

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский экономический университет имени Г.В. Плеханова»

(Техникум Пермского института (филиала) РЭУ им. Г.В. Плеханова)

РАБОЧАЯ ПРОГРАММА

учебной дисциплины	<u>ОП.17 Информационная безопасность</u>
код, специальность	<u>09.02.04 Информационные системы (по отраслям)</u>
образовательная база подготовки	Среднее общее образование
форма обучения	очная


Пермь, 2020

СОГЛАСОВАНА:

Цикловой методической комиссией гуманитарных, социально -экономических, естественнонаучных и общепрофессиональных дисциплин техникума Пермского института (филиала) РЭУ имени Г.В. Плеханова


Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования по специальности **09.02.04 Информационные системы (по отраслям)** для квалификации – **техник по информационным системам**

Протокол № 2
от «12» сентября 2020года

Председатель цикловой методической комиссии  / Чернавина Т.В. /

УТВЕРЖДЕНА:

Заместитель директора по учебно-воспитательной работе

 / В.Н. Яковлев/

Составитель (автор):

Серебрякова Н.А., преподаватель техникума Пермского института (филиала) РЭУ им. Г.В. Плеханова

Рецензент:

Шестаков А.П., кандидат пед.наук, доцент кафедры информатики и вычислительной техники ФГ БОУ ВО « Пермский государственный гуманитарно-педагогический университет» (ПГГПУ)

СОДЕРЖАНИЕ

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

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.17 Информационная безопасность является частью рабочей программы подготовки специалистов среднего звена в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям)

1.2. Место дисциплины в структуре ППССЗ

Учебная дисциплина ОП.17 Информационная безопасность входит в блок общепрофессиональных дисциплин профессионального цикла учебного плана по специальности 09.02.04 Информационные системы (по отраслям)

1.3. Цели и задачи учебной дисциплины - требования к результатам освоения дисциплины:

В ходе изучения дисциплины ставится задача формирования следующих компетенций:

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.

ОК5.Использовать информационно-коммуникационные технологии в профессиональной деятельности.

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

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

ПК 1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК 1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.1. Участвовать в разработке технического задания.

ПК 2.2. Программировать в соответствии с требованиями технического задания.

ПК 2.6. Использовать критерии оценки качества и надежности функционирования информационной системы.

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

- правильно проводить анализ угроз информационной безопасности;
- выполнять основные этапы решения задач информационной безопасности;
- применять на практике основные общеметодологические принципы теории информационной безопасности.

В результате освоения дисциплины обучающийся должен
знать:

- терминологию в области информационной безопасности;
- машинно-независимые свойства операционных систем;
- методы нарушения конфиденциальности;
- целостности и доступности информации;

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов
Максимальная учебная нагрузка (всего)	114
Обязательная аудиторная учебная нагрузка (всего)	80
В том числе:	-
лекции	51
практические занятия	28
Самостоятельная работа обучающегося (всего)	24
консультация	10
Итоговая аттестация в форме дифференцированного зачета	

2.3. Тематический план и содержание учебной дисциплины ОП.17 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
ВВЕДЕНИЕ	Лекция № 1. Общие проблемы безопасности. Роль и место информационной безопасности.	2	1
Раздел 1. Безопасность и управление доступом в информационных системах.		36	
Тема 1.1. Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности	Содержание учебного материала	4	
	Лекция № 2 Основные предметные направления защиты информации.	2	1
	Лекция № 3 Основные предметные направления защиты информации.	2	1
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Комплексный подход к обеспечению безопасности», «Объект защиты информации»	4	2
Тема 1.2. Информационные, программно – математические, физические и организационные угрозы системы	Содержание учебного материала	4	
	Лекция № 4 Понятие угрозы защиты информации, источники угроз.	2	1
	Лекция № 5. Понятие угрозы защиты информации, источники угроз.	2	1
	Практическая работа №1	2	2
	Угрозы информации в ЭВМ.	2	
	Практическая работа №2.	2	2
	Угрозы информации в ЭВМ.	2	
	Практическая работа № 3.	2	2
	Классификация угроз и их характеристики.	2	2
	Практическая работа № 4.	2	
	Функции и задачи защиты информации.	2	
	Практическая работа № 5,	2	
	Угроза безопасности информации в компьютерных системах.	2	
	Практическая работа № 6.	2	
	Угроза безопасности информации в компьютерных системах.	2	
Тема 1.3. Защита от несанкционированного доступа, модели, и основные принципы защиты информации.	Содержание учебного материала	4	
	Лекция № 6. Функции и задачи защиты информации.	2	1
	Лекция № 7. Методы и системы защиты информации.	2	1
	Практическая работа № 7.	2	2
	Основные свойства защищаемой информации.	2	2

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
	Практическая работа № 8.	2	2
	Методы и средства защиты информации от традиционных шпионажей и диверсий.	2	
	Практическая работа № 9	2	
	Методы и средства защиты информации от электромагнитных излучений и наводок.	2	
	Практическая работа № 10.	2	
	Методы и средства защиты информации от электромагнитных излучений и наводок.	2	
	Консультация студентов	2	
Раздел 2. Организация безопасности в автоматизированных информационных системах АИС.		22	
Тема 2.1. Понятие клиента прав доступа, групп, паролей, политики безопасности в современных АИС.	Содержание учебного материала	4	
	Лекция № 8. Элементы и объекты защиты информации в АИС. Угрозы безопасности информации.	2	1
	Лекция № 9. Методы подтверждения подлинности пользователей и разграничение доступа к компьютерным ресурсам.	2	1
	Практическая работа № 11.	2	
	Цели защиты информации в АИС. Информационные, программно-математические, физические и организационные угрозы.	2	2
	Практическая работа №12.	2	
	Обеспечение и поддержка целостности и согласованности данных в АИС. Основные цели политики безопасности современных АИС.	2	2
	Самостоятельная работа обучающихся	2	
	написание рефератов, докладов на темы: «Методы и приемы обеспечения безопасности информации в АИС», «Политика безопасности АИС».	2	2
Тема 2.2. Принципы организации равноуровневого доступа в АИС.	Содержание учебного материала	12	
	Лекция № 10 Принципы организации равноуровневого доступа в АИС.	2	1
	Лекция № 11. Принципы организации равноуровневого доступа в АИС.	2	1
	Лекция № 12 Способы защиты.	2	1
	Лекция № 13. Способы защиты.	2	1
	Лекция № 14 Разграничение и управление доступом к элементам защищаемой информации.	2	1
	Лекция № 15. Разграничение и управление доступом к элементам защищаемой информации	2	1
	Консультация студентов	2	

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Раздел 3. Защита от компьютерных вирусов.		16	
Тема 3.1. Проблема вирусного заражения программ.	Содержание учебного материала	6	
	Лекция № 16 Классификация вирусов.	2	1
	Лекция № 17. Классификация вирусов.	2	1
	Лекция № 18. Вред наносимый информации компьютерными вирусами.	2	1
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Классификация компьютерных вирусов и их характеристики», «Методы поиска вирусов», «Группировки компьютерных вирусов по особенностям их алгоритма», «Методы защиты от вирусов», «Профилактика заражения вирусами компьютерных систем».	4	2
Тема 3.2. Структура современных антивирусных программ и перспективные методы антивирусной защиты.	Содержание учебного материала	4	
	Лекция № 19. Структура современных антивирусных программ.	2	1
	Лекция № 20. Методы борьбы с компьютерными вирусами.	2	
	Практическая работа № 13.	2	2
	Методы борьбы с компьютерными вирусами	2	
Раздел 4. Защита от утечки информации по техническим причинам.		18	
Тема 4.1. Безопасность компьютерных сетей	Содержание учебного материала	4	1
	Лекция № 21. Элементы сети.	2	
	Лекция № 22. Возможности угрозы целостности информации сети	2	
	Практическая работа №14	2	2
	Защита информации в компьютерных сетях.	2	
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Политика безопасности работы в Интернете», «Требования к защищенности КС от несанкционированного изменения структур», «Система разграничения доступа к информации в КС», «Меры технологической безопасности информации в вычислительных сетях».	4	
Тема 4.2. Программные и технические средства защиты информации в	Содержание учебного материала	4	
	Лекция № 23. Программные и технические средства защиты информации в сети.	2	1
	Лекция № 24. Программные и технические средства защиты информации в сети.	2	1
	Самостоятельная работа обучающихся	4	2

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
сети.	написание рефератов, докладов на темы: «Криптографические методы защиты информации», «Модели и системы криптографической защиты информации».		
Раздел 5. Организационно- правовое обеспечение информационной безопасности.		6	
Тема 5.1. Правовые основы защиты информации.	Содержание учебного материала	4	
	Лекция № 25 Правовые основы защиты информации.	2	1
	Лекция № 26. Правовые основы защиты информации.	2	1
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Правовые и законодательные меры по защите информации», «Административные и организационные мероприятия информационной безопасности».	2	2
	Консультация студентов	6	
Всего		114	

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 УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация профессиональной дисциплины предполагает наличие учебного кабинета Информационных технологий.

Оборудование учебных кабинетов и рабочих мест кабинетов:

- технические средства обучения (компьютер, средства отображения информации, проектор, экран, монитор, ТВ и т.д.), с соответствующим программным обеспечением;
- наглядные пособия (плакаты, презентации);
- комплект учебно-методической документации.

Оборудование лабораторий и рабочих мест лабораторий:

- технические средства обучения;
- персональный компьютер;
- принтер;
- сканер;
- копировальный аппарат;
- факсимильный аппарат;
- средства хранения документов;
- телефонный аппарат;
- комплект учебно-методической документации;
- соответствующее программное обеспечение.

3.2. Информационное обеспечение обучения

	Основные источники
1	Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 416 с. — (Среднее профессиональное образование). — ISBN 978-5-16-101207-9. — Текст : электронный. — URL: https://znanium.com/catalog/product/1009605
2	Информационная безопасность : учебник / Мельников В.П. под ред., Куприянов А.И. Москва : КноРус, 2020. — 267 с. — (СПО). — ISBN 978-5-406-07382-7. — URL: https://book.ru/book/932059
	Дополнительные источники
3	Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 432 с. — (Среднее профессиональное образование). — ISBN 978-5-16-101302-1. — Текст : электронный. — URL: https://znanium.com/catalog/product/1081318
4	Баранова, Е. К. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. Москва : РИОР : ИНФРА-М, 2019. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4 . - ISBN 978-5-16-107531-9. - Текст : электронный. — URL: https://znanium.com/catalog/product/1014830
5	Прокушев, Я.Е. Информационная безопасность : практикум / Я.Е. Прокушев. Санкт-Петербург : ИЦ «Интермедия», 2018. — 288 с. : ил. — Библиогр.: с. 282-283. — ISBN 978-5-4383-0168-4 ; То же [Электронный ресурс]. — URL: http://biblioclub.ru/index.php?page=book&id=482805
6	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/449548
7	Зверева, В. П. Участие в планировании и организации работ по обеспечению защиты информации: учебник / В.П. Зверева, А.В. Назаров. Москва: КУРС:

	ИНФРА-М, 2020. — 320 с. — ISBN 978-5-16-105204-4. — Текст : электронный. — URL: https://new.znanium.com/catalog/product/1055808
8	Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). — ISBN 978-5-16-104336-3. — Текст : электронный. — URL: https://new.znanium.com/catalog/product/1082470
	Профессиональные базы данных, информационно-справочные системы
9	Научная электронная библиотека www.elibrary.ru
10	Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии http://window.edu.ru/catalog/?p_rubr=2.2.75.6
11	on-line библиотека свободно доступных материалов по информационным технологиям на русском языке http://citforum.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Образовательное учреждение, реализующее подготовку по учебной дисциплине, обеспечивает организацию и проведение промежуточной аттестации и текущего контроля индивидуальных образовательных достижений – демонстрируемых обучающимися знаний, умений и навыков.

Формы и методы промежуточной аттестации и текущего контроля по учебной дисциплине самостоятельно разрабатываются образовательным учреждением и доводятся до сведения обучающихся не позднее начала двух месяцев от начала обучения.

Текущий контроль проводится **в процессе проведения всех видов занятий, в соответствии с тематическим планом.**

Обучение по учебной дисциплине завершается промежуточной аттестацией в форме **дифференцированного зачета.**

Фонды оценочных средств (ФОС) разрабатываются образовательным учреждением. Они включают в себя педагогические контрольно-оценочные материалы, предназначенные для определения соответствия (или несоответствия) индивидуальных образовательных достижений основным показателям результатов подготовки (таблицы).

Результаты (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки
Уметь	
- правильно проводить анализ угроз информационной безопасности	Выполнение заданий практических работ 1-3, итоговое тестирование Устный опрос, самостоятельные работы по теме 1.2
- выполнять основные этапы решения задач информационной безопасности	Оценка выполнения заданий практических работ 4-5, итоговое тестирование Устный опрос, самостоятельные работы по теме 2.1
- применять на практике основные общеметодологические принципы теории информационной безопасности.	Оценка выполнения заданий практических работ № 6-7, 8-9 Итоговое тестирование
ЗНАТЬ	
- терминологию в области информационной безопасности	Оценка выполнения заданий Устный опрос. Ответы на итоговое тестирование
– машинно-независимые свойства операционных систем	Устный опрос. Ответы на итоговое тестирование
– методы нарушения конфиденциальности	Оценка выполнения заданий. Устный опрос. Ответы на итоговое тестирование

- Методы целостности и доступности информации	Оценка выполнения заданий Устный опрос Ответы на итоговое тестирование Самостоятельные работы
---	---

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Качественная оценка индивидуальных образовательных достижений	вербальный аналог
более 85	отлично
от 71 до 84	хорошо
от 55 до 70	удовлетворительно
менее 54	неудовлетворительно

Разработчик:

Серебрякова Н.А., преподаватель техникума Пермского института (филиала) Российского экономического университета имени Г.В. Плеханова