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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.17 Информационная безопасность организации

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

09.03.03 Прикладная информатика

Направленность (профиль)

09.03.03.04 Прикладная информатика в государственном и муниципальном управлении

Форма обучения очная

Год набора 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

кпн, Доцент, Янченко И.В.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью преподавания дисциплины является освоение и систематизация студентами знаний по информационной безопасности (ИБ) на уровне личности, предприятия, государства для защиты информационных ресурсов от вероятных угроз.

1.2 Задачи изучения дисциплины

Задачи изучения дисциплины включают освоение подходов к решению проблем защиты информации: на уровне применения отдельных организационных мероприятий, технических и программных средств (фрагментарный подход); на уровне применения целостной системы защиты компьютерной системы во все время ее функционирования (системный подход); на уровне непрерывного процесса защиты информации на всех этапах жизненного цикла компьютерной системы с комплексным применением всех имеющихся методов, средств и мероприятий (комплексный подход).

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: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Знать: место информационной безопасности в национальной безопасности страны; концепцию информационной безопасности, конституционные и законодательные основы ее реализации; меры ответственности за деяния, совершенные в сфере информационной деятельности; источники и виды угроз информационной безопасности организации; направления формирования и функционирования комплексной системы защиты информации в организации. Уметь: выявлять угрозы информационной безопасности организации и строить модель угроз; строить модель нарушителя информационной безопасности организации; строить концептуальную модель защиты информации. Владеть: навыками формирования требований к информационной системе в рамках информационной безопасности; навыками категорирования объектов критической информационной инфраструктуры; навыками защиты информации от вредоносных программ и сетевых атак с помощью антивирусных программ, криптографических и других методов

	защиты.

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=27026.

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)	
лабораторные работы	1 (36)	
Самостоятельная работа обучающихся:	**3,5 (126)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Да	
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. Правовое регулирование защиты информации в России									
	1. Понятие информации как объекта защиты. Уровни информационной безопасности. Концептуальная модель информационной безопасности	2	2						
	2. Содержание и структура законодательства в области информационной безопасности	2	2						
	3. Классификация угроз безопасности информации. Портрет нарушителя информационной безопасности. Криминалистическая характеристика компьютерного преступления	2	2						
	4. Лабораторная работа 1. Законодательство в сфере информационной безопасности					2	2		
	5. Изучение теоретического курса, курсовая работа							40	10
2. Организационно-правовые методы обеспечения защиты информации									

1. Организационные меры обеспечения защиты информации. Принципы политики безопасности. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности	2	2						
2. Концепция системы безопасности предприятия. Правовой статус службы безопасности	2	2						
3. Каналы утечки информации. Средства блокирования каналов утечки информации. Основные функции службы безопасности.	2	2						
4. Лабораторная работа 6. Концептуальная модель защиты информации на примере гипотетического предприятия					4	4		
5. Лабораторная работа 7. Порядок категорирования объектов КИИ					4	4		
6. Лабораторная работа 8. Категорирование объекта КИИ					4	4		
7. Изучение теоретического курса, курсовая работа							40	8
3. Программно-технические методы обеспечения информационной безопасности								
1. Программные средства защиты информации. Подходы к выбору средств защиты	2	2						
2. Основные положения и базовые криптографические понятия. Метод частотного криптоанализа. Базовые криптографические методы и схемы защиты информации.	2	2						
3. Комплексный подход к защите информации	2	2						
4. Лабораторная работа 9. Частотный криптоанализ для вскрытия шифра алфавитной замены					4	2		

5. Лабораторная работа 10. Симметричные алгоритмы шифрования.					4	2		
6. Лабораторная работа 11. Шифры гаммирования					4	2		
7. Лабораторная работа 12. Асимметричные алгоритмы шифрования. RSA					4	4		
8. Лабораторная работа 14. Шифрование средствами PGP					2	2		
9. Лабораторная работа 15. Защита электронных сообщений с помощью ЭЦП					4	4		
10. Изучение теоретического курса, курсовая работа							46	6
Всего	18	18			36	30	126	24

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие(Москва: Издательство "ФОРУМ").
2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
4. Партыка Т. Л., Попов И.И. Информационная безопасность: Учебное пособие(Москва: Издательство "ФОРУМ").
5. Соловьева Т. В. Информационная безопасность: учебное пособие (Абакан: ХТИ - филиал СФУ).
6. Янченко И.В Информационная безопасность: [учеб-метод. материалы к изучению дисциплины для ...09.03.03.04 Прикладная информатика в государственном и муниципальном управлении](Красноярск: СФУ).

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. Агент администрирования Kaspersky Security Center 10, Kaspersky Endpoint Security 10 для Windows, СЗИ от НСД Dallas Lock 8.0-C, PGP, Microsoft Office, браузеры и др.

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

1. Научная библиотека СФУ, URL: https://bik.sfu-kras.ru;
2. Электронный каталог АБИС-ИРБИС", URL: http://irbis.khti.ru/cgi-bin/irbis64r_15/cgiirbis_64.exe?LNG=&C21COM=F&I21DBN=KNIG&P21DBN=KNIG.
3. Система электронного обучения СФУ, URL: https://e.sfu-kras.ru.
4. Электронно-библиотечная система ZNANIUM.COM (ИНФРА-М) http://www.znanium.com/
5.

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 проводятся в лекционных аудиториях, оснащенных проекционным оборудованием, компьютером, рабочими местами для преподавателя и студентов, магнитно-маркерной или меловой доской.

Лабораторные работы и самостоятельная работа студентов выполняются в компьютерных классах, объединенных в локальную сеть с выходом в Интернет. Компьютерные классы оборудованы рабочими местами на 12 компьютеров.