Подписан: Шебзухова Татьяна Александровна
Дата: 2021-08-31 20:06:01
Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского федерального университета
Дата подписания: 05.09.2023 13:38:03
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1c8ef96f

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиала) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20___ г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ

ПМ.02 ПРИМЕНЕНИЕ МИКРОПРОЦЕССОРНЫХ СИСТЕМ, УСТАНОВКА И НАСТРОЙКА ПЕРИФЕРИЙНОГО ОБОРУДОВАНИЯ

МДК.02.03 ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)
Специальность СПО 09.02.01 Компьютерные системы и комплексы
Форма обучения очная
Учебный план 2021 года

РАССМОТРЕНО:
Предметно-цикловой комиссией
Протокол №___ от «___» _____
Председатель ПЦК
_____М.А. Крюкова

РАЗРАБОТАНО:
преподаватель
_____ А.А. Хаджиев
«__» _____ 20__г.

СОГЛАСОВАНО:
Учебно-методической комиссией
Протокол №___ от «___» _____
Председатель УМК института
_____ А.Б. Нарыжная
Зам. генерального директора ООО «Миллениум-Сервис»

_____А.А. Давыдов

Пятигорск, 2021г.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиала) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПМ.02 ПРИМЕНЕНИЕ МИКРОПРОЦЕССОРНЫХ СИСТЕМ, УСТАНОВКА И НАСТРОЙКА ПЕРИФЕРИЙНОГО ОБОРУДОВАНИЯ

МДК.02.03 ПЕРСОНАЛЬНАЯ КИБЕРБЕЗОПАСНОСТЬ

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)
Специальность СПО 09.02.01 Компьютерные системы и комплексы
Форма обучения очная
Учебный план 2021 года

РАССМОТРЕНО:
Предметно-цикловой комиссией
Протокол №___ от «___» _____
Председатель ПЦК
_____М.А. Крюкова

РАЗРАБОТАНО:
Преподаватель
_____ А.А. Хаджиев
«__» _____ 20__г.

СОГЛАСОВАНО:
Учебно-методической комиссией
Протокол №___ от «___» _____
Председатель УМК института
_____ А.Б. Нарыжная
Зам. генерального директора ООО «Миллениум-Сервис»

_____А.А. Давыдов

Пятигорск, 2021г.

1. ПАСПОРТ ПРОГРАММЫ

ПМ.02 Применение микропроцессорных систем, установка и настройка периферийного оборудования
МДК.02.03 Персональная кибербезопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины МДК.02.03 Персональная кибербезопасность является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы.

1.2. Место учебной дисциплины в структуре образовательной программы:

Дисциплина МДК.02.03 Персональная кибербезопасность относится к профессиональному модулю ПМ.02 Применение микропроцессорных систем, установка и настройка периферийного оборудования, изучается в 5 семестре.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате освоения учебной дисциплины обучающийся должен **знать**:

- базовую функциональную схему МПС;
- программное обеспечение микропроцессорных систем;
- структуру типовой системы управления (контроллер) и организацию микроконтроллерных систем;
- методы тестирования и способы отладки МПС;
- информационное взаимодействие различных устройств через информационно-телекоммуникационную сеть "Интернет" (далее - сеть Интернет);
- состояние производства и использование МПС;
- способы конфигурирования и установки персональных компьютеров, программную поддержку их работы;
- классификацию, общие принципы построения и физические основы работы периферийных устройств;
- способы подключения стандартных и нестандартных программных утилит;
- причины неисправностей и возможных сбоев;

В результате освоения учебной дисциплины обучающийся должен **уметь**:

- составлять программы на языке ассемблера для микропроцессорных систем;
- производить тестирование и отладку микропроцессорных систем (далее - МПС);
- выбирать микроконтроллер/микропроцессор для конкретной системы управления;
- осуществлять установку и конфигурирование персональных компьютеров, и подключение периферийных устройств;
- подготавливать компьютерную систему к работе;
- проводить инсталляцию и настройку компьютерных систем;
- выявлять причины неисправностей и сбоев, принимать меры по их устранению;

В результате освоения учебной дисциплины обучающийся должен **иметь практический опыт**:

- создания программ на языке ассемблера для микропроцессорных систем;
- тестирования и отладки микропроцессорных систем;
- применения микропроцессорных систем;
- установки и конфигурирования микропроцессорных систем и подключения периферийных устройств;
- выявления и устранения причин неисправностей и сбоев периферийного оборудования.

1.4. Перечень формируемых компетенций

В результате освоения учебной дисциплины студент должен овладевать следующими компетенциями:

Общими компетенциями:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Профессиональными компетенциями:

ПК 2.1. Создавать программы на языке ассемблера для микропроцессорных систем.

ПК 2.2. Производить тестирование, определение параметров и отладку микропроцессорных систем.

ПК 2.3. Осуществлять установку и конфигурирование персональных компьютеров, и подключение периферийных устройств.

ПК 2.4. Выявлять причины неисправности периферийного оборудования.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет:

64 академических часа, из них:

44 академических часа – аудиторные занятия, из них:

22 – аудиторных часа – лекционные занятия;

22 – аудиторных часа – практические занятия;

20 академических часов – самостоятельная работа.

2.1. Учебно-тематический план учебной дисциплины

№ п/п	**Наименование разделов, тем учебной дисциплины**	**Семестр**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость** *в часах*				**Формы текущего контроля успеваемости** *(по разделам дисциплины)* **Форма промежуточной аттестации** *(по семестрам)*
			Лекции	Лабораторные занятия	Практические занятия	СРС	

1.	**Тема 1.** Основные понятия персональной кибербезопасности. Информационная безопасность и кибербезопасность.	5	2	-	2		
2.	**Тема 2.** Причины киберпреступлений. Проблемы кибербезопасности.	5	2	-	2	2	**Реферат**
3.	**Тема 3.** Основные понятия и определения криптографии.	5	2	-	2		
4.	**Тема 4.** Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.	5	2	-	2	2	**Реферат**
5.	**Тема 5.** Алгоритмы шифрования с секретным ключом (симметричные). Алгоритмы шифрования с открытым ключом (асимметричные).	5	2	-	2	4	**Реферат**
6.	**Тема 6.** Методы криптоанализа. Обзор современных методов криптоанализа. Требования, предъявляемые к современным блочным алгоритмам шифрования.	5	2	-	2		
7.	**Тема 7.** Классификация вирусов. Антивирусная защита персональных компьютеров.	5	2	-	2	4	**Реферат**
8.	**Тема 8.** Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств защиты информации.	5	2	-	2		
9.	**Тема 9.** Современные методы защищенной аутентификации.	5	2	-	2		
10.	**Тема 10.** Идентификация, аутентификация и авторизация.	5	2	-	2	4	**Реферат**
11.	**Тема 11.** Электронная цифровая подпись. Виды электронной цифровой подписи.	5	2	-	2	4	**Реферат**
	ИТОГО:		**22**	**-**	**22**	**20**	**Диф. зачет**

2.2. Наименование и краткое содержание лекций

№	Наименование разделов и тем учебной дисциплины, их краткое содержание	Использование активных и интерактивных форм	Часы
5 семестр			
1.	**Тема 1. Основные понятия персональной кибербезопасности. Информационная безопасность и кибербезопасность.** Составляющие информационной безопасности.	*Лекция беседа*	2
2.	**Тема 2. Причины киберпреступлений. Проблемы кибербезопасности.** Социальные, экономические и правовые причины	*Проблемная лекция*	2

	киберпреступлений.		
3.	**Тема 3. Основные понятия и определения криптографии.** Криптография, криптоанализ, криптостойкость, криптология.		2
4.	**Тема 4. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.** Требования к системам защиты информации. Виды атак.		2
5.	**Тема 5. Алгоритмы шифрования с секретным ключом (симметричные). Алгоритмы шифрования с открытым ключом (асимметричные).** Виды шифрования. Симметричное и ассиметричное.		2
6.	**Тема 6. Методы криптоанализа. Обзор современных методов криптоанализа. Требования, предъявляемые к современным блочным алгоритмам шифрования.** Криптоанализ симметричных и ассиметричных шифров. Частотный анализ. Атака по ключам.		2
7.	**Тема 7. Классификация вирусов. Антивирусная защита персональных компьютеров.** Компьютерные вирусы. Виды вирусов.	*Лекция беседа*	2
8.	**Тема 8. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств защиты информации.** Firewall. Аппаратная защита информации. Защита от НСД.	*Проблемная лекция*	2
9.	**Тема 9. Современные методы защищенной аутентификации.** Методы аутентификации. Дактилоскопия. Биометрическая аутентификация. Защита биометрических данных.	*Лекция с разбором конкретных ситуаций*	2
10.	**Тема 10. Идентификация, аутентификация и авторизация.** Основные понятия идентификации. Многофакторная аутентификация.		2
11.	**Тема 11. Электронная цифровая подпись. Виды электронной цифровой подписи.** Электронные подписи, их виды и назначение.		2
	Итого		**22**

2.3. Наименование и краткое содержание лабораторных занятий

Данный вид работы не предусмотрен учебным планом.

2.4. Наименование и краткое содержание практических (семинарских) занятий

№	Наименование разделов и тем дисциплины, их краткое содержание	Использование интерактивных форм	Часы
	5 семестр		
1.	**Тема 1. Основные понятия персональной кибербезопасности. Информационная безопасность и кибербезопасность.** Практическое занятие №1. Шифры перестановки.		2
2.	**Тема 2. Причины киберпреступлений. Проблемы кибербезопасности.**		2

	Практическое занятие №2. Шифры замены.		
3.	**Тема 3. Основные понятия и определения криптографии.** Практическое занятие №3. Комбинированные шифры.		2
4.	**Тема 4. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.** Практическое занятие №4. Шифрование с открытым ключом.		2
5.	**Тема 5. Алгоритмы шифрования с секретным ключом (симметричные). Алгоритмы шифрования с открытым ключом (асимметричные).** Практическое занятие №5. Хеш-функция (MD5).		2
6.	**Тема 6. Методы криптоанализа. Обзор современных методов криптоанализа. Требования, предъявляемые к современным блочным алгоритмам шифрования.** Практическое занятие №6. Идентификация и аутентификация.		2
7.	**Тема 7. Классификация вирусов. Антивирусная защита персональных компьютеров.** Практическое занятие №7. Электронная цифровая подпись (RSA, ГОСТы 34.10-94 и 34.10-2001).		2
8.	**Тема 8. Брандмауэры. Средства аппаратной защиты информации. Организация программно-аппаратных средств защиты информации.** Практическое занятие №8. Контроль целостности (биты четности, контрольные цифры).		2
9.	**Тема 9. Современные методы защищенной аутентификации.** Практическое занятие №9. Тайные многосторонние вычисления и разделение секрета.		2
10.	**Тема 10. Идентификация, аутентификация и авторизация.** Практическое занятие №10. Представление чисел в двоичном виде.		2
11.	**Тема 11. Электронная цифровая подпись. Виды электронной цифровой подписи.** Практическое занятие №11. Стеганография.		2
	Итого		**22**

2.5. Виды и содержание самостоятельной работы студента; формы контроля

№	Наименование разделов и тем дисциплины, их краткое содержание	Использование интерактивных форм	Часы
	5 семестр		
1.	**Тема 2. Причины киберпреступлений. Проблемы кибербезопасности.** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Современные методы киберпреступлений. Методы противодействия киберпреступникам. Защита своих данных и денежных средств от киберпреступлений.	*Реферат*	2

2.	**Тема 4. Требования к криптографическим системам защиты информации. Реализация криптографических методов. Криптографические атаки.** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Виды алгоритмов шифрования данных. Криптографические методы шифрования и дешифрования информации.	*Реферат*	2
3.	**Тема 5. Алгоритмы шифрования с секретным ключом (симметричные). Алгоритмы шифрования с открытым ключом (асимметричные).** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Способы защиты информации методами криптографии. Передача секретной информации с помощью шифрования. Процесс передачи и получения зашифрованной информации. Методы расшифрования секретных данных.	*Реферат*	4
4.	**Тема 7. Классификация вирусов. Антивирусная защита персональных компьютеров.** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Виды компьютерных вирусов. Современные компьютерные вирусы. Антивирусные программы, их назначение и виды. Сравнение антивирусных программ по их характеристикам. Защита компьютера от вирусов встроенными средствами операционной системы.	*Реферат*	4
5.	**Тема 10. Идентификация, аутентификация и авторизация.** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Способы защиты баз данных, имеющих парольный доступ. Проверка пользователя при входе в систему государственных услуг. Защита данных пользователей портала государственных услуг.	*Реферат*	4
6.	**Тема 11. Электронная цифровая подпись. Виды электронной цифровой подписи.** *Вид самостоятельной работы:* Работа с литературой по теме занятия. Реферат на тему: Виды электронных цифровых подписей. Подписание документов с помощью цифровой подписи. Защита документов от изменения или искажения цифровой подписью.	*Реферат*	4
	Итого		**20**

3. ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр – Диф. зачет;

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Рекомендуемая литература

4.1.1. Основная литература:

1. Ермакова, А. Ю. Методы и средства защиты компьютерной информации: учебное пособие / А. Ю. Ермакова. — Москва: РТУ МИРЭА, 2020. — 223 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844

2. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учебное пособие / С. Н. Никифоров. — 3-е изд., стер. — Санкт-Петербург: Лань, 2020. — 124 с. — ISBN 978-5-8114-6352-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/146885

3. Никифоров, С. Н. Методы защиты информации. Шифрование данных: учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

4.1.2. Дополнительная литература:

1. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург: Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924

2. Тумбинская, М. В. Защита информации на предприятии: учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург: Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184

3. Фот, Ю. Д. Методы защиты информации: учебное пособие / Ю. Д. Фот. — Оренбург: ОГУ, 2019. — 230 с. — ISBN 978-5-7410-2296-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/159977

4.1.3. Методическая литература:

Методические указания для практических занятий.
Методические указания для самостоятельной работы.

4.1.4. Интернет-ресурсы:

- http://www.edu.ru/index.php?page_id=6 Федеральный портал Российское образование.
- http://informic.narod.ru/info.html Сайт преподавателя Информатики.
- http://www.stavminobr.ru Министерство образования ставропольского края.

4.2. Программное обеспечение:

Операционная система Microsoft Windows Профессиональная, Microsoft Office Standard 2013.

4.3. Материально-техническое обеспечение дисциплины

- Комплект учебной мебели (преподавательские стол, стул; столы и стулья для обучающихся)

Мультимедийное оборудование:

- Персональные компьютеры (12 шт.) в составе i3 2100/4096MB/500Gb/DVDRW/500W,
- Доска магнитно-маркерная 1-элементная 120x240,

- Короткофокусный мультимедиапроектор Epsc EB-436Wi с настенным креплением и набором кабелей.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, а также выполнения обучающимися рефератов.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**	**Перечень подтверждаемых компетенций**
знать: • базовую функциональную схему МПС; • программное обеспечение микропроцессорных систем; • структуру типовой системы управления (контроллер) и организацию микроконтроллерных систем; • методы тестирования и способы отладки МПС; • информационное взаимодействие различных устройств через информационно-телекоммуникационную сеть "Интернет" (далее - сеть Интернет); • состояние производства и использование МПС; • способы конфигурирования и установки персональных компьютеров, программную поддержку их работы; • классификацию, общие принципы построения и физические основы работы периферийных устройств; • способы подключения стандартных и нестандартных программных утилит; • причины неисправностей и возможных сбоев; **уметь**: • составлять программы на языке ассемблера для микропроцессорных систем; • производить тестирование и отладку микропроцессорных систем (далее - МПС); • выбирать микроконтроллер/микропроцессор для конкретной системы управления; • осуществлять установку и конфигурирование персональных компьютеров, и подключение периферийных устройств; • подготавливать компьютерную систему к работе;	Реферат	ОК 1-9 ПК 2.1-2.4

• проводить инсталляцию и настройку компьютерных систем; • выявлять причины неисправностей и сбоев, принимать меры по их устранению; **иметь практический опыт**: • создания программ на языке ассемблера для микропроцессорных систем; • тестирования и отладки микропроцессорных систем; • применения микропроцессорных систем; • установки и конфигурирования микропроцессорных систем и подключения периферийных устройств; • выявления и устранения причин неисправностей и сбоев периферийного оборудования.		