

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

Б1.В.ДВ.03.01 Защита программ и данных

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

27.03.03 СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ

Направленность (профиль)

27.03.03 СИСТЕМНЫЙ АНАЛИЗ И УПРАВЛЕНИЕ

Форма обучения

очная

Год набора

2020

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

PhD, доцент, Кирко И.Н.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины «Защита программ и данных» является формирование знаний, умений и навыков:

- ценностно-информационного подхода к проблемам защиты информации;
- осуществления организационно-правового и инженерно-технического обеспечения защиты информации;
- инсталляции, настройки программных СЗИ;
- обеспечения эффективного функционирования СЗИ с учетом требований по обеспечению ИБ;
- о методах и средствах защиты информации в компьютерных системах;
- о защитных механизмах, реализованных в средствах защиты компьютерных систем от несанкционированного доступа (НСД);
- о применении средств криптографической защиты информации и средств защиты от НСД для решения задач защиты информации;
- о современных программно-аппаратных комплексах защиты информации.

1.2 Задачи изучения дисциплины

Сформировать

способность использовать общеправовые знания в различных сферах деятельности

способность применять принципы оценки, контроля и менеджмента качества

способность к освоению новой техники, новых методов и новых технологий

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
ОК-6: способностью использовать общеправовые знания в различных сферах деятельности	
ОК-6: способностью использовать общеправовые знания в различных сферах деятельности	основные сферы правовой деятельности общества; способы использования полученного образования в своей профессиональной деятельности; основы построения нормативно-правовых документов; ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности; использовать правовые нормы в профессиональной и

	<p>общественной деятельности. использовать общеправовые знания в сферах защиты информации; системой законодательства и нормативных правовых актов, регламентирующих сферу профессиональной деятельности;</p> <p>правовыми нормами общеправовыми знаниями</p>
<p>ОПК-4: способностью применять принципы оценки, контроля и менеджмента качества</p>	
<p>ОПК-4: способностью применять принципы оценки, контроля и менеджмента качества</p>	<p>теоретические основы принципов оценки, контроля и менеджмента качества с учетом основных требований информационной безопасности основы использования принципов оценки, контроля и менеджмента качества на базе информационной культуры; подходы к освоению принципов оценки, контроля и менеджмента с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; использовать принципы оценки, контроля и менеджмента качества с учетом основных требований информационной безопасности; осваивать принципы оценки, контроля и менеджмента качества с учетом основных требований информационной безопасности. проводить анализ при оценке контроля и менеджмента качества с учетом основных требований информационной безопасности; навыками решения стандартных задач на основе принципов оценки, контроля и менеджмента качества в профессиональной деятельности;</p> <p>навыками профессиональной деятельности на основе применения принципов оценки, контроля и менеджмента качества; информационно-коммуникационными технологиями с учетом основных требований информационной безопасности в сфере менеджмента качества;</p>
<p>ОПК-7: способностью к освоению новой техники, новых методов и новых технологий</p>	

<p>ОПК-7: способностью к освоению новой техники, новых методов и новых технологий</p>	<p>теоретические основы современных методов, технологий в сфере защиты информации;й.</p> <p>способы использования новой техники, новых методов и новых технологий по защите информации; основы построения политики безопасности при появлении новой техники, новых методов и новых технологий</p> <p>ориентироваться в системе обеспечения новой</p>
	<p>техникой и новыми технологиями с позиций защиты ресурсов;</p> <p>использовать новую технику, новые методы и новые технологии с учетом основных требований информационной безопасности.</p> <p>использовать профессиональные знания в сферах защиты информации.</p> <p>способами анализа по замене устаревшего оборудования с учетом основных требований информационной безопасности;</p> <p>навыками составления планов и проектов по замене устаревшего оборудования с учетом основных требований информационной безопасности.</p> <p>навыками составления планов и проектов по замене устаревших технологий с учетом основных требований информационной безопасности.</p>
<p>ПК-1: способностью принимать научно-обоснованные решения на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности</p>	

<p>ПК-1: способностью принимать научно-обоснованные решения на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности</p>	<p>теоретические основы принятия научно-обоснованных решений на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний;</p> <p>способы использования принятия научно-обоснованных решений на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний;</p> <p>– основы построения постановки и выполнения экспериментов по проверке их корректности и эффективности.</p> <p>использовать принципы оценки, контроля и менеджмента качества с учетом основных требований информационной безопасности;</p>
	<p>осваивать принципы оценки, контроля и менеджмента качества с учетом основных требований информационной безопасности. проводить анализ при оценке контроля и менеджмента качества с учетом основных требований информационной безопасности; способами анализа научно-обоснованных решений на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, с учетом основных требований информационной безопасности;</p> <p>навыками составления планов и проектов научно-обоснованных решений на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, с учетом основных требований информационной безопасности.</p> <p>навыками выполнения экспериментов по проверке их корректности и эффективности с учетом основных требований информационной</p>

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=15242>.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е
		1
Контактная работа с преподавателем:	2 (72)	
занятия лекционного типа	1 (36)	
практические занятия	1 (36)	
Самостоятельная работа обучающихся:	2 (72)	
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.											
		1. Состав отечественного и международного законодательства в области обеспечения информационной безопасности	3								
		2. Изучение законов РФ в сфере защиты информации.			3						
		3. Работа с литературой							6		
		4. Программная и аппаратная антивирусная защита информации	4								
		5. Использование антивирусных пакетов			4						
		6. Работа с литературой							8		
		7. Принципы и средства защиты информации от несанкционированного доступа	3								
		8. Защита информации в текстовом процессоре Microsoft Word.			3						
		9. Работа с литературой							6		

10. Обеспечение информационной безопасности в системах управления базами данных	3							
11. Защита информации в программе Microsoft Office Excel.			3					
12. Работа с литературой							6	
13. Криптографическая защита информации	4							
14. Защита информации в программе Microsoft Access.			4					
15. Работа с литературой							8	
16. Система обнаружения атак и вторжений	3							
17. Алгоритмы шифрования			3					
18. Работа с литературой							6	
19. Классификация технических каналов утечки информации. Программно-аппаратные средства обнаружения ПЭМИ и наводок.	4							
20. Создание проекта по компьютерной защите информации с использованием технических средств ЗИ.			4					
21. Работа с литературой							8	
22. Программно-аппаратные средства обнаружения утечки речевой и видеоинформации	4							
23. Защита информации в среде программирования Matlab.			4					
24. Работа с литературой							8	
25. Облачные технологии	4							
26. Использование облачных технологий и вопросы защиты информации			4					
27. Работа с литературой							8	

28. Стеганография	4							
29. Стеганографические методы защиты информации			4					
30. Работа с литературой							8	
31.								
Всего	36		36				72	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие(Москва: Форум).
2. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: учебное пособие.; рекомендовано УМО по образованию в области информационных технологий и систем(М.: ИНФРА-М).
3. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие(Москва: Форум).
4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебное пособие(М.: ИНФРА-М).
5. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации: Учебное пособие(Москва: Издательский Центр РИО□).
6. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие(Москва: Издательство "ФОРУМ").
7. Вайнштейн Ю. В., Демин С. Л., Кирко И. Н., Кучеров М. Н., Сомова М. В. Основы информационной безопасности: электрон. учеб.-метод. комплекс дисциплины(Красноярск).

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. Язык высокого уровня C++;
2. Язык высокого уровня DELPHI;
3. Среда разработки MATHCAD;
4. Среда разработки MATHLAB.

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

1. Консультант Плюс

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)

Язык высокого уровня C++, пакеты MATHCAD, MATHLAB, MICROSOFT OFFICE, Справочная система Консультант Плюс, компьютерный класс, мультимедийная доска.