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

Направление подготовки (специальность) 09.03.03 Прикладная информатика

Профиль подготовки (специализация) 09.03.03.04 Прикладная информатика в государственном и муниципальном управлении

Форма обучения очная

Год набора 2021

Красноярск 2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили
Доцент,кф-мн _____ Таскин Андрей Николаевич

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 высшего образования:

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;	

1.4 Особенности реализации дисциплины.

URL-адрес и название электронного обучающего курса

https://e.sfu-kras.ru/course/view.php?id=37423

Дисциплина реализуется с применением ЭО и ДОТ

2 Объем дисциплины (модуля)

Вид учебной работы	**Всего, зачетных единиц (акад.час)**	**Семестр**
		5
Общая трудоемкость дисциплины	6 (216)	6 (216)
Контактная работа с преподавателем:	1,5 (54)	1,5 (54)
занятия лекционного типа	0,5 (18)	0,5 (18)
лабораторные работы	1 (36)	1 (36)
Самостоятельная работа обучающихся	3,5 (126)	3,5 (126)
Вид промежуточной аттестации (Экзамен)	36	Экзамен,КР

3 Содержание дисциплины (модуля)

№ п/п	Вид работ	Темы занятия	Объем часов	Семестр /курс	Часы в эл. формате	РО	Мероприятия текущего контроля и ПА
Раздел 1. Правовое регулирование защиты информации в России							
1.	Лек	Понятие информации как объекта защиты. Уровни информационной безопасности. Концептуальная модель информационной безопасности	2	5		ОПК-3	
2.	Лек	Содержание и структура законодательства в области информационной безопасности	2	5		ОПК-3	
3.	Лек	Классификация угроз безопасности информации. Портрет нарушителя информационной безопасности. Криминалистическая характеристика компьютерного преступления	2	5		ОПК-3	
4.	Лаб	Лабораторная работа 1. Законодательство в сфере информационной безопасности	2	5		ОПК-3	
5.	Ср	Изучение теоретического курса, курсовая работа	40	5			
Раздел 2. Организационно-правовые методы обеспечения защиты информации							
1.	Лек	Организационные меры обеспечения защиты информации. Принципы политики безопасности. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности	2	5		ОПК-3	
2.	Лек	Концепция системы безопасности предприятия. Правовой статус службы безопасности	2	5		ОПК-3	
3.	Лек	Каналы утечки информации. Средства блокирования каналов утечки информации. Основные функции службы безопасности.	2	5		ОПК-3	
4.	Лаб	Лабораторная работа 6. Концептуальная модель защиты информации на примере гипотетического предприятия	4	5		ОПК-3	
5.	Лаб	Лабораторная работа 7. Порядок категорирования объектов КИИ	4	5		ОПК-3	
6.	Лаб	Лабораторная работа 8. Категорирование объекта КИИ	4	5		ОПК-3	
7.	Ср	Изучение теоретического курса, курсовая работа	40	5		ОПК-3	
Раздел 3. Программно-технические методы обеспечения информационной безопасности							
1.	Лек	Программные средства защиты информации. Подходы к выбору средств защиты	2	5		ОПК-3	
2.	Лек	Основные положения и базовые криптографические понятия. Метод частотного криптоанализа. Базовые криптографические методы и схемы защиты информации.	2	5		ОПК-3	
3.	Лек	Комплексный подход к защите информации	2	5		ОПК-3	
4.	Лаб	Лабораторная работа 9. Частотный криптоанализ для вскрытия шифра алфавитной замены	4	5		ОПК-3	
5.	Лаб	Лабораторная работа 10. Симметричные алгоритмы шифрования.	4	5		ОПК-3	
6.	Лаб	Лабораторная работа 11. Шифры гаммирования	4	5		ОПК-3	

7.	Лаб	Лабораторная работа 12. Асимметричные алгоритмы шифрования. RSA	4	5		ОПК-3	
8.	Лаб	Лабораторная работа 14. Шифрование средствами PGP	2	5		ОПК-3	
9.	Лаб	Лабораторная работа 15. Защита электронных сообщений с помощью ЭЦП	4	5		ОПК-3	
10.	Ср	Изучение теоретического курса, курсовая работа	46	5		ОПК-3	
Раздел 4. Экзамен							
1.	Экзамен	Экзамен	36	5			

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Партыка Т. Л., Попов И. И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2019. - 432 с. – Режим доступа: https://znanium.com/catalog/document?id=327912 .

2. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО□, 2019. - 336 с. – Режим доступа: https://znanium.com/catalog/document?id=336219 .

3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО□, 2021. - 336 с. – Режим доступа: https://znanium.com/catalog/document?id=364911 .

4. Партыка Т. Л., Попов И.И. Информационная безопасность [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2021. - 432 с. – Режим доступа: https://znanium.com/catalog/document?id=364624 .

5. Соловьева Т. В. Информационная безопасность:учебное пособие. - Абакан: ХТИ - филиал СФУ, 2015. - 155 с..

6. Янченко И.В Информационная безопасность [Электронный ресурс]:[учеб-метод. материалы к изучению дисциплины для ...09.03.03.04 Прикладная информатика в государственном и муниципальном управлении]. - Красноярск: СФУ, 2020. - – Режим доступа: https://e.sfu-kras.ru/course/view.php?id=26545 .

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. Microsoft Office Professional Plus 2019 Russian Academic. Офисный пакет Microsoft Office.

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

1. Информационная безопасность
2. СПС КонсультантПлюс
3. СПС Гарант

5 Фонд оценочных средств

Фонд оценочных средств является приложением к рабочей программе дисциплины (модуля), хранится на кафедре, обеспечивающей преподавание данной дисциплины (модуля).

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.