Частное профессиональное образовательное учреждение

«Сочинский финансово-юридический колледж»

РАБОЧАЯ ПРОГРАММА
учебной дисциплины ОП.14. Информационная безопасность
специальность 09.02.07 Информационные системы и программирование

Сочи, 2021

Рассмотрена

Утверждена

Заместитель директора по УВР

«18» 08 2021 г.

директор ЧПОУ СФЮК

«28» « 08 » 2021 г.

Горшкова И.Ю.

Перминова Г.Е.

м.п.

Рассмотрена на заседании педагогического совета протокол № 1 от 2_.08. 2021 г.

Рассмотрена

Утверждена

Заместитель директора по УВР

«29» 08 2022 г.

директор ЧПОУ СФЮК

«29» « 08 » 2022 г.

Горшкова И.Ю.

Перминова Г.Е.

м.п.

Рассмотрена на заседании педагогического совета протокол № 1 от 29.08. 2022 г.

Рассмотрена

Утверждена

Заместитель директора по УВР

«28» 08 2023 г.

директор ЧПОУ СФЮК

«28» « 08 » 2023 г.

Горшкова И.Ю.

Перминова Г.Е.

м.п.

Рассмотрена на заседании педагогического совета протокол № 1 от 28.08. 2023 г.

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование утвержденного Приказом Минобрнауки России от № 1567, от 9 декабря 2016 г.

Организация разработчик: ЧПОУ СФЮК
Разработчик:
Старинчиков Сергей Михайлович, преподаватель информационных дисциплин ЧПОУ СФЮК

____
(подпись)

СОДЕРЖАНИЕ

стр.

1. **ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ** **4**
2. **СТРУКТУРА И СОДЕРЖАНИЕУЧЕБНОЙ ДИСЦИПЛИНЫ** **5**
3. **УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ** **10**
4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ** **11**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.14. Информационная безопасность

1.1. Место дисциплины в структуре основной профессиональной образовательной программы.

Учебная дисциплина ОП.14. Информационная безопасность является общепрофессиональной дисциплиной профессионального цикла, реализуется за счет вариативной части ОПОП.

1.2. Цель и планируемые результаты освоения дисциплины:

Цель учебной дисциплины – способствовать формированию профессиональных компетенций (ПК) ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8, ПК 9.9, ПК 9.10, ПК 11.6, общих компетенций (ОК) 1, 2, 4, 5, 6, 9, 10; личностных результатов (ЛР) 3, 4, 13, 14, 18.

В результате освоения дисциплины обучающийся должен

уметь:

- разрабатывать политику информационной безопасности;
- проводить оценку угроз безопасности объекта информатизации;
- реализовывать простые информационные технологии обеспечивающие методы защиты информации;
- применять методики оценки уязвимости в информационно-телекоммуникационных сетях;
- проектировать системы защиты информации.

знать:

- основные понятия информационной безопасности;
- основные направления защиты информации;
- законодательство Российской Федерации в области защиты информации;
- современные методы и средства защиты информации в информационно-телекоммуникационных системах;
- архитектуру защищённых экономических систем.

1.3. Количество часов на освоение программы учебной дисциплины:

Максимальная учебная нагрузка 57 часов, в том числе:

Обязательная аудиторная учебная нагрузка обучающегося 38 часов;
самостоятельной работы обучающегося 19 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	**57**
Обязательная аудиторная учебная нагрузка (всего)	**38**
в том числе:	
практические занятия	18
Самостоятельная работа обучающегося (всего)	**19**
Итоговая аттестация в форме дифференцированного зачета – 5 семестр	

Тематический план и содержание учебной дисциплины ОП.14. Информационная безопасность

Наименование разделов и тем	№ занятия	Дата	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1			2	3	4
Тема 1. Общие проблемы безопасности. Роль и место информационной безопасности			**Содержание учебного материала**	**12**	ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8, ПК 9.9, ПК 9.10, ПК 11.6 ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10 ЛР 03, ЛР 04, ЛР 13, ЛР 14, ЛР 18
	1		**Национальные интересы и информационная безопасность России. Уровни обеспечения национальной безопасности. Основные угрозы безопасности России. Информационная война**	**2**	
			Самостоятельная работа № 1 Информационное оружие. Принципы, основные задачи и функции обеспечения информационной безопасности (ИБ). Отечественные и зарубежные стандарты информационной безопасности. Подготовка сообщений «Основные задачи в сфере обеспечения ИБ».	**2**	
	2		**ПЗ. Функции государственной системы по обеспечению ИБ. Защита информации (ЗИ).** Основные предметные направления ЗИ. Охрана персональных данных.	**2**	
	3		Коммерческая тайна. Банковская тайна. Профессиональная тайна, Служебная тайна, Охрана интеллектуальной собственности. Правовые основы защиты информации. **Ответственность за нарушение законодательства в информационной сфере. Статьи Кодекса РФ, Уголовного кодекса РФ.**	**2**	
			Самостоятельная работа № 2 Решение задач по теме: «Ответственность за нарушение законодательства в информационной сфере». Подготовка сообщения по теме: «Уровни доступа к информации с точки зрения законодательства»	**2**	
	4		**ПЗ. Анализ Гражданского кодекса РФ в сфере ИБ. Объекты защиты информации в АСОД. Надежность информации. Уязвимость информации.**	**2**	
Тема 2. Защита информации в			**Содержание учебного материала**	**12**	ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8,
	5		**Основные элементы АСОД и типовые структурные компоненты. Дестабилизирующие факторы АСОД. Преднамеренные угрозы**	**2**	

автоматизированных системах обработки данных			**безопасности АСОД. Причины нарушения целостности информации.**		ПК 9.9, ПК 9.10, ПК 11.6 ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10 ЛР 03, ЛР 04, ЛР 13, ЛР 14, ЛР 18
			Самостоятельная работа № 3 Подготовка сообщения по теме «Каналы несанкционированного получения информации в АСОД». Функции и задачи защиты информации. Механизмы защиты, их управление.	**2**	
	6		**ПЗ. Методы и системы защиты информации.** Подтверждение подлинности пользователя и разграничение их доступа к компьютерным ресурсам. Общие сведения о контроле информационной целостности.	**2**	
	7		**Создание и управление учетными записями в ОС Windows 8. Настройка параметров безопасности в ОС Windows 8**	**2**	
			Самостоятельная работа № 4 Средства безопасности в MS Excel 2010. Контроль правильности функционирования системы защиты.	**2**	
	8		**ПЗ. Регистрация действий пользователя. Криптология и основные этапы ее развития».**	**2**	
Тема 3 **Криптографические методы защиты информации**			**Содержание учебного материала**	**12**	ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8, ПК 9.9, ПК 9.10, ПК 11.6 ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10 ЛР 03, ЛР 04, ЛР 13, ЛР 14, ЛР 18
	9		**Криптология и основные этапы ее развития. Методы криптографического преобразования данных. Шифрование заменой (подстановка).**	**2**	
			Самостоятельная работа № 5 Шифрование методом перестановки. Шифрование методом граммирования. Системы с открытым ключом. Электронная цифровая подпись.	**2**	
	10		**ПЗ. Технические и программные средства защиты криптографии.** Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации.	**2**	
	11		**Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. Стандарт симметричного шифрования AES RIJNDAEL.**	**2**	
			Самостоятельная работа № 6 Генерация простых чисел, используемых в асимметричных системах шифрования. Электронная цифровая подпись.	**2**	
	12		**ПЗ. Шифрование методом скользящей перестановки. Шифрование на**	**2**	

			языке программирования TPascal.		
Тема 4. Классификация вирусов. Настройка параметров безопасности.			**Содержание учебного материала**	**12**	ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8, ПК 9.9, ПК 9.10, ПК 11.6 ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10 ЛР 03, ЛР 04, ЛР 13, ЛР 14, ЛР 18
	13		**Проблема управления ключами. Характеристики криптографических средств защиты. Криптографические стандарты.**	**2**	
			Самостоятельная работа № 7 Защита персонального компьютера от несанкционированного доступа. Угрозы информации. Вредоносные закладки в ПК и борьба с ними.	**2**	
	14		**ПЗ. Настройка параметров безопасности в ОС Windows 8. Изучение программных продуктов защиты информации.**	**2**	
	15		**Программа поиска и удаления вредоносных закладок Ad-Aware. Программное обеспечение для защиты информации в ПК.**	**2**	
			Самостоятельная работа № 8 Средства вторжения в частную жизнь. Подготовка сообщения по теме «Троянские и другие вредоносные программы».	**2**	
	16		**ПЗ. Классификация вирусов. Алгоритмы вирусов. Признаки появления вируса. Классы антивирусных программ.** Примеры антивирусных программ.	**2**	
Тема 5. Антивирусные программы			**Содержание учебного материала**	**7**	ПК 4.1, ПК 4.4, ПК 5.3, ПК 6.4, ПК 7.5, ПК 9.8, ПК 9.9, ПК 9.10, ПК 11.6 ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10 ЛР 03, ЛР 04, ЛР 13, ЛР 14, ЛР 18
	17		**Антивирусная программа Dr.Web. Рассмотрение распространенных антивирусных программ. Антивирус Касперского, Антивирус Panda.**	**2**	
			Самостоятельная работа № 8 Антивирус-ревизор. Symantec AntiVirus.	**2**	
	18		**Цели, функции и задачи защиты информации в сетях ЭВМ. Понятие сервисов безопасности.** Архитектура механизмов защиты информации в сетях ЭВМ. Услуги механизмов защиты в сетях. Протоколирование и аудит в ОС Windows 8. Межсетевой экран – брандмауэр в ОС Windows 8. Корректирующие коды для контроля целостности информации. Коды Хэмминга. Циклические кода.	**2**	
			Самостоятельная работа № 8 Технические средства защиты АСОД. Средства контроля доступа. Комплекс физической защиты АСОД.	**1**	

			Содержание учебного материала	**2**	
	19		**ПЗ. Дифференцированный зачёт.**	**2**	
Всего часов				**57**	

Примечания:

1) используемые сокращения: ПЗ – практическое занятие

2) учебные занятия, без указания вида – считать лекционными

3) самостоятельная работа обучающихся – это учебная деятельность обучающихся без непосредственного контакта с преподавателем согласно установленного расписания в аудиториях колледжа или дистанционно

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета информатики.

Оборудование учебного кабинета:

- рабочее место преподавателя;
- компьютеры, установленные в кабинете в единую сеть, с выходом через прокси-сервер в Интернет;
- компьютерные столы по числу рабочих мест обучающихся;
- вентиляционное оборудование, обеспечивающие комфортные условия проведения занятий.

Технические средства обучения:

- компьютер с лицензионным программным обеспечением и мультимедийный проектор;
- Таблицы

3.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий:

Интернет – ресурсы:

1. ЭБС ЮРАЙТ www.biblio-online.ru:

1. 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, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — URL: https://urait.ru/bcode/467356

2. 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, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — URL: https://urait.ru/bcode/456792

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения	Критерии оценки	Формы и методы оценки
Перечень **знаний**, осваиваемых в рамках дисциплины: – основные понятия информационной безопасности; – основные направления защиты информации; – законодательство Российской Федерации в области защиты информации; – современные методы и средства защиты информации в информационно-телекоммуникационных системах; – архитектуру защищённых экономических систем.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Примеры форм и методов контроля и оценки • Самостоятельная работа. • Практическое занятие • Наблюдение за выполнением практического задания. (деятельностью студента) • Оценка выполнения практического задания (работы) • Подготовка и выступление с докладом, сообщением, презентацией • Дифференцированный зачет
Перечень **умений**, осваиваемых в рамках дисциплины: – разрабатывать политику информационной безопасности; – проводить оценку угроз безопасности объекта информатизации; – реализовывать простые информационные технологии обеспечивающие методы защиты информации; – применять методики оценки уязвимости в информационно-телекоммуникационных сетях; – проектировать системы защиты информации.		