

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

Б1.В.09 Информационная безопасность и защита
информации

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.03.04 Прикладная математика

Направленность (профиль)

01.03.04 Прикладная математика

Форма обучения

очная

Год набора

2021

Красноярск 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

канд.пед.наук, доцент, Кирко И.Н.

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью освоения дисциплины является формирование у будущего специалиста способности и умения защищать информационные ресурсы от всех возможных угроз информационной безопасности.

1.2 Задачи изучения дисциплины

Задачи изучения дисциплины включают:

освоение методов обеспечения конфиденциальности, целостности и доступности информационных ресурсов;

приобретение практических навыков использования методов защиты информации.

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 |
|--|--|
| ПК-3: Способен применять математический аппарат для решения поставленных задач. | |
| ПК-3.1: Знать основы применения математического аппарата для решения поставленных задач. | принципы применения математического аппарата для решения задач информационной безопасности способы применения математического аппарата для решения задач информационной безопасности методы применения математического аппарата для решения задач информационной безопасности применить инструменты математического аппарата для решения задач информационной безопасности применить базовые основы математического аппарата для решения задач информационной безопасности применить подходы математического анализа для решения задач информационной безопасности принципами применения математического аппарата для решения задач информационной безопасности способами применения математического аппарата для решения задач информационной безопасности методами применения математического аппарата для решения задач информационной безопасности |

| | |
|---|--|
| <p>ПК-3.2: Уметь самостоятельно разрабатывать математические модели, на основе содержательного и физического описания процессов и объектов.</p> | <p>основные понятия информационной безопасности на основе содержательного и физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>криптографические методы обеспечения конфиденциальности, целостности и аутентичности информации на основе содержательного и</p> |
| | <p>физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>способы защиты от вредоносных программ на основе содержательного и физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>пользоваться основными понятиями информационной безопасности в сфере законодательства на основе содержательного и физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>использовать методы защиты информационных систем от несанкционированного доступа на основе содержательного и физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>использовать способы защиты программного обеспечения от несанкционированного использования на основе содержательного и физического описания процессов и объектов с учетом основных требований информационной безопасности.</p> <p>приемами по обеспечению защиты программного обеспечения от несанкционированного использования;</p> <p>технологиями криптографической защиты информации</p> <p>алгоритмами защиты от вредоносных программ;</p> |

| | |
|--|---|
| <p>ПК-3.3: Владеть основными понятиями и результатами основополагающих математических дисциплин;</p> | <p>основные понятия основополагающих математических дисциплин с учетом основных требований информационной безопасности и защиты информации</p> <p>основные понятия основополагающих математических дисциплин с учетом основных требований информационной безопасности для</p> |
| | <p>обеспечения антивирусной защиты</p> <p>основные понятия основополагающих математических дисциплин с учетом основных требований информационной безопасности для обеспечения защиты в сетях</p> <p>воспользоваться результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности и конфиденциальности</p> <p>воспользоваться результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности и целостности</p> <p>воспользоваться результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности и доступности</p> <p>Владеть основными понятиями и результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности по вопросам антивирусной защиты</p> <p>Владеть основными понятиями и результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности по вопросам защиты в сетях</p> <p>Владеть основными понятиями и результатами основополагающих математических дисциплин с учетом основных требований информационной безопасности по вопросам конфиденциальности, целостности и защиты</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=31738>.

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 | |

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 | | |
| 1. | | | | | | | | | | | |
| | | 1. Состав отечественного и международного законодательства в области обеспечения информационной безопасности | 2 | | | | | | | | |
| | | 2. Изучение законов РФ в сфере защиты информации. | | | 4 | | | | | | |
| | | 3. Работа с литературой | | | | | | | 5 | | |
| | | 4. Программная и аппаратная антивирусная защита информации | 2 | | | | | | | | |
| | | 5. Использование антивирусных пакетов | | | 4 | | | | | | |
| | | 6. Работа с литературой | | | | | | | 5 | | |
| | | 7. Принципы и средства защиты информации от несанкционированного доступа | 2 | | | | | | | | |
| | | 8. Защита информации в текстовом процессоре Microsoft Word. | | | 4 | | | | | | |
| | | 9. Работа с литературой | | | | | | | 5 | | |

| | | | | | | | | |
|---|---|--|---|--|--|--|---|--|
| 10. Обеспечение информационной безопасности в системах управления базами данных | 2 | | | | | | | |
| 11. Защита информации в программе Microsoft Office Excel. | | | 4 | | | | | |
| 12. Работа с литературой | | | | | | | 5 | |
| 13. Криптографическая защита информации | 2 | | | | | | | |
| 14. Защита информации в программе Microsoft Access. | | | 4 | | | | | |
| 15. Работа с литературой | | | | | | | 5 | |
| 16. Система обнаружения атак и вторжений | 1 | | | | | | | |
| 17. Алгоритмы шифрования | | | 3 | | | | | |
| 18. Работа с литературой | | | | | | | 5 | |
| 19. Классификация технических каналов утечки информации. Программно-аппаратные средства обнаружения ПЭМИ и наводок. | 2 | | | | | | | |
| 20. Создание проекта по компьютерной защите информации с использованием технических средств ЗИ. | | | 3 | | | | | |
| 21. Работа с литературой | | | | | | | 6 | |
| 22. Программно-аппаратные средства обнаружения утечки речевой и видеоинформации | 2 | | | | | | | |
| 23. Защита информации в среде программирования Matlab. | | | 3 | | | | | |
| 24. Работа с литературой | | | | | | | 6 | |
| 25. Облачные технологии | 1 | | | | | | | |
| 26. Использование облачных технологий и вопросы защиты информации | | | 3 | | | | | |
| 27. Работа с литературой | | | | | | | 6 | |

| | | | | | | | | |
|---|----|--|----|--|--|--|----|--|
| 28. Стеганография | 2 | | | | | | | |
| 29. Стеганографические методы защиты информации | | | 4 | | | | | |
| 30. Работа с литературой | | | | | | | 6 | |
| 31. | | | | | | | | |
| Всего | 18 | | 36 | | | | 54 | |

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.