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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.19 Информационная безопасность

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

09.03.03 Прикладная информатика

Направленность (профиль)

09.03.03 Прикладная информатика

Форма обучения очная

Год набора 2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

Юронен Е.А.

должность, инициалы, фамилия

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

Информационная безопасность – сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ базис. Это – первая задача курса, для решения которой привлекается объектно-ориентированный подход.

Успех в области ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода – вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и программно-технического уровней. Приводятся сведения о российском и зарубежном законодательстве в области ИБ, о проблемах, существующих в настоящее время в российском законодательстве. На административном уровне рассматриваются политика и программа безопасности, их типовая структура, меры по выработке и сопровождению. На процедурном уровне описываются меры безопасности, имеющие дело с людьми. Формулируются основные принципы, помогающие успеху таких мер. Программно-технический уровень, в соответствии с объектным подходом, трактуется как совокупность сервисов. Дается описание каждого сервиса.

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
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	
ОПК-3.1: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе	

информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
ОПК-3.3: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно- исследовательской работе с учетом требований информационной безопасности	
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	
ОПК-4.1: Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	
ОПК-4.2: Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	
ОПК-4.3: Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы	

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

URL-адрес и название электронного обучающего курса: https://e.sfu-kras.ru/course/view.php?id=1752

.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е 1
Контактная работа с преподавателем:	**1,5 (54)**	
занятия лекционного типа	0,5 (18)	
практические занятия	1 (36)	
Самостоятельная работа обучающихся:	**1,5 (54)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	
Промежуточная аттестация (Экзамен)	**1 (36)**	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		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 термины и понятия									
	1. Понятие информационной безопасности. Основные составляющие. Важность проблемы	1							
	2. Самостоятельное изучение теоретического курса							2	
2. Угрозы информационной безопасности									
	1. Наиболее распространенные угрозы	1							
	2. Определение окон опасности, уязвимых мест защиты			2					
	3. Основные угрозы целостности			2					
	4. Основные угрозы доступности			2					
	5. Самостоятельное изучение теоретического курса							2	
	6. Подготовка и выполнение практических работ							4	
	7. Подготовка и защита реферата							12	
3. Уровни информационной безопасности									

1. Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	1							
2. Процедурный уровень информационной безопасности. Управление рисками	1							
3. Выделение уровней информационной безопасности в структуре предприятия/подразделения			2					
4. Самостоятельное изучение теоретического курса							2	
5. Подготовка и выполнение практических работ							4	
4. Стандарты информационной безопасности								
1. Стандарты и спецификации в области информационной безопасности	1							
2. Проведение сравнительного анализа международных и национальных стандартов и спецификаций в области информационной безопасности			4					
3. Самостоятельное изучение теоретического курса							2	
4. Подготовка и выполнение практических работ							4	
5. Вредоносное программное обеспечение и защита от него								
1. Основные программно-технические меры. Протоколирование и аудит, шифрование, контроль целостности. Экранирование, анализ защищенности	1							
2. Вредоносное программное обеспечение, классификация вирусов			4					
3. Вредоносное программное обеспечение, признаки присутствия на компьютере вредоносных программ			4					
4. Методы защиты от вредоносных программ			4					
5. Классификация антивирусов, основы работы антивирусных программ			2					

6. Антивирусная защита компьютерной сети и мобильных пользователей			2					
7. Самостоятельное изучение теоретического курса							2	
8. Подготовка и выполнение практических работ							12	
6. Обеспечение доступности и защищенности информационных систем								
1. Обеспечение высокой доступности	4							
2. Туннелирование и управление	2							
3. Самостоятельное изучение теоретического курса							2	
7. Проект модели угроз информационной безопасности								
1. Создание модели угроз информационной безопасности	6							
2. Составление модели угроз физической и информационной безопасности предприятия/подразделения			4					
3. Разработка политики безопасности предприятия/подразделения			4					
4. Самостоятельное изучение теоретического курса							2	
5. Подготовка и выполнение практических работ							4	
Всего	18		36				54	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Широков А. Н., Юркова С. Н. Местное самоуправление в современной России: концептуальные основы, законодательное регулирование и практическая реализация: монография(Москва: КноРус).
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).
3. Бабурин С. Н., Урсул А. Д., Дзлиев М. И. Стратегия национальной безопасности России: теоретико-методологические аспекты: Монография(Москва: Издательство "Магистр").
4. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
5. Ищейнов В. Я., Мецатунян М. В. Основные положения информационной безопасности: Учебное пособие(Москва: Издательство "ФОРУМ").
6. Белько Е. С., Богульская Н. А. Информационная безопасность: учебно-методическое пособие(Красноярск: СФУ).
7. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М., Казанцев С.Я. Правовое обеспечение информационной безопасности: учеб. учебное для студентов вузов(Москва: Академия).
8. Осипов Г. В., Лисичкин В. А., Вирин М. М. Становление информационного общества в России и за рубежом: Учебное пособие (Москва: ООО "Юридическое издательство Норма").
9. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие(Москва: Издательство "ФОРУМ").
10. Балдин К. В. Информационные системы в экономике: Учебное пособие (Москва: ООО "Научно-издательский центр ИНФРА-М").
11. Одинцов Б. Е. Информационные системы управления эффективностью бизнеса: учебник и практикум для бакалавриата и магистратуры по экономическим направлениям и специальностям(Москва: Юрайт).

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

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

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.
2. Электронная информационно-образовательная среда Университета обеспечивает:
3. доступ к учебным планам, рабочим программам дисциплин (модулей), практик, и к изданиям электронных библиотечных систем и электронным образовательным ресурсам, указанным в рабочих программах;
4. фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения основной образовательной программы;
5. проведение всех видов занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;
6. формирование электронного портфолио обучающегося, в том числе сохранение работ обучающегося, рецензий и оценок на эти работы со стороны любых участников образовательного процесса;
7. взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети Интернет.
8.

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)

Специально оборудованная аудитория, проектор, компьютер.