

Министерство образования и науки Самарской области  
государственное автономное профессиональное образовательное учреждение  
Самарской области  
«Тольяттинский колледж сервисных технологий и предпринимательства»

УТВЕРЖДАЮ

Директор

ГАПОУ ТКСТП

\_\_\_\_\_ С.В. Дятлов

11 апреля 2022г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ  
ОП.17 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

*общепрофессиональный цикл  
программы подготовки специалистов среднего звена  
по специальности*

*09.02.07 Информационные системы и программирование*

Тольятти, 2022 г.

## **ОДОБРЕНО**

предметной (цикловой) комиссией  
общеобразовательных дисциплин  
технологического направления

Председатель \_\_\_\_\_ Е.Б. Фокина

Протокол № 8 от 04.04.2022 г.

Составитель:

Шайкенова А.Э., преподаватель ГАПОУ ТКСТП

Рабочая программа учебной дисциплины разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки РФ № 1547 от 09.12.2016г.;
- акта согласования вариативной составляющей 2022г. по специальности 09.02.07 Информационные системы и программирование.

## **СОДЕРЖАНИЕ**

<b>1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>стр. 4</b>
<b>2.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>6</b>
<b>3.УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>10</b>
<b>4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ</b>	<b>12</b>

# **1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.17 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

## **1.1. Область применения программы**

Рабочая программа учебной дисциплины (далее программа УД) – является частью программы подготовки специалистов среднего звена (ППССЗ) по специальности 09.02.07 Информационные системы и программирование, разработанной в ГАПОУ ТКСТП, разработанной в соответствии с ФГОС СПО.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке.

## **1.2. Место дисциплины в структуре основной профессиональной образовательной программы**

Учебная дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина, изучается за счет часов вариативной части.

Учебная дисциплина имеет практическую направленность и междисциплинарные связи с общепрофессиональными дисциплинами: ОП. 01 Операционные системы и среды, ОП.03.Информационные технологии, и ОП.11.Компьютерные сети.

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

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

- *классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;*
- *применять основные правила и документы системы сертификации Российской Федерации;*
- *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;*
- *источники угроз информационной безопасности и меры по их предотвращению;*
- *жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;*
- *современные средства и способы обеспечения информационной безопасности.*

В процессе освоения дисциплины у студентов должны сформироваться общие компетенции (ОК):

ОК.01.Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК.02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК.05.Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК.09.Использовать информационные технологии в профессиональной деятельности.

ОК.10.Пользоваться профессиональной документацией на государственном и иностранном языке.

В процессе освоения дисциплины у студентов должны сформироваться профессиональные компетенции (ПК):

ПК.4.1.Осуществлять установку, настройку и обслуживание программного обеспечения компьютерных систем.

ПК.4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК.6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания.

ПК.6.5. Осуществлять техническое сопровождение, обновление и восстановление данных информационной системы в соответствии с техническим заданием.

ПК 7.2. Осуществлять администрирование отдельных компонент серверов.

ПК.7.3 Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов..

ПК.7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.

ПК.10.1 Обрабатывать статический и динамический информационный контент.

#### **1.4. Количество часов на освоение программы дисциплины:**

Объём образовательной нагрузки обучающегося - 46 часов, в том числе:  
нагрузка во взаимодействии с преподавателем - 40 часов;  
самостоятельной работы студента - 6 часов.

## **2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

### **2.1. Объем учебной дисциплины и виды учебной работы**

<b>Вид учебной работы</b>	<b>Объем часов</b>
<b>Объем образовательной нагрузки</b>	<b>46</b>
<b>Суммарная учебная нагрузка во взаимодействии с преподавателем</b>	<b>40</b>
в том числе:	
теоретическое обучение	24
практические занятия	14
<b>самостоятельная работа</b>	<b>6</b>
Промежуточная аттестация в форме дифференцированного зачёта	<b>2</b>

## 2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Информационная безопасность и уровни ее обеспечения			
Тема 1.1 Понятие "информационная безопасность"	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Введение. Проблема информационной безопасности общества	2	
	Самостоятельная работа №1 Подготовка доклада по одной из тем : Значение информационной безопасности для общества. Выдающиеся личности в истории вычислительной техники; Общество в период развития информатизации;	2	
Тема 1.2. Составляющие информационной безопасности	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Доступность информации. Целостность информации. Конфиденциальность информации	2	
	Самостоятельная работа №2 Подготовка доклада по теме: Основные методы определения объема информации.	2	
Тема 1.3. Система формирования режима информационной безопасности	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Задачи информационной безопасности общества	2	
	Практическая работа №1 Параметры безопасности программы Microsoft Outlook	2	
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Правовые основы информационной безопасности общества. Государственная система обеспечения информационной безопасности.	2	
	Практическая работа № 2 Права на использование директории для определенного пользователя	2	
Раздел 2. Стандарты Информационной безопасности			
Тема 2.1. Стандарты информационной безопасности: "Об-	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4,
	Требования безопасности к информационным системам. Принцип иерархии: класс – семейство – компонент – элемент	2	

щие критерии"	Практическая работа №3 Проверка компьютера на предмет наличия уязвимостей	2	ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
Тема 2.2. Стандарты информационной безопасности распределенных систем	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Сервисы безопасности в вычислительных сетях. Администрирование средств безопасности	2	
	Самостоятельная работа №3 Подготовка доклада по теме: Роль стандартов информационной безопасности	2	
Тема 2.3. Стандарты информационной безопасности в РФ	Содержание учебного материала	2	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ	2	
Тема 2.4. Административный уровень обеспечения информационной безопасности	Содержание учебного материала	2	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Цели, задачи и содержание административного уровня. Политика безопасности и меры противодействия.	2	
Тема 2.5. Классификация угроз "информационной безопасности"	Содержание учебного материала	4	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации	2	
	Практическая работа №4 Разграничение доступа к системам	2	
Раздел 3. Компьютерные вирусы и защита от них			
Тема 3.1. Вирусы как угроза информационной безопасности в РФ	Содержание учебного материала	2	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Компьютерные вирусы и информационная безопасность. Воздействия на программно-аппаратные средства защиты информации. Характерные черты компьютерных вирусов	2	
Тема 3.2. Классификация компьютерных вирусов	Содержание учебного материала	2	ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям	2	
Тема 3.3. Характери-	Содержание учебного материала	8	ОК.01, ОК.02, ОК.05,



<b>стика "вирусоподобных" программ</b>	Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы. Способы заражения программ. Признаки проявления вируса. Методы защиты.	2	ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1
	<b>Практическая работа № 5</b> Исследование реестра, на предмет возможных уязвимостей для вирусов	2	
	<b>Практическая работа № 6</b> Приемы работы с защищенными программами	2	
	<b>Практическая работа № 7</b> Использование брандмауэров	2	
<b>Дифференцированный зачёт</b>		<b>2</b>	
<b>Всего</b>		<b>46</b>	

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ**

#### **3.1. Требования к минимальному материально-техническому обеспечению**

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория "Программного обеспечения и сопровождения компьютерных систем" оснащенная необходимым для реализации программы учебной дисциплины оборудованием, приведенным в п 6.1.2.1 примерной программы по данной специальности.

**Лаборатория «Программного обеспечения и сопровождения компьютерных систем»:**

- Автоматизированные рабочие места на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;) или аналоги;
- Автоматизированное рабочее место преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб;)или аналоги;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения

#### **3.2. Информационное обеспечение обучения.**

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе

##### **3.2.1. Печатные издания**

1. Клейменов С.А., Мельников В.П. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. Гриф МО РФ. 7-е изд. - М.: Издательство: Академия, 2012. – 336 с.

**Дополнительные источники:**

1. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие – М.: Финансы и статистика, 2005. – 176 с.
2. С. П. Расторгуев Основы информационной безопасности – М.: Академия, 2007. – 192 с.
3. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности – М.: Горячая Линия – Телеком, 2006. – 544 с.
4. Цирлов В.Л. Основы информационной безопасности: краткий курс/Профессиональное образование. – М.: Феникс, 2008. – 400 с.

**Интернет-ресурсы:**

- 1) <http://fcior.edu.ru/> - Федеральный центр информационно- образовательных ресурсов
- 2) <http://www.edu.ru/> - Федеральные образовательные ресурсы
- 3) [http:// www.adinf.ru/](http://www.adinf.ru/) – Web-сайт разработчиков антивируса ADinf.
- 4) [http:// www.dials.ru/](http://www.dials.ru/) – сервер антивирусной лаборатории.
- 5) [http:// www.symantec.ru](http://www.symantec.ru) – Российское интернет-представительство компании Symantec, производящей антивирусный пакет Norton AntiVirus.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	Формируемые общие и профессиональные компетенции	Формы и методы контроля и оценки результатов обучения
<p>Уметь</p> <ul style="list-style-type: none"> <li>- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;</li> <li>- применять основные правила и документы системы сертификации Российской Федерации;</li> <li>- классифицировать основные угрозы безопасности информации;</li> </ul> <p>Знать</p> <ul style="list-style-type: none"> <li>- сущность и понятие информационной безопасности, характеристику ее составляющих;</li> <li>- место информационной безопасности в системе национальной безопасности страны;</li> <li>- источники угроз информационной безопасности и меры по их предотвращению;</li> <li>- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;</li> <li>- современные средства и способы обеспечения информационной безопасности.</li> </ul>	<p>ОК.01, ОК.02, ОК.05, ОК.09, ОК.10, ПК.4.1, ПК.4.4, ПК.6.4, ПК.6.5, ПК.7.2, ПК.7.3, ПК.7.5, ПК.10.1</p>	<p>Оценка результатов деятельности обучающихся при выполнении и защите результатов практических занятий, тестировании, внеаудиторной самостоятельной работы, других видов текущего контроля.</p> <p>Оценка результатов деятельности обучающихся при выполнении и защите результатов практических занятий, тестировании, внеаудиторной самостоятельной работы, и других видов текущего контроля.</p>