

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Колледж радиоэлектроники имени П.Н. Яблочкова



Рабочая программа учебной дисциплины

Информационная безопасность

09.02.07 Информационные системы и программирование


Профиль подготовки
технологический

Квалификация выпускника
программист

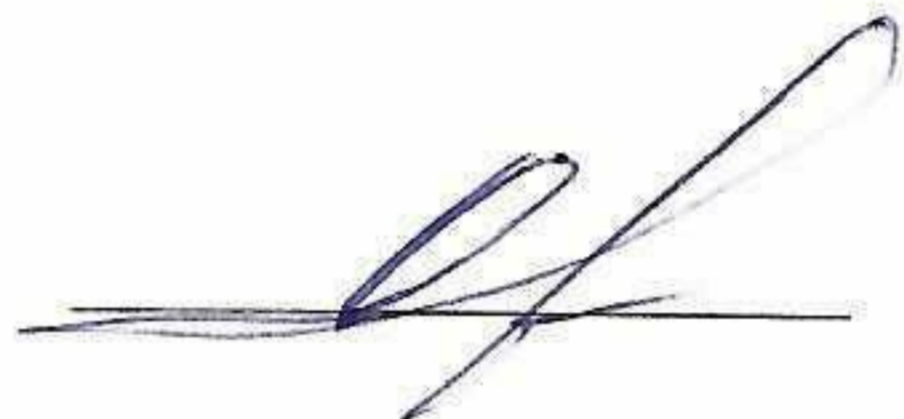
Форма обучения
очная

Саратов
2025

Разработчик: преподаватель А.Ю. Будюков 
Программа одобрена на заседании ЦК информационных систем и программирования
от 06.03.2025 протокол № 11

Председатель ЦК информационных систем и программирования
 Е.В. Гожий

Директор
Колледжа радиоэлектроники
имени П. Н. Яблочкова

 О. В. Бреус

Зам. директора по УР

 Н. Н. Чернова

Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование Приказ Министерства образования и науки РФ от 9 декабря 2016 г. № 1547 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование» (Зарегистрировано в Минюсте РФ 26 декабря 2016 г., регистрационный № 44936)).

Организация-разработчик: ФГБОУ ВО «СГУ имени Н.Г. Чернышевского» Колледж радиоэлектроники имени П.Н. Яблочкова

Разработчик: Будюков А. Ю. - преподаватель Колледжа радиоэлектроники имени П. Н. Яблочкова.

СОДЕРЖАНИЕ

	стр.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	8
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	10

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена: учебная дисциплина относится к общепрофессиональному циклу.

1.3. Цель и планируемые результаты освоения дисциплины:

В результате освоения учебной дисциплины обучающийся должен уметь:

— применять правовые, организационные, технические и программные средства защиты информации;

— создавать программные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен знать:

— источники возникновения информационных угроз;

— модели и принципы защиты информации от несанкционированного доступа;

— методы антивирусной защиты информации;

— состав и методы организационно-правовой защиты информации.

ПК и ОК, которые актуализируются при изучении учебной дисциплины:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ПК 1.1. Формировать алгоритмы разработки программных модулей в соответствии с техническим заданием.

ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

1.4 Количество часов на освоение программы дисциплины:

учебной нагрузки обучающегося 54 часа,

в том числе:

учебной нагрузки обучающегося во взаимодействии с преподавателем 40 часов;

практической подготовки 10 часов;

самостоятельной учебной работы обучающегося 8 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объём в часах
Учебной нагрузки обучающегося (всего)	54
Учебная нагрузка во взаимодействии с преподавателем (всего)	40
в том числе:	
теоретическое обучение	26
практические занятия	12
в том числе практическая подготовка	10
консультации	2
Самостоятельная учебная работа обучающегося (всего)	8
в том числе:	
работа с информационными источниками	2
подготовка презентационных материалов	2
подготовка к экзамену	4
Экзамен	6
Промежуточная аттестация в форме экзамена	

2.2 Тематический план и содержание учебной дисциплины Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект).	Объем часов	Уровень освоения
Введение	Роль дисциплины в становлении специалистов. Взаимосвязь дисциплин	2	
Раздел 1 Информационная безопасность. Общие понятия и определения		4	
Тема 1.1 Информационная безопасность. Общие понятия и определения	Содержание	2	
	Актуальность информационной безопасности. Свойства информации, влияющие на информационную безопасность	2	1
Тема 1.2 Компьютерные преступления	Содержание	2	
	Классификация компьютерных преступлений и способы их совершения. Причины уязвимости сети интернет	4	1
Раздел 2 Вредоносные программы и защита от компьютерных вирусов		8	
Тема 2.1. Классификация компьютерных вирусов	Содержание	2	
	Условия существования вирусов. Классификация компьютерных вирусов. Классические компьютерные вирусы. Компьютерные черви и троянские программы	2	1
Тема 2.2 Защита от компьютерных вирусов	Лабораторные занятия	6	
	Лабораторная работа №1 (Практическая подготовка) Макровирусы и борьба с ними в MS Office	6	
	Лабораторная работа №2 (Практическая подготовка)Профилактика проникновения «Троянских программ» Лабораторная работа №3 Антивирус Касперского. Настройка и поиск вирусов		
Раздел 3 Методы и средства защиты компьютерной информации		4	
Тема 3.1. Защита информации. Основные принципы	Содержание	2	
	Понятие защиты информации. Основные принципы защиты информации	2	1
Тема 3.2. Методы и средства защиты информации	Содержание	2	1
	Методы и средства защиты информации. Разграничение прав пользователей. Регистрация всех обращений к информации, защита от копирования	2	
Раздел 4 Криптографические методы защиты информации		18	
Тема 4.1. Основные этапы развития криптологии	Содержание	2	
	Криптология и основные этапы ее развития	2	1
Тема 4.2. Классификация методов	Содержание	6	

криптографического закрытия информации	Шифрование заменой. Криптоанализ. Основные понятия. Шифрование методом перестановки и гаммированием. Шифрование с помощью аналитических преобразований	2	1
	Лабораторные занятия	4	2
	Лабораторная работа №5 (Практическая подготовка) Шифрование методом замены Лабораторная работа №6 (Практическая подготовка) Криптоанализ по оценке частотности символов Лабораторная работа №7 (Практическая подготовка) Шифрование методом перестановки Лабораторная работа №8 (Практическая подготовка) Шифрование методом гаммирования		
Тема 4.3. Системы с открытым ключом	Содержание	6	
	Принцип работы систем с открытым ключом. Криптографические стандарты DES и ГОСТ 28147-89. Алгоритм RSA	4	1
	Лабораторные занятия	2	2
Лабораторная работа №9 (Практическая подготовка) Шифрование с открытым ключом. Алгоритм RSA			
Тема 4.4 Проблемы реализации и характеристики криптографических средств защиты	Содержание	4	
	Оценка криптостойкости шифров. Техничко-экономические показатели криптографических методов защиты информации	4	1
Раздел 5 Правовое обеспечение информационной безопасности		6	
Тема 5.1. Правовое обеспечение информационной безопасности	Содержание	6	
	Законодательство в области защиты информации. Основные законы, защищающие целостность информации. Мировая практика в области защиты информации	2	1
	Самостоятельная работа	4	3
	Тематика самостоятельной работы: работа с информационными источниками по темам: «Выбор средств защиты для собственной программы», «Программно-аппаратная реализация средств защиты»		
Промежуточная аттестация		12	
в том числе			
консультация к экзамену		2	
самостоятельная работа (подготовка к экзамену)		4	
экзамен		6	
Всего:		54	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1- ознакомительный (узнавание ранее изученных объектов, свойств);

2- репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3- продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Реализация рабочей программы предусматривает возможность использования различных образовательных технологий, в том числе дистанционного обучения.

При реализации рабочей программы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья (далее – ОВЗ) предусмотрено информационное обеспечение обучения, включающее предоставление учебных материалов в различных формах.

В рамках освоения рабочей программы осуществляется практическая подготовка обучающихся.

Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций.

Практическая подготовка осуществляется в колледже и в следующих структурах СГУ:

- УЦИТ СГУ имени Н.Г. Чернышевского,
- а также на приведенных ниже предприятиях и в организациях:
- АО «НПП «Контакт»;
- АО «КБПА»;
- АО «САЗ»;
- АО «НПП «Алмаз»;
- АО «Транспортное машиностроение»;
- ПАО «СЭЗ имени Серго Орджоникидзе»;
- ООО «СЭПО-ЗЭМ»;
- ООО «Источник»;
- ООО «Роберт Бош Саратов»;
- ООО «НПФ «Вымпел»;
- ООО «Геофизмаш»;
- ООО «КАРСАР»;
- ООО «Бош Пауэр Тулз»;
- АО «Саратовский полиграфический комбинат»;
- ООО Энгельское приборостроительное объединение «Сигнал»;
- АО Энгельское опытно-конструкторское бюро «Сигнал» им. А.И. Глухарева;
- ЗАО «СПГЭС»;
- ООО Завод «Саратовгазавтоматика»;
- АО «КБ «Электроприбор»;
- Саратовское отделение ООО внедренческая фирма «ЭЛНА»;
- ООО «ИНТЕРКАРА».

3.1 Материально-техническое обеспечение

Реализация программы дисциплины требует наличия лаборатории информационных ресурсов

Технические средства обучения:

- интерактивная доска с мультимедийным проектором,
- персональный компьютер для преподавателя,
- несколько рабочих станций для проверки знаний студентов.

Оборудование лаборатории и рабочих мест лаборатории: компьютерные рабочие станции для работы студентов.

3.2 Информационное обеспечение обучения

Перечень учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

- 1 **Шаньгин, В. Ф.** Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. – Москва : ФОРУМ : ИНФРА-М, 2024. – 416 с. – (Среднее профессиональное образование). – Текст : электронный. – URL: <https://znanium.com/catalog/product/2130242> (дата обращения: 18.03.2025). – Режим доступа: по подписке.
- 2 **Мельников, В. П.** Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов ; под редакцией В. П. Мельникова. – Москва : КноРус, 2021. – 267 с. – (Среднее профессиональное образование). – Текст : электронный. – URL: <https://book.ru/book/939292> (дата обращения: 18.03.2025). – Режим доступа: для авторизир. пользователей.
- 3 **Партыка, Т. Л.** Информационная безопасность : учебное пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. – Москва : ФОРУМ : ИНФРА-М, 2021. – 432 с. – (Среднее профессиональное образование). – Текст : электронный. – URL: <https://znanium.com/catalog/product/1189328> (дата обращения: 18.03.2025). – Режим доступа: по подписке.

Дополнительные источники:

- 1 **Шаньгин, В. Ф.** Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – 2-е изд. – Саратов : Профобразование, 2019. – 543 с. – Текст : электронный. – URL: <https://www.iprbookshop.ru/87992.html> (дата обращения: 18.03.2025). – Режим доступа: для авторизир. пользователей.
- 2 **Сычев, Ю. Н.** Основы информационной безопасности : учебно-методический комплекс / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2012. – 342 с. – Текст : электронный. – URL: <https://www.iprbookshop.ru/14642.html> (дата обращения: 18.03.2025). – Режим доступа: для авторизир. пользователей.
- 3 **Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мецераков, А. А. Шелупанов.** – Москва : Горячая линия-Телеком, 2011. – 558 с. : ил. – Текст : электронный. – URL: <https://znanium.com/catalog/product/405159> (дата обращения: 18.03.2025). – Режим доступа: по подписке.

Моло

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе устных и письменных опросов обучающихся, решения задач, в процессе проведения лабораторных занятий, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Формы и методы контроля и оценки результатов обучения адаптированы для обучающихся инвалидов и лиц с ОВЗ с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости предусмотрено для них увеличение времени на подготовку к зачетам и экзаменам, а также предоставление дополнительного времени для подготовки ответа на зачете/экзамене и проведение аттестации в несколько этапов.

Результаты обучения (освоенные умения, усвоенные знания)	Основные показатели оценки результата
<p>Перечень умений, осваиваемых в рамках дисциплины:</p> <ul style="list-style-type: none"> — применять правовые, организационные, технические и программные средства защиты информации; — создавать программные средства защиты информации. <p>Перечень знаний, осваиваемых в рамках дисциплины:</p> <ul style="list-style-type: none"> — источники возникновения информационных угроз; — модели и принципы защиты информации от несанкционированного доступа; — методы антивирусной защиты информации; — состав и методы организационно-правовой защиты информации. 	<ul style="list-style-type: none"> - понимание правовых, организационных, технических и программных средств защиты информации, программных средств защиты информации; - анализ источников возникновения информационных угроз; - оценка модели и принципов защиты информации от несанкционированного доступа, методов антивирусной защиты информации; - анализ состава и методов организационно-правовой защиты информации. - владение методиками кодирования информации; - анализ криптостойкости алгоритмов шифрования.