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

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра цифровых технологий управления	**Кафедра цифровых технологий управления**
наименование кафедры	наименование кафедры
	А.А. Ступина
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дисциплина Б1.В.ДВ.07.01 Информационная безопасность

Направление подготовки / специальность 38.05.01 Экономическая безопасность
Специализация 38.05.01.01 Экономико-правовое обеспечение экономической

Направленность (профиль)

Форма обучения очная

Год набора 2017

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

380000 «ЭКОНОМИКА И УПРАВЛЕНИЕ»

Направление подготовки /специальность (профиль/специализация)

Специальность 38.05.01 Экономическая безопасность Специализация 38.05.01.01 Экономико-правовое обеспечение экономической безопасности

Программу составили Доцент, Юронен Е.А.

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Цель изучения данной дисциплины – подготовить будущих специалистов-практиков к использованию современных методов и средств защиты информации в организационно-управленческой и аналитической деятельности.

В рамках курса рассматриваются основные понятия информационной безопасности (ИБ), структура мер в области ИБ, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней.

1.2 Задачи изучения дисциплины

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей;

-изучить теорию и практику новейших достижений и перспектив в развития в области создания систем безопасности локальных вычислительных сетей и сети Internet;

- формирование знаний о криптографических методах зашиты информации; основах криптографии; основных методах и приемах защиты от несанкционированного доступа; о компьютерных вирусах и антивирусных программах; организационно-правовом

обеспечение ИБ;

- развитие способности работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

- формирование навыков выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и умения обосновывать свой выбор.

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

ПК-20:способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
Уровень 1	- содержание базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программноаппаратных, математических и т.п. средств их реализации; - современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня.
Уровень 1	- ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; - обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; - ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.
Уровень 1	навыком анализа информационной инфраструктуры государства и общества; навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней.

1.4 Место дисциплины (модуля) в структуре образовательной программы

Информационные технологии в управлении
Экономико-математические методы
Экономическая безопасность
Основы математического программирования

Подготовка к процедуре защиты и защита ВКР

1.5 Особенности реализации дисциплины

Язык реализации дисциплины Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

https://e.sfu-kras.ru/course/view.php?id=1752

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		9
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	Основные термины и понятия	2	0	0	2	ПК-20
2	Угрозы информационной безопасности	1	3	0	24	ПК-20
3	Уровни информационной безопасности	4	1	0	12	ПК-20
4	Стандарты информационной безопасности	2	1	0	8	ПК-20
5	Вредоносное программное обеспечение и защита от него	4	12	0	12	ПК-20
6	Обеспечение доступности и защищенности информационных систем	3	0	0	6	ПК-20
7	Проект модели угроз информационной безопасности	2	1	0	8	ПК-20
Всего		18	18	0	72	

3.2 Занятия лекционного типа

№	№ раздела	Наименование занятий	Объем в акад.часах

п/п	дисциплины		Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	1	0	0
2	1	Объектно-ориентированный подход к информационной безопасности	1	0	0
3	2	Наиболее распространенные угрозы	1	0	0
4	3	Законодательный уровень информационной безопасности	1	0	0
5	3	Административный уровень информационной безопасности	1	0	0
6	3	Процедурный уровень информационной безопасности	1	0	0
7	3	Управление рисками	1	0	0
8	4	Стандарты и спецификации в области информационной безопасности	2	0	0
9	5	Основные программно-технические меры	1	0	0
10	5	Идентификация и аутентификация, управление доступом	1	0	0
11	5	Протоколирование и аудит, шифрование, контроль целостности	1	0	0
12	5	Экранирование, анализ защищенности	1	0	0
13	6	Обеспечение высокой доступности	2	0	0

14	6	Туннелирование и управление	1	0	0
15	7	Создание модели угроз информационной безопасности	2	0	0
Всего			18	0	0

3.3 Занятия семинарского 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	2	Определение окон опасности, уязвимых мест защиты	1	0	0
2	2	Основные угрозы целостности	1	0	0
3	2	Основные угрозы доступности	1	0	0
4	3	Выделение уровней информационной безопасности в структуре предприятия/подразделения	1	0	0
5	4	Проведение сравнительного анализа международных и национальных стандартов и спецификаций в области информационной безопасности	1	0	0
6	5	Вредоносное программное обеспечение, классификация вирусов	3	0	0
7	5	Вредоносное программное обеспечение, признаки присутствия на компьютере вредоносных программ	2	0	0
8	5	Методы защиты от вредоносных программ	3	0	0
9	5	Классификация антивирусов, основы работы антивирусных программ	2	0	0

10	5	Антивирусная защита компьютерной сети и мобильных пользователей	2	0	0
11	7	Составление модели угроз физической и информационной безопасности предприятия/подразделения	1	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					

4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Одинцов Б. Е.	Информационные системы управления эффективностью бизнеса: учебник и практикум для бакалавриата и магистратуры по экономическим направлениям и специальностям	Москва: Юрайт, 2017

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	Широков А. Н., Юркова С. Н.	Местное самоуправление в современной России: концептуальные основы, законодательное регулирование и практическая реализация: монография	Москва: КноРус, 2009

Л1.2	Громов Ю. Ю., Драчев В. О., Иванова О. Г., Шахов Н. Г.	Основы информационной безопасности: учебное пособие для студентов вузов по направлению "Информационные системы и технологии"	Старый Оскол: ТНТ, 2017
Л1.3	Бабурин С. Н., Урсул А. Д., Дзлиев М. И.	Стратегия национальной безопасности России: теоретико-методологические аспекты: Монография	Москва: Издательство "Магистр", 2017
Л1.4	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2017
Л1.5	Ищейнов В. Я., Мецатунян М. В.	Основные положения информационной безопасности: Учебное пособие	Москва: Издательство "ФОРУМ", 2018
Л1.6	Белько Е. С., Богульская Н. А.	Информационная безопасность: учебно-методическое пособие	Красноярск: СФУ, 2018
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	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
Л2.2	Казанцев С.Я., Згадзай О.Э., Оболенский Р.М., Казанцев С.Я.	Правовое обеспечение информационной безопасности: учеб. учебное для студентов вузов	Москва: Академия, 2008
Л2.3	Осипов Г. В., Лисичкин В. А., Вирин М. М.	Становление информационного общества в России и за рубежом: Учебное пособие	Москва: ООО "Юридическое издательство Норма", 2014
Л2.4	Гришина Н. В.	Информационная безопасность предприятия: Учебное пособие	Москва: Издательство "ФОРУМ", 2015
Л2.5	Балдин К. В.	Информационные системы в экономике: Учебное пособие	Москва: ООО "Научно-издательский центр ИНФРА-М", 2017
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год

Л3.1	Одинцов Б. Е.	Информационные системы управления эффективностью бизнеса: учебник и практикум для бакалавриата и магистратуры по экономическим направлениям и специальностям	Москва: Юрайт, 2017

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

Э1	Web-сервер Международной организации по стандартизации [Электронный ресурс]. Режим доступа: www.iso.ch	www.iso.ch
Э2	Web-сервер Международного телекоммуникационного союза [Электронный ресурс]. Режим доступа: www.itu.int	www.itu.int
Э3	Web-сервер с материалами по "Общим критериям"[Электронный ресурс]. Режим доступа: www.commoncriteria.org	www.commoncriteria.org
Э4	Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации [Электронный ресурс]. Режим доступа: www.fstec.ru	www.fstec.ru
Э5	Сервер Государственной технической комиссии при Президенте Российской Федерации[Электронный ресурс]. Режим доступа: www.infotecs.ru	www.infotecs.ru
Э6	Web-сервер Британского института стандартов [Электронный ресурс]. Режим доступа: www.bsi-global.com	www.bsi-global.com

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Организация процесса работы по дисциплине «Информационная безопасность» направлена на обучение и контроль знаний студентов - бакалавров, обучающихся по направлению 09.03.03 «Прикладная информатика», профиль 09.03.03 «Прикладная информатика в государственном и муниципальном управлении». В рамках реализации дисциплины предусмотрено:

- теоретическое обучение - изучение лекционного материала, учебной литературы, научных статей; знакомство с методологическими положениями по основным разделам дисциплины, периодическими статистическими изданиями и ежегодниками,

нормативно-правовыми документами и актами;

- практическое обучение – подготовка к семинарским занятиям, выполнение творческих заданий, подготовка, выполнение и защита реферата, отчета по практическим работам с предоставлением презентационных материалов;
- письменный и устный опрос – проверка знаний по темам курса и при завершении изучения каждого из разделов дисциплины.

Для полного и своевременного освоения темы студент должен изучить лекционный материал и соответствующую теме литературу до семинарского занятия по этой теме.

В ходе изучения дисциплины «Информационная безопасность» предусмотрены следующие виды самостоятельной работы:

1) Самостоятельное изучение теоретического курса по темам предполагает составление опорных конспектов в виде блок-схем и таблиц по темам курса в объеме не менее 2 страниц по каждой теме, запоминание основных понятий, положений и категорий, в т.ч., используя тесты для самоконтроля. Опорные конспекты, в т.ч., блок-схемы и таблицы, сдаются ведущему преподавателю и обсуждаются на практических (семинарских) занятиях по соответствующим темам. Данный вид самостоятельной работы предполагает также подготовку к контрольным (аттестационным) работам.

Для проверки знаний и компетенций по темам в каждом разделе курса студентам предлагаются контрольные вопросы. Результирующая оценка знаний студента по каждому из разделов дисциплины складывается на основе обобщения оценок текущей работы студента и итогового контроля с учетом определенных весовых коэффициентов. Формами текущего контроля по каждому модулю являются следующие виды работ:

- работа студента в аудитории в течение семинарских занятий;
- выполнение домашней работы;
- выполнение индивидуальных и групповых заданий.

Формой итогового контроля является экзамен

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

9.1 Перечень необходимого программного обеспечения

9.1.1	□ электронные таблицы Excel;
9.1.2	□ средство для создания и просмотра презентаций “Microsoft Office PowerPoint”.

9.2 Перечень необходимых информационных справочных систем

9.2.1	Каждый обучающийся в течение всего периода обучения по дисциплине обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде Университета. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к сети Интернет, и отвечают техническим требованиям организации, как на территории Университета, так и вне ее.
9.2.2	Электронная информационно-образовательная среда Университета обеспечивает:
9.2.3	□ доступ к учебным планам, рабочим программам дисциплин (модулей), практик, и к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;
9.2.4	□ фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
9.2.5	□ проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
9.2.6	□ формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;
9.2.7	□ взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети Интернет.
9.2.8	

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

Специально оборудованная аудитория, проектор, компьютер.