

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

СОГЛАСОВАНО

Заведующий кафедрой

**Кафедра прикладной
математики и компьютерной
безопасности (ПМКБ_ИКИТ)**

наименование кафедры

подпись, инициалы, фамилия

«___» _____ 20__ г.

институт, реализующий ОП ВО

УТВЕРЖДАЮ

Заведующий кафедрой

**Кафедра прикладной математики
и компьютерной безопасности
(ПМКБ_ИКИТ)**

наименование кафедры

Кытманов А.А.

подпись, инициалы, фамилия

«___» _____ 20__ г.

институт, реализующий дисциплину

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ И ЗАЩИТА
ИНФОРМАЦИИ**

Дисциплина Б1.О.19 Информационная безопасность и защита информации

Направление подготовки / 09.03.01 Информатика и вычислительная техника
специальность

Направленность
(профиль)

Форма обучения очная

Год набора 2020

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования с учетом профессиональных стандартов по укрупненной группе

090000 «ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА»

Направление подготовки /специальность (профиль/специализация)

Направление 09.03.01 Информатика и вычислительная техника

Программу
составили

канд.пед.наук, доцент, Кирко И.Н.

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью дисциплины 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 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

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

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:Знать: 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.	
Уровень 1	Знает принципы на основе информационной и решения стандартных задач библиографической культуры с профессиональной деятельности на применении информационно-основе информационной и коммуникационных технологий и с библиографической культуры с учетом основных требований применении информационно-информационной безопасности коммуникационных технологий и с учетом основных требований информационной безопасности
Уровень 2	Знает методы на основе информационной и решения стандартных задач библиографической культуры с профессиональной деятельности на применении информационно-основе информационной и коммуникационных технологий и с библиографической культуры с учетом основных требований применении информационно-информационной безопасности коммуникационных технологий и с учетом основных требований информационной безопасности
Уровень 3	Знает средства на основе информационной и решения стандартных задач библиографической культуры с профессиональной деятельности на применении информационно-основе информационной и коммуникационных технологий и с библиографической культуры с учетом основных требований применении информационно-информационной безопасности коммуникационных технологий и с учетом основных требований информационной безопасности
Уровень 1	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-

	коммуникационных технологий и с учетом основных требований информационной безопасности.
Уровень 2	Умеет нестандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
Уровень 3	Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, которые носят ситуативный характер
Уровень 1	Владеет навыками подготовки обзоров, по научно-исследовательской работе с учетом требований информационной безопасности.
Уровень 2	Владеет навыками подготовки аннотаций, составления рефератов, научных докладов, публикаций по научно-исследовательской работе с учетом требований информационной безопасности.
Уровень 3	Владеет навыками подготовки библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ОПК-3.2: Уметь: 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: Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	

1.4 Место дисциплины (модуля) в структуре образовательной программы

Б1.О Информационные системы и технологии

Изучение дисциплины необходимо для прохождения

Б1.В.01 Разработка и стандартизация программных средств и информационных технологий

1.5 Особенности реализации дисциплины

Язык реализации дисциплины Русский.

Дисциплина (модуль) реализуется с применением ЭО и ДОТ

<https://e.sfu-kras.ru/course/view.php?id=32785>

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		4
Общая трудоемкость дисциплины	3 (108)	3 (108)
Контактная работа с преподавателем:	1,5 (54)	1,5 (54)
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа		
в том числе: семинары		
практические занятия	1 (36)	1 (36)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
Самостоятельная работа обучающихся:	1,5 (54)	1,5 (54)
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Зачёт)		

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад. час)	Занятия семинарского типа		Самостоятельная работа, (акад. час)	Формируемые компетенции
			Семинары и/или Практические занятия (акад. час)	Лабораторные работы и/или Практикумы (акад. час)		
1	2	3	4	5	6	7
1		18	36	0	18	ОПК-3.1 ОПК-3.2 ОПК-3.3
Всего		18	36	0	18	

3.2 Занятия лекционного типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад. часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Состав отечественного и международного законодательства в области обеспечения информационной безопасности	2	0	0
2	1	Программная и аппаратная антивирусная защита информации	2	0	0
3	1	Принципы и средства защиты информации от несанкционированного доступа	1	0	0
4	1	Обеспечение информационной безопасности в системах управления базами данных	2	0	0

5	1	Криптографическая защита информации	2	0	0
6	1	Система обнаружения атак и вторжений	2	0	0
7	1	Классификация технических каналов утечки информации. Программно-аппаратные средства обнаружения ПЭМИ и наводок.	2	0	0
8	1	Программно-аппаратные средства обнаружения утечки речевой и видеоинформации	2	0	0
9	1	Облачные технологии	2	0	0
10	1	Стеганография	1	0	0
Всего			18	0	0

3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в acad. часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Изучение законов РФ в сфере защиты информации.	4	0	0
2	1	Использование антивирусных пакетов	4	0	0
3	1	Защита информации в текстовом процессоре Microsoft Word.	3	0	0
4	1	Защита информации в программе Microsoft Office Excel.	3	0	0
5	1	Защита информации в программе Microsoft Access.	4	0	0
6	1	Алгоритмы шифрования	3	0	0
7	1	Создание проекта по компьютерной защите информации с использованием технических средств ЗИ.	4	0	0

8	1	Защита информации в среде программирования Matlab.	4	0	0
9	1	Использование облачных технологий и вопросы защиты информации	4	0	0
10	1	Стеганографические методы защиты информации	3	0	0
Всего			26	0	0

3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад. часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
Всего					

4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Вайнштейн Ю. В., Демин С. Л., Кирко И. Н., Кучеров М. Н., Сомова М. В.	Основы информационной безопасности: электрон. учеб.-метод. комплекс дисциплины	Красноярск, 2007

5 Фонд оценочных средств для проведения промежуточной аттестации

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Гришина Н.В.	Информационная безопасность предприятия: Учебное пособие	Москва: Форум, 2015

Л1.2	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, 2013
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Партыка Т. Л., Попов И. И.	Информационная безопасность: учебное пособие	Москва: Форум, 2014
Л2.2	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие	М.: ИНФРА-М, 2014
Л2.3	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2017
Л2.4	Партыка Т. Л., Попов И. И.	Информационная безопасность: Учебное пособие	Москва: Издательство "ФОРУМ", 2018
6.3. Методические разработки			
	Авторы, составители	Заглавие	Издательство, год
Л3.1	Вайнштейн Ю. В., Демин С. Л., Кирко И. Н., Кучеров М. Н., Сомова М. В.	Основы информационной безопасности: электрон. учеб.-метод. комплекс дисциплины	Красноярск, 2007

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Э1	Защита программ и данных	https://e.sfu-kras.ru/course/view.php?id=1955
----	--------------------------	---

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Дисциплина базируется на использовании электронного образовательного ресурса. ЭОР в соответствии с программой дисциплины включает теоретический материал, перечень практических работ, а также ресурс для самостоятельной работы. Формы работы – аудиторная и внеаудиторная (дистанционная).

Всего количество часов для изучения дисциплины: лекции – 18, практические работы и лабораторные работы – 36, самостоятельная работа – 54.

Структура ресурса содержит следующие компоненты:

- Аннотация

- Рабочая программа
- ФОС
- Методические рекомендации
- Новостной форум
- Глоссарий
- Описание режима обучения
- Входной тест
- Темы

Тема «Разное» включает учебный фильм, темы для самостоятельной работы, а также список основной и дополнительной литературы.

Изучение курса начинается с входного тестирования.

Теоретическое изучение курса начинается с работы в лекционной аудитории. Современные средства обучения (интерактивная доска, локальная сеть) позволяют использовать ЭОР по дисциплине как преподавателю, так и студентам непосредственно на лекции.

Гиперссылки на внешние источники дают возможность студентам углубить свои познавательные интересы и актуализировать ранее изученные материалы.

Практические и лабораторные работы содержат 10 заданий. Постановка задачи и инструкции к выполнению практических работ представлены в каждой теме. Выполнение работы в рамках аудиторного времени рассчитано на 1-2 часа. Студенты, не успевшие выполнить работу, могут закончить ее в режиме самостоятельной работы. Практические работы предполагают использование современного языка высокого уровня. Защита работы осуществляется в режиме аудиторных занятий.

Видеофильм студенты просматривают в режиме самостоятельной работы. Обсуждение просмотренного материала запланировано на лекции, посвященной программно-аппаратным средствам обнаружения утечки информации.

В рамках самостоятельной работы после каждой лекции студенты должны пройти тестирование и выполнить задание (дистанционно), которое приведено в конце каждой темы. Преподаватель в свою очередь делает замечание на ответы по заданиям и дает оценку проведенной работы. Студенты, получившие низкий балл по тестированию к заданию могут повторно обратиться к ресурсу (дистанционно).

Темы для самостоятельной работы содержатся в рабочей программе. 36 часов, которые отводятся для самостоятельной работы, позволяют студентам развить свой обучающий потенциал и освоить образовательную программу в полном объеме, независимо от их местонахождения. Доступ к электронному ресурсу в любое время и в любом месте дает возможность использовать весь потенциал дистанционной формы обучения.

Преподаватель может своевременно обновлять материал и давать объявление на форуме. Законодательство в сфере информационной безопасности очень динамично и студенты имеют возможность получить актуальные знания в соответствии с требованиями современных научных достижений.

Глоссарий позволяет студентам освежить знания терминов и определений в среде защиты информации.

Итоговый тест содержит вопросы из разных тем ресурса и позволяет повторить пройденный материал.

На завершающем этапе обучения – зачете, преподаватель учитывает уровень проработки тестового материала, заданий и рефератов. Выполнение всего списка практических работ является обязательным требованием для допуска к зачету. Студенты, которые находятся на индивидуальном обучении, при наличии официального разрешения, имеют возможность обучаться дистанционно в полном объеме и получать консультации с использованием электронной почты. Присутствие таких студентов на зачете является обязательным.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

9.1 Перечень необходимого программного обеспечения

9.1.1	1.	Язык высокого уровня C++;
9.1.2	2.	Язык высокого уровня DELPHI;
9.1.3	3.	Среда разработки MATHCAD;
9.1.4	4.	Среда разработки MATHLAB.

9.2 Перечень необходимых информационных справочных систем

9.2.1	Консультант Плюс
-------	------------------

10 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.