

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
РОСТОВСКОЙ ОБЛАСТИ «САЛЬСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»
(ГБПОУ РО «СИТ»)

УТВЕРЖДАЮ:

Заместитель директора по учебной работе


_____ Т.В. Якимова

« 01 » июля 2025 г.

Номер регистрации РП 09.02.01 ОП.13

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

**ОП.13ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
В КОМПЬЮТЕРНЫХ СИСТЕМАХ**

(базовый уровень)

профиль обучения: технологический

для специальности 09.02.01 Компьютерные системы и комплексы

г. Сальск
2025

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СИСТЕМАХ»

1.1 Место дисциплины в структуре основной образовательной программы:

Рабочая программа учебной дисциплины является частью ППССЗ в соответствии с ФГОС по специальности (специальностям) СПО 09.02.01 Компьютерные системы и комплексы. Особое значение дисциплина имеет при формировании и развитии ОК 01, ОК 02, ОК 09.

Дисциплина «Информационная безопасность в компьютерных системах» является общепрофессиональной и входит в общепрофессиональный учебный цикл.

Рабочая программа учебной дисциплины «Информационная безопасность в компьютерных системах» может быть использована в дополнительном профессиональном образовании в программах повышения квалификации и переподготовки работников в области информационных технологий.

Дисциплина «Информационная безопасность в компьютерных системах» реализуется частично в форме практической подготовки при освоении практических занятий. Дисциплина добавлена из часов вариативной части.

1.2. Цель и планируемые результаты освоения дисциплины:

1.2.1 Студент, освоивший программу дисциплины «Информационная безопасность в компьютерных системах» обязан освоить общие и профессиональные компетенции:

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 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.5. Выполнять установку и обновление версий управляющих программ (с учетом миграции – при необходимости).

1.2.2. В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ПК, ОК, ЛР	Умения	Знания
ОК 01. ОК 02. ОК 09. ПК 2.5.	<p><u>Уметь:</u></p> <ul style="list-style-type: none"> – Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – Применять основные правила и документы системы сертификации Российской Федерации; – Классифицировать основные угрозы безопасности информации; – Соблюдать процедуру 	<p><u>Знать:</u></p> <ul style="list-style-type: none"> – Сущность и понятие информационной безопасности, характеристику ее составляющих; – Место информационной безопасности в системе национальной безопасности страны; – Источники угроз информационной безопасности и меры по их предотвращению; – Жизненные циклы конфиденциальной информации в

	<p>установки прикладного программного обеспечения в соответствии с требованиями организации-производителя;</p> <p>– Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки.</p>	<p>процессе ее создания, обработки, передачи;</p> <p>– Современные средства и способы обеспечения информационной безопасности.</p> <p>– Лицензионные требования по настройке устанавливаемого программного обеспечения;</p> <p>– Типовые причины инцидентов, возникающих при установке программного обеспечения;</p> <p>– Основы архитектуры, устройства и функционирования вычислительных систем;</p> <p>– Принципы организации, состав и схемы работы операционных систем;</p> <p>– Стандарты информационного взаимодействия систем.</p>
--	---	--

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

Всего - 84 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 84 часа, в том числе в форме практической подготовки - 22 часа, консультации- 2 часа.

Промежуточная аттестация *в форме* экзамена – 8 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	84
в т.ч. в форме практической подготовки	22
в т. ч.:	
теоретическое обучение	52
практические работы	22
<i>Самостоятельная работа</i>	
Консультации	2
Промежуточная аттестация в форме экзамена	8

2.2. Тематический план и содержание учебной дисциплины ОП.13. Информационная безопасность в компьютерных системах

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов	В форме практической подготовки	Коды компетенций, формированию которых способствует элемент программы
1	2	3		4
Раздел 1 Информационная безопасность Российской Федерации		20	6	
Тема 1.1 Информационная безопасность как состояние защищенности национальных интересов в информационной сфере	Содержание учебного материала	8	2	ОК 01. ОК 02. ОК 09. ПК 2.5.
	1 Основные понятия в области информационной безопасности и их взаимосвязь	2		
	2 Деятельность государства по обеспечению информационной безопасности Российской Федерации	2		
	3 Цели и принципы государственной информационной политики Российской Федерации	2		
	Практические занятия	2	2	
	Практическая работа №1 Обоснование применения норм уголовного права в конкретных ситуациях, связанных с созданием и использованием вредоносного программного обеспечения	2	2	
Тема 1.2 Угрозы информационной безопасности Российской Федерации	Содержание учебного материала	6	2	
	1 Виды и источники угроз информационной безопасности Российской Федерации	2		
	2. Состояние информационной безопасности в различных сферах жизнедеятельности общества и государства.	2		
	Практические занятия	2	2	
	Практическая работа №2 Выявление угроз информационной безопасности в конкретных ситуациях	2	2	
Тема 1.3 Защита информации как один из видов деятельности	Содержание учебного материала	6	2	
	1 Защита информации, ее составляющие и виды	2		
	2 Цели и направления защиты информации	2		
	Практические занятия	2	2	
	Практическая работа №3 Выполнение проверки компьютера на	2	2	

		наличие признаков заражения вредоносным программным обеспечением			
Раздел 2 Безопасность компьютерных систем			54	16	
Тема 2.1. Основные понятия и принципы сетевой безопасности	Содержание учебного материала		8	2	ОК 01. ОК 02. ОК 09. ПК 2.5.
	1.	Информационная система как система контролируемого доступа к ресурсам	2		
	2.	Типы и примеры сетевых атак	2		
	3.	Анализ уязвимостей и угроз информационной безопасности	2		
	Практические занятия		2	2	
	Практическая работа №4 Обеспечение безопасности сети: изучение угроз сетевой безопасности. Обеспечение безопасности сетевых устройств		2	2	
Тема 2.2. Системный подход к управлению безопасностью	Содержание учебного материала		8	2	
	1	Иерархия средств защиты от информационных угроз	2		
	2.	Политика информационной безопасности.	2		
	3	Принципы защиты информационной системы	2		
	Практические занятия		2	2	
	Практическая работа №5 Разработка политики информационной безопасности организации		2	2	
Тема 2.3. Базовые технологии компьютерной безопасности	Содержание учебного материала		24	6	
	1	Основные понятия криптографии	2		
	2.	Симметричные и ассиметричные алгоритмы шифрования	2		
	3.	Разновидности атак на криптосистемы	2		
	4.	Технология аутентификации. Факторы аутентификации	2		
	5.	Аутентификация на основе сертификатов	2		
	6	Аутентификация информации. Электронная подпись	2		
	7	Технологии авторизации и управления доступом. Формы представления ограничений доступа	2		
	8	Фильтрация и мониторинг трафика	2		
	9	Безопасность локальных беспроводных сетей	2		
	Практические занятия		6	6	
	Практическая работа №6 Выполнение установки программного обеспечения для работы с инфраструктурой открытых ключей. Создание открытого и закрытого криптографических ключей		2	2	
	Практическая работа №7 Выполнение операций по обмену открытыми		2	2	

	ключами через инфраструктуру открытых ключей, отправке и получению зашифрованных и подписанных ЭЦП документов			
	Практическая работа №8 Выполнение настройки межсетевых экранов: создание правил фильтрации пакетов для предотвращения доступа к внутренним сервисам	2	2	
Тема 2.4 Безопасность системного и прикладного программного обеспечения	Содержание учебного материала	14	6	
	1. Архитектурная безопасность операционной системы	2		
	2. Аутентификация пользователей в операционной системе Windows	2		
	3. Аутентификация пользователей в операционной системе Linux	2		
	4. Стандарт безопасности и сертификация операционных систем и программных систем	2		
	Практические занятия	6	6	
	Практическая работа №9 Создание пользователей и групп в операционной системе Windows. Решение задач поиска и сброса паролей пользователей	2	2	
	Практическая работа №10 Выполнение настройки системы парольной защиты в локальной политике безопасности операционной системы Windows	2	2	
Практическая работа №11 Выполнение настройки параметров аудита в операционной системе Windows в заданных условиях. Получение и интерпретация результатов аудита	2	2		
Консультация	2			
Промежуточная аттестация (экзамен):	8			
Всего:	84	22		

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Учебная дисциплина реализуется в **лаборатории информатики и информационных технологий в профессиональной деятельности:**

1 Специализированная мебель и системы хранения:

- стол преподавателя с ящиками для хранения;
- кресло преподавателя;
- доска учебная;
- шкафы для хранения наглядных пособий и учебно-методического комплекса;
- стол ученический;
- стул ученический;
- компьютеризированные рабочие места обучающихся с базовой комплектацией, объединенные в единую сеть с выходом в Интернет;
- компьютеризированное рабочее место преподавателя.

2 Технические средства:

- компьютеры по количеству посадочных мест для учащихся;
- компьютер преподавателя;
- локальная компьютерная сеть и глобальная сеть Интернет;
- офисный пакет программного обеспечения;
- образовательный контент и система защиты от вредоносной информации;
- сетевой фильтр;
- аппаратный комплекс стационарный (проектор, интерактивная доска);
- лицензионное программное обеспечение: операционная система Windows (Linux, Mac OS), AutoCAD, КОМПАС-График, 3Д, Solidworks, MARC, ANSYS. Основные прикладные программы: текстовый редактор, электронные таблицы, система управления базами данных, программа разработки презентаций, средства электронных коммуникаций, интернет-браузер, справочно-правовая система;
- сетевое оборудование;
- принтер.

3. Демонстрационные учебно-наглядные пособия

- комплект учебно-наглядных пособий
- комплект учебно-методической документации, в том числе на электронном носителе (учебники и учебные пособия, карточки-задания, комплекты тестовых заданий, задания для контрольных работ, промежуточной аттестации, методические рекомендации и разработки).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основная:

Дополнительная:

1. Бубнов А.А. Основы информационной безопасности: учебник для студ. учреждений сред. проф. образования/ А.А.Бубнов, В.Н. Пржегорлинский, О.А. Савинкин. – М.: Издательский центр «Академия», 2018. – 256 с.
2. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей. – М.: Горячая линия – Телеком, 2018. – 644 с.
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд.,

перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340>

4. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717>

5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567521>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
1	2
умения:	
<p>Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;</p> <p>Применять основные правила и документы системы сертификации Российской Федерации;</p> <p>Классифицировать основные угрозы безопасности информации;</p> <p>Соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации-производителя;</p> <p>Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки.</p>	<p>Произведена классификация защищаемой информации и отнесение ее к одной из разновидностей;</p> <p>Соотнесение конкретной производственной ситуации и документов, регламентирующих спорные вопросы, возникающие в процессе ее реализации;</p> <p>Способность отнесения конкретной угрозы информационной безопасности к одному из видов;</p> <p>Произведена установка антивирусного программного обеспечения и программных инструментов криптографической защиты данных в соответствии с заявленными разработчиком требованиями;</p> <p>Решены возникающие проблемные ситуации при установке программного обеспечения.</p>
Знания:	
<p>Сущность и понятие информационной безопасности, характеристику ее составляющих;</p> <p>Место информационной безопасности в системе национальной безопасности страны;</p> <p>Источники угроз информационной безопасности и меры по их предотвращению;</p> <p>Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;</p> <p>Современные средства и способы обеспечения информационной безопасности.</p> <p>Лицензионные требования по настройке устанавливаемого программного обеспечения;</p> <p>Типовые причины инцидентов, возникающих при установке программного обеспечения;</p> <p>Основы архитектуры, устройства и функционирования вычислительных систем;</p> <p>Принципы организации, состав и схемы работы операционных систем; Стандарты информационного взаимодействия систем.</p>	<p>Не менее 60 % правильных ответов</p> <p>Соответствие результатов выполнения практических работ примерам</p>

РЕЦЕНЗИЯ
на рабочую программу
по дисциплине «Информационная безопасность в компьютерных системах»

для специальности 09.02.01 Компьютерные системы и комплексы
квалификация выпускника – специалист по компьютерным системам
профиль – технологический
форма обучения – очная

Автор Кашимова Л.В., преподаватель ГБПОУ РО «СИТ».

В рабочей программе, представленной на рецензирование, отражены:

- Цели освоения дисциплины, соотношенные с общими целями программы подготовки специалистов среднего звена.
- Место дисциплины в структуре образовательной программы: цикл общепрофессиональных дисциплин.
- Компетенции обучающегося, формируемые в результате освоения дисциплины согласно ФГОС СПО по специальности 09.02.01 Компьютерные системы и комплексы, утвержденного Приказом Минпросвещения России от 25.05.2022 №362 (ред. от 03.07.2024). Указан перечень и описание компетенций, а так же требования к знаниям, умениям и навыкам, полученным в ходе изучения дисциплины.
- Структура и содержание дисциплины, включающая общую трудоемкость в часах, формы контроля по учебному плану – экзамен; тематический план содержания дисциплины; тематика лекционных и практических занятий, списки литературы и электронных образовательных ресурсов.
- Образовательные технологии, указанные по видам учебной деятельности.
- Оценочные средства для текущего контроля успеваемости, промежуточной аттестации, учебно-методическое обеспечение.

Учебно-методическое и информационное обеспечение дисциплины содержит перечень основной и дополнительной литературы, программного обеспечения и электронных образовательных ресурсов.

В разделе «Материально-техническое обеспечение» указаны специализированные лаборатории и кабинеты с перечнем оборудования и технических средств обучения, обеспечивающих реализацию всех видов учебной работы.

При изучении дисциплины приняты во внимание специализация с учетом региональных особенностей структуры предприятий.

Заключение: данная рабочая программа учебной дисциплины «Информационная безопасность в компьютерных системах» рекомендуется к использованию при подготовке специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы.

Рецензент:

Ирашко Роман Борисович

(фамилия, имя, отчество)

Начальник Службы охраны связи и радио

(должность, организация)

Подпись

[Подпись]

дата

Телефон

М.П.



РЕЦЕНЗИЯ
на рабочую программу
по дисциплине **«Информационная безопасность в компьютерных системах»**
для специальности 09.02.01 Компьютерные системы и комплексы
квалификация выпускника – специалист по компьютерным системам
профиль –технологический
форма обучения – очная

Автор Кашимова А.В., преподаватель ГБПОУ РО «СИТ».

Рабочая программа учебной дисциплины **«Информационная безопасность в компьютерных системах»** разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по программе подготовки специалистов среднего звена специальности 09.02.01 Компьютерные системы и комплексы.

Учебная дисциплина **«Информационная безопасность в компьютерных системах»** является обязательной частью общепрофессионального цикла примерной основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.01 Компьютерные системы и комплексы. Добавлена из часов вариативной части.

В каждом разделе четко обозначены: цели и задачи изучения дисциплины, направленные на формирование у обучающихся умений:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации;
- соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации-производителя;
- идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки..

Выделены требования к входным знаниям, умениям, компетенциям обучающихся и представлены ожидаемые результаты образования и компетенции по завершении освоения дисциплины **«Информационная безопасность в компьютерных системах»**.

В результате освоения учебной знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.
- лицензионные требования по настройке устанавливаемого программного обеспечения;
- типовые причины инцидентов, возникающих при установке программного обеспечения;
- основы архитектуры, устройства и функционирования вычислительных систем;
- принципы организации, состав и схемы работы операционных систем;

