проблемы прикладной информатики в современном информационном обществе: [учебное пособие для студентов напр. 230700.68 «Прикладная информатика» программы подготовки 230700.68.00.02 «Реинжиниринг бизнес-процессов»]	Красноярск: СФУ, 2013
Л1.2	Корпачева Л.Н.	Перспективные направления прикладной информатики: [учеб-метод. материалы к изучению дисциплины для ...09.04.03.02 - Реинжиниринг бизнес-процессов]	Красноярск: СФУ, 2017
Л1.3	Коршун К.В.	Основы информационной безопасности в компьютерных сетях: [учеб-метод. материалы к изучению дисциплины для ...09.04.01.05 Сети ЭВМ и телекоммуникации]	Красноярск: СФУ, 2018
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Горбенко А. О.	Основы информационной безопасности (введение в профессию): Учебное пособие	Санкт-Петербург: Интермедия, 2017

## **8 Методические указания для обучающихся по освоению дисциплины (модуля)**

Во время лекций студент должен уметь сконцентрировать внимание на рассматриваемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого ему необходимо конспектировать материал, излагаемый преподавателем. Необходимо выделять главное и фиксировать основные моменты «своими словами».

Наряду с прослушиванием лекций, важное место в учебном процессе занимают практические занятия. Порядок решения задач студентами может быть различным.

Самостоятельная работа студента состоит в поиске, изучении и систематизации сведений по изучаемой дисциплине, подготовке к практическим занятиям.

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

9.1 Перечень необходимого программного обеспечения

9.2 Перечень необходимых информационных справочных систем

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