Частное профессиональное образовательное учреждение
«Сочинский финансово-юридический колледж»

РАБОЧАЯ ПРОГРАММА
учебной дисциплины
ОП.12 Информационная безопасность
09.02.03 Программирование в компьютерных системах

2020

Рассмотрена
ЦМК общепрофессиональных дисциплин
и профессиональных модулей
по программированию в
компьютерных системах
«25» 08 2020 г.
Председатель
_____А.В. Ткач

Утверждена
директор ЧПОУ СФЮК
«28» 08 2020 г.
_____Г.Е.Фертик
М.П.

Рассмотрена на заседании педагогического совета
протокол № 1 от 28.08. 2020 г.

Рассмотрена
ЦМК общепрофессиональных дисциплин
и профессиональных модулей
по программированию в
компьютерных системах
«28» 08 2021 г.
Председатель
_____

Утверждена
директор ЧПОУ СФЮК
«28» 08 2021 г.
_____
М.П.

Рассмотрена на заседании педагогического совета
протокол № 1 от 28.08. 2021 г.

Рассмотрена
ЦМК общепрофессиональных дисциплин
и профессиональных модулей
по программированию в
компьютерных системах
«29» 08 2022 г.
Председатель
_____

Утверждена
директор ЧПОУ СФЮК
«30» 08 2022 г.
_____
М.П.

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

Рассмотрена
ЦМК общепрофессиональных дисциплин
и профессиональных модулей
по программированию в
компьютерных системах
«29» 08 2023 г.
Председатель
_____

Утверждена
директор ЧПОУ СФЮК
«30» 08 2023 г.
_____
М.П.

Рассмотрена на заседании педагогического совета
протокол № 1 от 29.08. 2023 г.

Рабочая программа разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.03 Программирование в компьютерных системах утвержденного Приказом Минобрнауки России от № 804, от 28 июля 2014 г., учебного плана специальности 09.02.07 Информационные системы и программирование, год набора 2020.

Организация разработчик: ЧПОУ СФЮК
Разработчик:
Ткач Андрей Владимирович, преподаватель
Информационных дисциплин ЧПОУ СФЮК

_____
(подпись)

Оглавление

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.12 Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы СФЮК по специальности СПО 09.02.03 «Программирование в компьютерных системах»

Рабочая программа составлена для очной формы обучения.

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Дисциплина «Информационная безопасность» является общепрофессиональной дисциплиной профессионального цикла.

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

В результате изучения учебной дисциплины «Информационная безопасность» обучающийся должен

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.

уметь:

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

1.4. Перечень формируемых компетенций:

Техник-программист должен обладать общими компетенциями, включающими в себя способность:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Вариативная часть - « предусмотрено»

1.5. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки студента 113 часов, в том числе:

обязательной аудиторной учебной нагрузки студента 76 часов;

самостоятельной работы студента - 37 часов;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	113
Обязательная аудиторная учебная нагрузка (всего)	76
в том числе:	
практические занятия	36
Самостоятельная работа обучающегося (всего)	37
Итоговая аттестация в форме ***дифференцированного зачёта***	

2.2 Тематический план и содержание учебной дисциплины
ОП.12 Информационная безопасность

Наименование разделов и тем	Дата проведения занятия	Номер занятия	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа студентов	Объем часов	Уровень освоения
Тема 1 **Общие вопросы информационной безопасности**					
		1.	**Стандарты информационной безопасности** Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации.	2	1
		2.	**Международные стандарты информационного обмена** Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.	2	1
		3.	**ПЗ № 1** **Международные стандарты информационной безопасности**		3
	Самостоятельная работа обучающихся: **Сам.раб. № 1** (Занятие № 1-3) Свойства информации как объекта защиты			2	
		4.	**Требования к защите информации** Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.	2	1
	Самостоятельная работа обучающихся: **Сам.раб. № 2** (Занятие № 4) Требования к защите информации.			1	
Тема 2 **Государственная система информационной безопасности**					
		5.	**Структура государственной безопасности** Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной	2	1

			безопасности Российской Федерации. Структура государственной системы информационной безопасности.		
		6.	**ПЗ № 2** **Структура государственной системы информационной безопасности**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 3** (Занятие № 5-6) Международные стандарты в области информационной безопасности и защиты информации			2	
		7.	**Законодательная база информационной безопасности** Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.	2	1
		8.	**ПЗ № 3** **Структура законодательной базы по вопросам информационной безопасности**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 4** (Занятие № 7-8) Основной закон Российской Федерации.			2	
Тема 3 **Угрозы безопасности**					
		9.	**Классификация угроз** Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.	2	1
		10.	**ПЗ № 4** **Классификация угроз информационной безопасности**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 5** (Занятие № 9-10) Модели угроз и модели нарушителей информационных систем.			2	
		11.	**Целостность информации** Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.	2	1

		12.	**ПЗ № 5** **Угрозы безопасности**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 6** (Занятие № 11-12) Дестабилизирующие факторы.			2	
Тема 4 **Теоретические основы методов защиты информационных систем**					
		13.	**Модели безопасности** Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы.	2	1
		14.	**ПЗ № 6** **Модели безопасности и их применение**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 7** (Занятие № 13-14) Модели угроз согласно нормативным документам ФСТЭК России.			2	
		15.	**Ролевая политика безопасности** Ролевая политика безопасности. Ограничения на области применения формальных моделей.	2	1
		16.	**ПЗ № 7** **Политика безопасности**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 8** (Занятие № 15-16) Ограничения на области применения формальных моделей			2	
Тема 5 **Методы защиты средств вычислительной техники**					
		17.	**Средства защиты компьютерных систем** Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы.	2	1
		18.	**ПЗ № 8** **Обеспечение защиты компьютерных систем**	2	3
		Самостоятельная работа обучающихся: **Сам.раб. № 9** (Занятие № 17-18)		2	

		Электронные ключи, электронные замки.			
		19.	**Целостность и резервирование данных** Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.	2	1
		20.	**ПЗ №9** **Средства операционных систем для защиты информации**	2	3
		Самостоятельная работа обучающихся: **Сам.раб. № 10** (Занятие № 19-20) Средства для оценки защищенности		2	
Тема 6 **Криптография и криптоанализ**					
		21.	**Основы криптографии** Методы криптографии. Симметричное и асимметричное шифрование.	2	1
	Самостоятельная работа обучающихся: **Сам.раб. № 11** (Занятие № 21) Стандарты шифрования ГОСТ 28147-89, DES, AES, RSA, PGP. Стандарты электронно-цифровой подписи ГОСТ 34.10-04, ГОСТ 34.10-2001, DSS			1	
		22.	**Алгоритмы шифрования** Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты.	2	1
		23.	**ПЗ № 10** **Разработка программного обеспечения блочных симметричных шифров.**	2	3
		24.	**ПЗ № 11** **Разработка программного обеспечения асимметричных шифров.**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 12** (Занятие № 22-24) Стандарты электронно-цифровой подписи ГОСТ 34.10-04, ГОСТ 34.10-2001, DSS			1	
		25.	**ПЗ № 12** **Криптоанализ** Криптоанализ и атаки накриптосистемы. **Криптосистемы**	2	2

	Самостоятельная работа обучающихся: **Сам.раб. № 13** (Занятие № 25) Сжатие информации.			2	
Тема 7 Архитектура защищенных экономических систем					
		26.	**Технологии защиты информационных систем** Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации.	2	1
		27.	**ПЗ № 13** **Технологии построения защищённых систем**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 14** (Занятие № 26-27) Электронные платежи.			2	
		28.	**Технологии защиты экономических систем** Стратегии защиты информации. Особенности экономических информационных систем.	2	1
		29.	**ПЗ № 14** **Технологии построения защищённых экономических систем**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 15** (Занятие № 28-29) Электронный кошелек			2	
Тема 8 Алгоритмы привязки программного обеспечения к аппаратному окружению					
		30.	**Средства привязки** Индивидуальные параметры вычислительной системы. Блок проверки аппаратного окружения. Дискета как средство привязки. Технология HASP, эмуляторы. Временные метки и запись в реестр. Обеспечение требуемого количества запусков (trial version).	2	1
		31.	**ПЗ № 15** **Алгоритмы привязки программного обеспечения к аппаратному окружению**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 16** (Занятие № 30-31) Средства идентификации. Биометрическая идентификация.			2	
		32.	**Шифрование исполняемого кода**	2	1

			Технология spyware. Виды распространения программного обеспечения. Шифрование и запутывание исполняемого кода.		
		33.	**ПЗ № 16** **Распространение программного обеспечения**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 17** (Занятие № 32-33) Виды распространения программного обеспечения.			2	
Тема 9 **Алгоритмы безопасности в компьютерных сетях**					
		34.	**Безопасность в компьютерных сетях** Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании».	2	1
		35.	**ПЗ № 17** **Защита серверов и рабочих станций**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 18** (Занятие № 34-35) Удостоверяющий центр. Использование сертификатов ЭЦП для работы в сети. Использование SSL, TLS.			4	
		36.	**Алгоритмы безопасности в компьютерных сетях** Протоколирование. Сетевые защищенные протоколы.	2	1
		37.	**Электронно-цифровая подпись**	2	1
		38.	**ПЗ № 18** **Дифференцированный зачет**	2	3
	Самостоятельная работа обучающихся: **Сам.раб. № 19** (Занятие № 36-37) Использование SSL, TLS.			2	
			Всего:	**113**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
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 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

Дополнительные источники:

1. Перечень печатных изданий ЧПОУ СФЮК

Интернет – ресурсы:

1. ЭБС ЮРАЙТ www.biblio-online.ru:

1. 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 ДИСЦИПЛИНЫ

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Знания:	
З1. основные понятия информационной безопасности;	Оценка выполнения практических работ
З2. основные направления защиты информации;	Оценка выполнения практических работ
З3. законодательство Российской Федерации в области защиты информации;	Оценка выполнения практических работ
З4. современные методы и средства защиты информации в информационно-телекоммуникационных системах;	Оценка выполнения практических работ
З5. архитектуру защищённых экономических систем.	Оценка выполнения практических работ
Умения:	
У 1. разрабатывать политику информационной безопасности;	Оценка выполнения домашних заданий.
У2. проводить оценку угроз безопасности объекта информатизации;	Оценка выполнения практических работ
У3. реализовывать простые информационные технологии реализующие методы защиты информации;	Оценка выполнения практических работ
У4. применять методики оценки уязвимости в информационно-телекоммуникационных сетях;	Оценка выполнения практических работ
У5. проектировать системы защиты информации.	Оценка выполнения практических работ

Вопросы к зачёту

1. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Защита информации, тайна, средства защиты информации.
3. Международные стандарты информационной безопасности
4. Основные нормативные руководящие документы, касающиеся государственной тайны
5. нормативно-справочные документы.
6. Доктрина информационной безопасности Российской Федерации.
7. Структура государственной системы информационной безопасности.
8. Структура законодательной базы по вопросам информационной безопасности.
9. Лицензирование и сертификация в области защиты информации.
10. Классификация угроз информационной безопасности.
11. Причины нарушения целостности информации.
12. Основные положения теории информационной безопасности информационных систем
13. Модели безопасности и их применение.
14. Использование защищенных компьютерных систем.
15. Аппаратные и программные средства для защиты компьютерных систем от НСД.
16. Средства операционной системы.
17. Средства резервирования данных.
18. Способы и средства восстановления работоспособности.
19. Методы криптографии. Симметричное и асимметричное шифрование.
20. Алгоритмы шифрования.
21. Электронно-цифровая подпись.
22. Алгоритмы электронно-цифровой подписи. Хеширование.
23. Криптоанализ и атаки на криптосистемы.
24. Основные технологии построения защищенных экономических информационных систем.
25. Классы задач защиты информации.
26. Стратегии защиты информации.
27. Индивидуальные параметры вычислительной системы.
28. Алгоритмы привязки программного обеспечения к аппаратному окружению
29. Межсетевые экраны.
30. Атаки на сервера. Атаки на рабочие станции.
31. Протоколирование. Сетевые защищенные протоколы.