

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.07.01 Информационная безопасность

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

38.05.01 ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

Направленность (профиль)

38.05.01.01 Экономико-правовое обеспечение экономической
безопасности

Форма обучения

очная

Год набора

2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

к.техн. наук, Доцент, Скуратенко Е.Н.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью изучения дисциплины является формирование теоретических знаний и практических навыков деятельности, связанной с применением методов управления информационной безопасностью объектов информатизации.

1.2 Задачи изучения дисциплины

Достижение планируемых в рамках дисциплины результатов обучения . Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии (организации);

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

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ПК-20: способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	
ПК-20: способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности	Знает базовые требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности Знает основные требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности Знает большинство требований, установленных нормативными правовыми актами в области защиты государственной тайны и информационной безопасности Умеет соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области информационной безопасности Умеет соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности Умеет соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны, режима коммерческой тайны

	<p>и информационной безопасности, обеспечивать соблюдение режима секретности</p> <p>Владеет базовыми навыками организации работы с соблюдением требований информационной безопасности</p> <p>Владеет основными навыками организации работы с соблюдением требований информационной безопасности</p> <p>Владеет навыками организации работы с соблюдением требований информационной безопасности и соблюдения режима секретности</p>
--	---

1.4 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)	е
		1
Контактная работа с преподавателем:	1 (36)	
занятия лекционного типа	0,5 (18)	
практические занятия	0,5 (18)	
Самостоятельная работа обучающихся:	2 (72)	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

		Контактная работа, ак. час.							
№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Основные понятия и определения информационной безопасности									
	1. Проблемы информационной безопасности в современном обществе. Основные понятия в области защиты информации.	1							
	2.			1					
	3. Проблемы информационной безопасности в современном обществе. Основные понятия в области защиты информации.							8	
	4. Уровни информационной безопасности (личности, общества, государства).	1							
	5.			1					
	6. Уровни информационной безопасности (личности, общества, государства).							6	
2. Угрозы информационной безопасности									

1. Общий анализ угроз безопасности информации. Пути реализации угроз информационной	2							
2. Угрозы безопасности информации			2					
3. Общий анализ угроз безопасности информации. Пути реализации угроз информационной							8	
4. Классификация угроз безопасности информации. Анализ киберугроз.	2							
5. Методические основы оценки угроз.			2					
6. Классификация угроз безопасности информации. Анализ киберугроз.							10	
3. Государственная система информационной безопасности. Законодательный уровень информационной безопасности								
1. Содержание и структура законодательства в области информационной безопасности.	2							
2. Правовое регулирование защиты информации в России.			2					
3. Содержание и структура законодательства в области информационной безопасности.							8	
4. Обзор документов в области обеспечения информационной безопасности по отраслям права. Регуляторы в области информационной безопасности.	1							
5. Изучение нормативных документов в сфере обеспечения информационной безопасности. ФЗ "О персональных данных"			1					
6. Обзор документов в области обеспечения информационной безопасности по отраслям права. Регуляторы в области информационной безопасности.							4	

7. Обзор документов в области юридической ответственности за правонарушения в области информационной безопасности.	1							
8. Обзор документов в области юридической ответственности за правонарушения в области информационной безопасности.			1					
9. Обзор документов в области юридической ответственности за правонарушения в области информационной безопасности.							4	
4. Методы обеспечения информационной безопасности								
1. Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации.	3							
2. Соблюдение режима секретности.			3					
3. Управление информационными рисками. Соблюдение режима секретности. Комплексная защита информации.							10	
4. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации.	2							
5. Аудит информационной безопасности организации. Обзор методических материалов организационных мер защиты информации.			2					
6. Критическая информационная инфраструктура. Категорирование объекта КИИ. Организационные меры обеспечения защиты информации.							8	
7. Программно-технические средства защиты информации.	3							
8. Программно-технические средства защиты информации.			3					

9. Программно-технические средства защиты информации.							6	
Всего	18		18				72	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Сычев Ю.Н. Защита информации и информационная безопасность: Учебное пособие(Москва: ООО "Научно-издательский центр ИНФРА-М").
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
3. Партыка Т. Л., Попов И.И. Информационная безопасность: Учебное пособие(Москва: Издательство "ФОРУМ").
4. Сидорова Т.Ю Информационное пространство и информационная безопасность: [учеб-метод. материалы к изучению дисциплины для ...41.03.05.01 Международные отношения и внешняя политика] (Красноярск: СФУ).
5. Дамм И.А., Акунченко Е.А. Информационные технологии и информационная безопасность в сфере противодействия коррупции: Учебно-методическое пособие для практических занятий, самостоятельной работы и выполнения контрольных работ(Красноярск: СФУ).
6. Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. Информационная безопасность и защита информации: практикум (Дубна: Государственный университет «Дубна»).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. ПО, используемое в учебном процессе по данной дисциплине:
2. регулярно обновляемый интернет-браузер (Mozilla Firefox, Google Chrome, Yandex Browser, либо иной);
3. офисный пакет (MS Office, Libre Office, Open Office, либо иной).

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Информационно-правовой портал Гарант.ру, URL: <http://www.garant.ru>.
2. Официальный сайт компании "КонсультантПлюс", URL: <http://www.consultant.ru>.
3. Сайт библиотеки СФУ. Режим доступа: <http://bik.sfu-kras.ru/>
4. Электронный каталог библиотеки СФУ. Режим доступа: <http://catalog.sfu-kras.ru/>
5. Электронно-библиотечная система Издательства «Лань» <http://e.lanbook.com/>
6. ЭБС ЮРАЙТ <http://www.biblio-online.ru/>
7. Электронно-библиотечная система elibrary <https://elibrary.ru>

8. Электронно-библиотечная система ZNANI-UM.COM (ИНФРА-М)
<http://www.znanium.com/>

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

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

Лекционные занятия –(лекционная аудитория): рабочее место преподавателя, рабочие места обучающихся, компьютер, активные колонки, проектор.учебные аудитории, позволяющие выступающему (преподавателю, студенту) демонстрировать слайды в форматах pdf, PowerPoint и других графических форматах на экране с одновременным выступлением перед аудиторией;

Практические работы – (компьютерный класс): рабочее место преподавателя. Рабочие места обучающихся оснащены доступом в интернет и пакетом офисных программ.

ПО, используемое в учебном процессе по данной дисциплине:

регулярно обновляемый интернет-браузер (Mozilla Firefox, Google Chrome, Yandex Browser, либо иной);

офисный пакет (MS Office, Libre Office, Open Office, либо иной).