

Министерство образования и науки РТ
Государственное автономное профессиональное
образовательное учреждение
«КАЗАНСКИЙ РАДИОМЕХАНИЧЕСКИЙ КОЛЛЕДЖ»



**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ**

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

основной профессиональной образовательной программы (ОПОП)
по программе подготовки специалистов среднего звена (ППССЗ)
09.02.11 «Разработка и управление программным обеспечением»

Казань, 2025

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением, утверждённого приказом Министерства просвещения РФ от 24 февраля 2025 г. N 138 и с учетом примерной программы по дисциплине ОП.05 Основы информационной безопасности (Приказ ФГБОУ ДПО ИРПО № 01-09-580/2025 от 13.10.2025).

Организация-разработчик: ГАПОУ «Казанский радиомеханический колледж»

Разработчик:

Никулина Валентина Сергеевна, преподаватель

РАССМОТРЕНО

Предметно-цикловой комиссией

Протокол №1 от « 08 » 09 2025 г.

Председатель ПЦК №3

Коклюгина Н.А.



СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	8
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	9

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения программы

Программа учебной дисциплины является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности среднего профессионального образования образовательной программы подготовки специалистов среднего звена (далее – СПО ППССЗ) 09.02.11 «Разработка и управление программным обеспечением».

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Программа учебной дисциплины «Основы информационной безопасности» входит в цикл «Общепрофессиональный».

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

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

- классифицировать защищаемую информацию по видам тайны и степеням секретности;
- классифицировать основные угрозы безопасности информации.

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

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

Результаты освоения дисциплины направлены на формирование общих и профессиональных компетенций (ОК/ПК):

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 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации.

1.4. Количество часов на освоение программы учебной дисциплины:

учебная нагрузка обучающегося 48 часов, в том числе:

- во взаимодействии с преподавателем 48 часов,
- самостоятельная работа обучающегося 0 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Учебная нагрузка обучающегося (всего)	48
Самостоятельная работа	
во взаимодействии с преподавателем	48
в том числе:	
теоретическое обучение	28
практические занятия	20
лабораторные занятия	
в том числе практическая подготовка	20
курсовый проект (работа)	
Консультации	
<i>Промежуточная аттестация форме <i>Дифференцированного зачета</i></i>	

2.2. Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности			
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала	4	
	1 ТБ. Понятие информационной безопасности. Место информационной безопасности в системе национальной безопасности страны (основные составляющие национальных интересов РФ, положения государственной политики, направления международного сотрудничества РФ)	2	2
	2 Основные виды и источники угроз информационной безопасности РФ (элементы организационной основы системы обеспечения информационной безопасности РФ).	2	2
	Практические занятия (практическая подготовка)	2	
	1 Подготовка сообщений на тему: «Информационная война. Информационное оружие. Радиоэлектронная борьба»	2	3
Тема 1.2. Основы защиты информации	Содержание учебного материала	4	
	1 Информация. Жизненные циклы конфиденциальной информации (целостность, доступность и конфиденциальность информации). Классификация.	4	2
	Практические занятия (практическая подготовка)	10	
	1 Подготовка сообщений об охране различных видов тайн (государственной, коммерческой, банковской, профессиональной, служебной тайн, медицинской и персональных данных)	6	3
	2 Авторское право и интеллектуальная собственность	4	3
	3 Система лицензирования и сертификации РФ в области защиты информации	4	3
Раздел 2. Современные средства и методы обеспечения информационной безопасности			
Тема 2.1. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	18	
	1 Элементы и объекты защиты. Методы, средства и механизмы защиты.	2	2
	2 Технологии предотвращения, парирования и нейтрализации угроз информационной безопасности.	2	2
	3 Криптография. Классификация методов криптографического закрытия.	2	2
	4 Системы с открытыми ключами. Электронная цифровая подпись.	2	2
	5 Классификация вирусов. Технологии борьбы. Антивирусные программы	2	2

6	Основные механизмы защиты ПК от несанкционированного доступа (физическая защита, аутентификация, разграничение доступа, криптографическое закрытие, регистрация обращений).	2	2
7	Инженерная защита и техническая охрана объектов информатизации.	2	2
8	Автоматизированные системы контроля доступа (АСКД) (использование пластиковых идентификационных карточек, смарт-карт, логотипов, эмбоссирования и биометрических систем идентификации).	4	2
Практические занятия (практическая подготовка)		8	
1	Классификация угроз безопасности информации на типовом объекте информатизации	2	3
2	Выбор мер защиты информации, необходимых в колледже	2	3
3	Работа на тему: «Моя домашняя антивирусная программа. Плюсы и минусы»	2	3
4	Защита файлов и папок на персональном компьютере.	2	3
Дифференцированный зачет		2	
Всего:		48	

Для характеристики уровня усвоения учебного материала используются следующие обозначения:

1. ознакомительный (узнавание ранее изученных объектов);
2. репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3. продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия лаборатории Компьютерных сетей и основ информационной безопасности.

Оборудование учебного кабинета:

- проектор – 1 шт.;
- интерактивная доска – 1 шт.;
- 3D принтер – 3 шт.;
- принтер -1 шт;
- столы и стулья – 14/28;
- персональный компьютер с программным обеспечением – 19 шт;
- плоттер – 1 шт.;
- локальный сервер.

3.2. Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основные источники:

1. Батаев А.В. Операционные системы и среды. - М.: Издательский центр «Академия», 2023. — 288 с.

Электронные издания (электронные ресурсы)

1. Рудаков, А. В. Операционные системы и среды: учебник / А.В. Рудаков. — Москва: КУРС: ИНФРА-М, 2021. — 304 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-85-1. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1423328>
2. Партика, Т. Л. Операционные системы, среды и оболочки: учебное пособие / Т.Л. Партика, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 560 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-501-1. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1189335>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
<p>Умения:</p> <ul style="list-style-type: none"> – классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации. 	<p>Наблюдение за выполнением практического и лабораторного задания (деятельностью студента) Оценка выполнения практического и лабораторного задания</p>
<p>Знания</p> <ul style="list-style-type: none"> – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, действующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности. 	<p>Индивидуальный и фронтальный опрос в ходе аудиторных занятий, контроль выполнения индивидуальных и групповых заданий, заслушивание рефератов.</p>

Результаты обучения (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 1.1. Проектировать базы данных.	– профессиональное применение полученных знаний при проектировании баз данных	Устные опросы, практические занятия, выполнение заданий, подготовка докладов
ПК 2.2. Разрабатывать модули программного обеспечения.	– профессиональное применение полученных знаний при разработке модулей программного обеспечения	Устные опросы, практические занятия, выполнение заданий, подготовка докладов
ПК 3.2. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.	– профессиональное применение полученных знаний при разработке проектной документации на разработку	Устные опросы, практические занятия, выполнение заданий, подготовка докладов

	информационной системы в соответствии с требованиями заказчика.	
--	---	--

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений, а также личностных результатов воспитания.

Результаты обучения (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
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;	Стремление освоить работу с разными видами информации: диаграммами, символами, графиками, текстами, таблицами; Владение современными средствами получения и передачи информации (факс, сканер, компьютер, принтер и т.д.) и информационными и телекоммуникационными технологиями (аудиовидеозапись, электронная почта, СМИ. Интернет)	Наблюдение и оценка на практических занятиях, при выполнении работ по учебным и производственным практикам.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;	Стремление поддерживать российскую гражданскую идентичность, патриотизм, уважение к своему народу, чувства ответственности перед Родиной, гордости за свой край, свою Родину, прошлое и настоящее многонационального народа России, уважение государственных символов (герб, флаг, гимн); гражданскую позицию как активного и ответственного члена российского общества, осознающего свои конституционные права и обязанности, уважающего закон и правопорядок, обладающего чувством собственного достоинства, осознанно принимающего традиционные национальные и общечеловеческие гуманистические и демократические ценности; готовность к служению	Наблюдение и оценка на практических занятиях, на зачетном занятии, на практике

	<p>Отечеству, его защите;</p> <p>OK 09. Пользоваться профессиональной документацией на государственном и иностранном языках.</p>	<p>Владение навыками устной и письменной речи, ведения деловой переписки на государственном и иностранном языке. Использование справочной и технической документации на государственном и иностранном языках при выполнении поставленных задач.</p>
--	--	---