ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Принято учебно-методической
комиссией факультета среднего
профессионального образования
протокол № 7 от «24» апреля 2023 г.

Утверждаю:
Декан факультета среднего
Профессионального образования
_____ О.С. Гаврилова
«24» апреля 2023 г.

РАБОЧАЯ ПРОГРАММА

УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.15 Информационная безопасность

Программы подготовки специалистов среднего звена

по специальности среднего профессионального образования
09.02.07 Информационные системы и программирование
базовый уровень подготовки

Профиль получаемого профессионального образования:
технологический

Квалификация выпускника
Программист

Форма обучения
очная

г. Ставрополь, 2023 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.15 Информационная безопасность»

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.15 Информационная безопасность является обязательной вариативной частью общепрофессионального цикла ОПОП-П в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

Особое значение дисциплина имеет при формировании и развитии ОК 01, ОК 02., ОК 05, ОК 09

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01	анализировать задачу и/или проблему и выделять еёсоставные части;	алгоритмы выполненияработ в профессиональной исмежных областях;
	определять этапы решениязадачи;	структуру плана длярешения задач;
	выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы	порядок оценкирезультатов решениязадач профессиональной деятельности
	составлять план действия;	
	определять необходимыересурсы	
	реализовывать составленныйплан;	
	оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	
ОК 02	определять задачи для поиска информации;	приемы структурирования информации
	выделять наиболее значимое в	формат оформления результатов поиска информации, современные средства и устройства информатизации

	перечне информации	порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств
	оценивать практическую значимость результатовпоиска	
	использовать современное программное обеспечение	
ОК 05	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе	правила оформления документов и построенияустных сообщений
ОК 09	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы	правила построения простых и сложных предложений на профессиональные темы
	строить простые высказывания о себе и о своей профессиональной деятельности	правила чтения текстов профессиональной направленности
	кратко обосновывать и объяснять свои действия (текущие и планируемые)	
	писать простые связные сообщения на знакомые или интересующие профессиональные темы	

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	**58**
в т.ч. в форме практической подготовки	**28**
в т. ч.:	
теоретическое обучение	10
лабораторные работы	
практические занятия	36
курсовая работа (проект)	
Самостоятельная работа	2
Промежуточная аттестация	**2**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	**Содержание учебного материала и формы организациидеятельности обучающихся**	**Объем, акад. ч / в том числе в форме практической подготовки, акад. ч**	**Коды компетенций и личностных результатов, формированиюкоторых способствует элемент программы**
1	***2***	***3***	***4***
Раздел 1. Вопросы информационной безопасности.			
Тема 1 Основные понятия теории информационной безопасности	**Содержание учебного материала**	**6/4**	
	История становления теории информационной безопасности. **Основные понятия и определения, предметная область теории информационной безопасности** Основные термины и определения правовых понятий в области информационных отношений Понятия информация, информатизация, информационная система, информационная безопасность. Основные составляющие информационной безопасности: целостность, доступность конфеденциальность	2	ОК 01
	В том числе практических занятий и лабораторных работ	**4**	
	Защита документооборота в вычислительных системах Проведение анализа информационной системы	2 2	ОК 05 ОК 09
	Самостоятельная работа обучающихся		
Тема 2. Государственная	**Содержание учебного материала**	**10/8**	

политика информационной безопасности	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Административный уровень информационной безопасности Программа синхронизации информационной безопасности с жизненным циклом систем Программно – технический уровень информационной безопасности	2	ОК 01
	В том числе практических занятий и лабораторных работ	**8**	
	Изучение доктрины информационной безопасности Законодательство РФ в области информационной безопасности Обеспечение информационной безопасности в ведущих зарубежных странах	2 4 2	ОК 01 ОК 02 ОК 05 ОК 09
	Самостоятельная работа обучающихся		
Тема 3. Угрозы безопасности.		**12/8/2**	
	Компьютерная система как объект защиты Источники угроз. Предпосылки появления угроз Классификация и виды угроз информационной безопасности Понятие угрозы. Виды противников или «нарушителей». Источники угроз. Предпосылки появления угроз Анализ уязвимостей системы Случайные или преднамеренные угрозы информационной безопасности Классификация и виды угроз информационной безопасности. Виды угроз. Основные нарушения Основные направления и методы реализации угроз Характер происхождения угроз (умышленные и естественные факторы).. Оценка уязвимости системы Классы каналов несанкционированного доступа к иформации	2	ОК 01 ОК 09
	В том числе практических занятий и лабораторных работ	**8**	

	1 Анализ источников, каналов распространения и каналов утечки информации Криптографические методы защиты Основные направления и методы реализации угроз Оценка уязвимости системы Шифрование методом IDEA	2 2 2 2	ОК 02 ОК 05 ОК 09
	Самостоятельная работа обучающихся Виды защиты 2. Выявление угроз и уязвимостей	**2**	ОК 02 ОК 05 ОК 09
Тема 4 Системы защиты от угроз	**Содержание учебного материала**	**12/10**	
	Компьютерная система как объект защиты Источники угроз. Предпосылки появления угроз Классификация и виды угроз информационной безопасности.	2	ОК 01 ОК 09
	В том числе практических занятий и лабораторных работ	**10**	
	Методы аутентификации, использующие пароли Криптографические методы защиты. Изучение политики безопасности ОС Windows Управление шаблонами безопасности в ОС Windows Шифрование методом IDEA Настройка безопасности почтового клиента Антивирусные программные комплексы. Восстановление зараженных файлов	2 2 2 2 2	ОК 02 ОК 05 ОК 09
	Самостоятельная работа обучающихся		
Тема 5 Политика и модели безопасности	**Содержание учебного материала**	**8/6**	
	Политика безопасности Аксиомы политики безопасности Парольные системы разграничения доступа	2	ОК 01 ОК 02
	В том числе практических занятий и лабораторных работ	**6**	
	1. Криптосистема Эль-Гамаля	2	ОК 01

	Шифрование методом Вернам Криптоанализ	2 2	ОК 02
	Самостоятельная работа обучающихся		
Промежуточная аттестация		**2**	
Всего:		**50**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Вычислительной техники, архитектуры ПК и периферийных устройств»**,** оснащенная в соответствии с п. 6.1.2.1. образовательной программы по специальности 09.02.07 Информационные системы и комплексы.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1 ЭБС «Юрайт»: Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 03.01.2022).— Режим доступа : https://urait.ru/book/informacionnaya-bezopasnost-467370

2 2. ЭБС «Лань»: Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 03.01.2022). — Режим доступа https://e.lanbook.com/book/195510

3.2.2. Основные электронные издания

1 ЭБС «Юрайт»: Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/467370 (дата обращения: 03.01.2022).— Режим доступа : https://urait.ru/book/informacionnaya-bezopasnost-467370

2 2. ЭБС «Лань»: Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 03.01.2022). — Режим доступа https://e.lanbook.com/book/195510

3.2.2. Дополнительные источники

1. ЭБС «Юрайт»: Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2021. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/475889 (дата обращения: 03.01.2022). — Режим доступа: https://urait.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-475889#page/1
2. ЭБС «Лань»: Программные продукты и системы (периодические издания)
3. ЭБС «Лань»: Информатика и системы управления (периодические издания)
4. CHIP+DVD (периодические издания)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Методы оценки***
- сущность и понятие информационной безопасности, характеристику ее составляющих; - основные виды угроз; - современные методы защиты информации; - виды продуктов вирусов; - требования к защите информации, критерии оценки угроз. - современные законы, стандарты, методы и технологии в области защиты информации	- знать сущность и понятие информационной безопасности, ориентироваться в ее составляющих; -знать основные виды угроз и уметь их классифицировать ; - знать, понимать и уметь применять современные методы защиты информации; -знать, и ориентироваться в основных федеральных, региональных законах защиты информации; -знать основные компоненты программного обеспечения компьютерных систем; -знать, понимать основные принципы управления ресурсами и организации доступа к этим ресурсам.	Оценка: -устных ответов; -выполнения практических заданий; -тестирование - дифференцированный зачет
- использовать современные программно-аппаратные средства защиты информации - Подобрать и обеспечить защиту информации -	демонстрировать умение получать информацию о угрозах информационной безопасности; - уметь устранять угрозы связанные с несанкционированным доступом к информации; -правильно подключать дополнительное оборудование и настраивать связь между элементами компьютерной системы; -грамотно производить инсталляцию и настройку программного обеспечения компьютерных систем.	Оценка: -устных ответов; -выполнения практических заданий; - тестирование - дифференцированный зачет