

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

Б1.В.10 Основы информационной безопасности
телекоммуникационных систем

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль)

11.03.02 Инфокоммуникационные технологии и системы связи

Форма обучения

очная

Год набора

2023

Красноярск 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили _____

канд.техн.наук, доцент, Черников Дмитрий Юрьевич; Старший

преподаватель, Тарбазанов Кирилл Викторович

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Формирование у обучающихся базовых теоретических знаний в области информационной безопасности и развитие необходимых практических навыков их применения в будущей профессиональной деятельности.

1.2 Задачи изучения дисциплины

1. Ознакомление с теорией и практикой обеспечения информационной безопасности;
2. Изучение основных требований и рекомендаций по защите информации, составляющей государственную тайну и иную служебную информацию;
3. Формирование у обучающегося конкретных практических умений и навыков использования современных компьютерных средств и методов защиты данных.

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-10: Способен к администрированию процесса оценки производительности и контроля использования и производительности сетевых устройств, программного обеспечения информационно-коммуникационной системы | |
| ПК-10.1: Понимает протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем | основные направления обеспечения информационной безопасности основные угрозы информационной безопасности обосновывать выбор технических средств обеспечения информационной безопасности обосновывать меры обеспечения информационной безопасности в соответствии с законодательством РФ сформулировать комплекс мер по обеспечению информационной безопасности предприятия методикой определения видов и форм информации, подверженной угрозам анализом угрозы информационно-вычислительным системам |

| | |
|--|---|
| <p>ПК-10.2: Анализирует корреляции различных параметров при изменениях производительности</p> | <p>математический аппарат для решения профессиональных задач</p> <p>программные средства системного, прикладного и специального назначения</p> <p>применять соответствующий математический аппарат для решения профессиональных задач</p> <p>применять программные средства системного, прикладного и специального назначения</p> <p>способностью применять соответствующий</p> |
| | <p>математический аппарат для решения профессиональных задач</p> <p>способностью применять инструментальные средства, языки и системы программирования для решения профессиональных задач</p> <p>способностью применять инструментальные средства, языки и системы программирования для решения профессиональных задач</p> |
| <p>ПК-5: Способен оценивать параметры безопасности и защиты программного обеспечения и сетевых устройств администрируемой сети с помощью специальных средств управления безопасностью</p> | |
| <p>ПК-5.1: Понимает защищенные протоколы управления; основные средства криптографии</p> | <p>особенности применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных</p> <p>способы применения программных и программно-аппаратных средств защиты информации в компьютерных сетях, базах данных</p> <p>использования программных и программно-аппаратных средств для защиты информации в сети</p> <p>устанавливать и настраивать программные и программно-аппаратные средства защиты информации</p> <p>применять программные и программно-аппаратные средства защиты информации</p> <p>программными и программно-аппаратными средствами защиты информации</p> |

| | |
|--|---|
| <p>ПК-5.2: Применяет программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа</p> | <p>особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных типовые модели управления данных доступом, средств, методов и типовые модели управления протоколов идентификации и доступом, средств, методов и аутентификации</p> <p>протоколы идентификации применять программные аутентификации; программно-аппаратные средства основные понятия криптографии для защиты информации в базах типовых криптографических данных применять методы и средства защиты, проверять</p> |
| | <p>выполнение требований информации по защите информации применять программные и несанкционированного доступа при программно-аппаратные средства аттестации объектов для защиты информации в базах информатизации по требованиям данных безопасности информации; проверять выполнение требований навыками решения задач по защите информации от защиты от НСД к информации несанкционированного доступа ограниченного доступа с помощью при аттестации объектов программных и программно-информатизации по требованиям аппаратных средств защиты безопасности информации</p> <p>приемами математического аппарата для выполнения криптографических преобразований навыками решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации</p> |

| | |
|---|--|
| <p>ПК-5.3: Оценивает безопасность и защиту приложений от несанкционированного доступа</p> | <p>особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации основные понятия криптографии и типовых криптографических методов и средств защиты информации</p> <p>применять программные и программно-аппаратные средства для защиты информации в базах данных проверять выполнение требований по защите</p> |
| | <p>информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации</p> <p>применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись навыками решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации</p> <p>навыками применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных</p> |

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

| Вид учебной работы | Всего, зачетных единиц (акад.час) | е |
|--|--|---|
| | | 1 |
| Контактная работа с преподавателем: | 1 (36) | |
| практические занятия | 1 (36) | |
| Самостоятельная работа обучающихся: | 1 (36) | |
| курсовое проектирование (КП) | Нет | |
| курсовая работа (КР) | Нет | |

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

| | | Контактная работа, ак. час. | | | | | | | |
|--|--|--------------------------------|--------------------------|---|--------------------------|--|--------------------------|-------------------------------------|--------------------------|
| № п/п | Модули, темы (разделы) дисциплины | 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. Основы информационной безопасности телекоммуникационных систем | | | | | | | | | |
| | 1. Понятийный аппарат и основы терминологии информационной и национальной безопасности | | | 4 | | | | | |
| | 2. Виды национальной безопасности и их краткая характеристика | | | 4 | | | | | |
| | 3. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация | | | 4 | | | | | |
| | 4. Информационная война как высшая форма угрозы информационной безопасности | | | 4 | | | | | |
| | 5. Национальные интересы личности, общества и государства в информационной сфере | | | 4 | | | | | |
| | 6. Государственные органы обеспечения информационной безопасности | | | 4 | | | | | |

| | | | | | | | | |
|--|--|--|----|--|--|--|----|--|
| 7. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства | | | 4 | | | | | |
| 8. Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности | | | 4 | | | | | |
| 9. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения | | | 4 | | | | | |
| 10. Основы информационной безопасности телекоммуникационных систем | | | | | | | 36 | |
| Всего | | | 36 | | | | 36 | |

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Култыгин О.П. Администрирование баз данных. СУБД MS SQL Server: учебное пособие(Москва: МФПА).
2. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие(Москва: Форум).
3. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов по направлению 552800 "Информатика и вычислительная техника" и по специальностям 220100 "Вычислительные машины, комплексы, системы и сети", 220200 "Автоматизированные системы обработки информации и управления" и 220400 "Программное обеспечение вычислительной техники и автоматизированных систем".(Москва: Питер).
4. Гаипов К. Э., Турбов А. Ю. Технологии локальных инфокоммуникационных сетей: учеб.-метод. пособие для лаб. и самостоят. работ [для студентов напр. 210400.62 «Телекоммуникации» и спец. «210406.65» «Сети связи и системы коммутации»](Красноярск: СФУ).
5. Тоискин В. С., Жук А. П. Системы документальной электросвязи: Учебное пособие(Москва: Издательский Центр РИО□).

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. Операционная система Windows XP, Windows 7.
2. Прикладное программное обеспечение: Microsoft Office, утилиты, оболочки, сервисные программы.
3. Антивирусное программное обеспечение Касперский антивирус.

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

1. Справочные правовые системы «Консультант Плюс», Гарант, Кодекс

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)

Мультимедийный проектор с экраном для презентаций.

Класс персональных компьютеров, объединенных в локальную сеть.

Доступ к сети Интернет.

Комплект учебно-методической, научной и справочной литературы по дисциплине.

Читальный зал с возможностью оперативного доступа к сети ИНТЕРНЕТ.