Приложение 5

К ППССЗ специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан «Технический колледж имени Р.Н. Ашуралиева»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.01. Основы информационной безопасности

Специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника: Техник по защите информации

Махачкала 2025 г.

ОДОБРЕНО

предметной (цикловой) комиссией УГС 09.00.00. Информатика и вычислительная техника и 10.00.00 Информационная безопасность

Председатель П(Ц)К

 Ш.М. Мусаева

Протокол №1 от 29 июня 2025 г.

Рабочая программа учебной дисциплины ОП.01. Основы информационной безопасности разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016 г., (зарегистрирован Министерством юстиции РФ 26 декабря 2016 г. N 44938);

с учетом:

- Примерной основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий и специальностей 10.00.00 Информационная безопасность (протокол № 1 от 28.03.2017)

в соответствии с рабочим учебным планом по специальности.

Разработчик:

- Ханахмедов Мурад Илгарович, преподаватель ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.01. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.01 Основы информационной безопасности принадлежит общепрофессиональному циклу ОП.00 обязательной части ФГОС специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Дисциплина ОП.01 Основы информационной безопасности является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

1.2. Цель и планируемые результаты освоения дисциплины:

Освоение дисциплины должно способствовать формированию общих компетенций:

- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения;
- ОК 9. Использовать информационные технологии в профессиональной деятельности;
- ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

Освоение дисциплины должно способствовать овладению профессиональными компетенциями:

- ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

В результате освоения дисциплины обучающийся должен уметь:

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

В результате освоения 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.

Код ПК, ОК	Умения	Знания

ОК 03 ОК 06 ОК 09 ОК 10 ПК 2.4	– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации.	– 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.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.01. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы	60
в том числе:	
Теоретическое обучение	30
Лабораторные занятия	12
Практические занятия	6
Самостоятельная работа	12
Промежуточная аттестация в форме дифференцированного зачета	-

– Объем времени обязательной части ППССЗ 48 час.

– Объем времени вариативной части ППССЗ 12 час.

Вариативная часть используется на углубление подготовки по дисциплине.

2.2. Тематический план и содержание учебной дисциплины ОП.01. Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Теоретические основы информационной безопасности		**26**	
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	4	
	1. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.		
	2. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.		
Тема 1.2. Основы защиты информации	**Содержание учебного материала**	6	
	3. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.		
	4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи		
	Практические занятия	6	
	5. Определение объектов защиты на типовом объекте информатизации.		
	6. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.		
Тема 1.3. Угрозы безопасности защищаемой информации	**Содержание учебного материала**	4	
	7. Понятие угрозы безопасности информации		
	8. Системная классификация угроз безопасности информации.		
	9. Каналы и методы несанкционированного доступа к информации		
	10. Уязвимости. Методы оценки уязвимости информации		
	Лабораторные работы	6	
	11. Определение угроз объекта информатизации и их классификация		
Раздел 2. Методология защиты информации		**22**	
Тема 2. 1. Методологические подходы к защите информации	**Содержание учебного материала**	4	
	12. Анализ существующих методик определения требований к защите информации.		
	13. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.		
	14. Виды мер и основные принципы защиты информации.		
	15. Анализ существующих методик определения требований к защите информации.		
	Содержание учебного материала	4	

Тема 2. 2. Нормативно - правовое регулирование защиты информации	16.	Организационная структура системы защиты информации		
	17.	Законодательные акты в области защиты информации.		
	18.	Российские и международные стандарты, определяющие требования к защите информации.		
	19.	Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации		
	Лабораторные работы		6	
	20.	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности		
Тема 2. 3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**		6	
	21.	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.		
	22.	Программные и программно-аппаратные средства защиты информации		
	23.	Инженерная защита и техническая охрана объектов информатизации		
	24.	Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.		
	Лабораторные занятия		2	
	25.	**Выбор мер защиты информации для автоматизированного рабочего места**		
Самостоятельная работа обучающихся:			**12**	
	Изучить теоретический материал и составить тезисы (краткий конспект): – Анализ рисков информационной безопасности – Обеспечение информационной безопасности в ведущих зарубежных странах – Построение концепции информационной безопасности предприятия – Процедура аутентификации пользователя на основе пароля – Механизмы контроля целостности данных			
	Промежуточная аттестация в форме дифференцированного зачета		**-**	
	Всего:		**60**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.01. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Материально-техническое обеспечение

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения: учебный кабинет «Информационной безопасности» и лаборатория «Информационных технологий».

Оборудование учебного кабинета «Информационной безопасности»:

- Рабочие места на 25 обучающихся;
- Магнитно-маркерная доска.
- Комплект учебно-методической документации;
- Фонд оценочных средств по дисциплине.

Лаборатория «Информационных технологий»

- Рабочие места на 25 обучающихся;
- Компьютеры, объединенные в локальную вычислительную сеть;
- Автоматизированные рабочие места на 12 обучающихся, подключенные к локальной вычислительной сети и сети «Интернет»;
- Автоматизированное рабочее место преподавателя;
- Интерактивная доска, проектор, кронштейн;
- МФУ;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения;
- Программное обеспечение сетевого оборудования;
- Браузер;
- Антивирусная программа.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Бубнов А.А., Пржегорлинский В.Н., Савинкин О.А. Основы информационной безопасности. –М.: Академия. 2024.

3.2.2. Дополнительные печатные источники:

1. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. – М.: Издательство КДУ.
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. - М: Горячая линия-Телеком. - 544 с.: ил. Допущено УМО ИБ.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита. Учебное пособие. – М.: Инфа-М. 2022.
4. Бабаш А.В. Информационная безопасность. Лабораторный практикум (+CD) : учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — 2-е изд., стер. – М.: КНОРУС, 2022.
5. Нестеров С.А. Основы информационной безопасности. Учебное пособие. – С-Пб.: Лань. 2023.

6. Пржегорлинский В.Н. Организационно-правовое обеспечение информационной безопасности. –М.: Академия. 2023.
7. Проскурин В.Г. Защита программ и данных: Учебное пособие для ВУЗов. - –М.: Академия. 2022.
8. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. – С-Пб.: Изд. Питер. 2022.
9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. ДМК Пресс, 2022.

3.2.4. Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: bit.mephi.ru/

3.2.3. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Кадровое обеспечение образовательного процесса

Реализация программы учебной дисциплины обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках.

Требования к квалификации педагогических работников. Высшее профессиональное образование или среднее профессиональное образование по направлению подготовки "Образование и педагогика" или в области, соответствующей преподаваемой дисциплине, без предъявления требований к стажу работы, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы.

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	**Критерии оценки**	**Формы и методы оценки**
Знания: – 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.	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование
Умения: – классифицировать – защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации.	Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности	Экспертное наблюдение в процессе практических занятий