МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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 **ОП.18 Информационная безопасность**

код, специальность **09.02.04 Информационные системы (по отраслям)**

Образовательная база подготовки **основное общее образование**

форма обучения **очная**

Пермь, 2018

СОГЛАСОВАНА:
Цикловой методической комиссией гуманитарных, социальных, экономических, естественных и научных дисциплин техникума ПИ (ф) РЭУ им. Г.В. Плеханова

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
09.02.04 Информационные системы (по отраслям)

Протокол № 1
от «12» сентября 2018 года

Председатель цикловой методической комиссии
_____ /Чернавина.Т.В./

Заместитель директора по учебно-воспитательной работе
_____ /Яковлев В.Н./

Составитель (автор): Серебрякова Н.А. преподаватель ПИ (ф) РЭУ им. Г.В. Плеханова

Рецензент: Шестаков А.П., к.пед.н., доцент кафедры информатики и вычислительной техники ФГБОУ ВО «Пермский государственный гуманитарно-педагогический университет» (ПГГПУ)

СОДЕРЖАНИЕ

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ 4
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ.....7
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 16
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....19

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.18 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), квалификация:, техник по информационным системам

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.18 Информационная безопасность входит в профессиональный цикл общепрофессиональных дисциплин 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 ставиться задача формирования следующих компетенций:

ОК1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК5.Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК1.2. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

ПК1.10. Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК2.1. Участвовать в разработке технического задания.

ПК2.2. Программировать в соответствии с требованиями технического задания.

ПК2.6. Использовать критерии оценки качества и надежности функционирования информационной системы

В результате освоения дисциплины обучающийся должен

уметь:

- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации.

В результате освоения дисциплины обучающийся должен

знать:

- источники возникновения информационных угроз;
- модели и принципы защиты информации от несанкционированного доступа;
- методы антивирусной защиты информации;
- состав и методы организационно-правовой защиты информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количествочасов
Максимальная учебная нагрузка (всего)	78
Обязательная аудиторная учебная нагрузка (всего)	54
В том числе:	-
лекции	40
практические занятия	14
Самостоятельная работа обучающегося (всего)	24
Итоговая аттестация в форме **дифференцированного зачета**	

2.3. Тематический план и содержание учебной дисциплины ОП.18 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
	Лекция № 1. Общие проблемы безопасности. Роль и место информационной безопасности.	**2**	**1**
Раздел 1. Безопасность и управление доступом в информационных системах.		**26**	
Тема 1.1. Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности.	**Содержание учебного материала**	**4**	**1**
	Лекция № 2. Основные предметные направления защиты информации.	2	
	Лекция № 3. Основные предметные направления защиты информации.	2	
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Комплексный подход к обеспечению безопасности», «Объект защиты информации»	**4**	
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
	Практические занятия	**6**	
	Практическое занятие №1. Угрозы информации в ЭВМ.	2	
	Практическое занятие № 2. Классификация угроз и их характеристики. Функции и задачи защиты информации.	2	
	Практическое занятие № 3. Угроза безопасности информации в компьютерных системах.	2	
Тема 1.3. Защита от несанкционированного доступа, модели, и основные принципы защиты информации.	**Содержание учебного материала**	**6**	
	Лекция № 6. Функции и задачи защиты информации.	2	**1**
	Лекция № 7. Функции и задачи защиты информации.	2	
	Лекция № 8. Методы и системы защиты информации.	2	
	Практические занятия		
	Практическое занятие № 4. Основные свойства защищаемой информации. Методы и средства защиты информации от традиционных шпионажей и диверсий.	**1**	
	Практическое занятие № 5. Методы и средства защиты информации от электромагнитных излучений и наводок.	**1**	
Раздел 2. Организация безопасности в автоматизированных информационных системах АИС.		**16**	
Тема 2.1. Понятие	**Содержание учебного материала**	**4**	

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
клиента прав доступа, групп, паролей, политики безопасности в современных АИС.	**Лекция № 9.** Элементы и объекты защиты информации в АИС. Угрозы безопасности информации.	2	**1**
	Лекция № 10. Методы подтверждения подлинности пользователей и разграничение доступа к компьютерным ресурсам.	2	
	Практические занятия		
	Практическое занятие № 6. Цели защиты информации в АИС. Информационные, программно-математические, физические и организационные угрозы.	**1**	
	Практическое занятие №7. Обеспечение и поддержка целостности и согласованности данных в АИС. Основные цели политики безопасности современных АИС.	**1**	
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Методы и приемы обеспечения безопасности информации в АИС», «Политика безопасности АИС».	**4**	
Тема 2.2. Принципы организации равноуровнего доступа в АИС.	**Содержание учебного материала**	**6**	
	Лекция № 11. Принципы организации разноуровневого доступа в АИС.	2	1
	Лекция № 12. Способы защиты.	2	1
	Лекция №13. Разграничение и управление доступом к элементам защищаемой информации.	2	1
Раздел 3. Защита от компьютерных вирусов.		**14**	
Тема 3.1. Проблема вирусного заражения программ.	**Содержание учебного материала**	**4**	
	Лекция № 14. Классификация вирусов.	2	1
	Лекция № 15. 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**	
Тема 3.2. Структура современных антивирусных программ и перспективные методы антивирусной защиты.	**Содержание учебного материала**	**4**	
	Лекция № 16. Структура современных антивирусных программ.	2	**1**
	Лекция № 17. Методы борьбы с компьютерными вирусами.	2	
	Практические занятия	**2**	
	Практическое занятие № 8-9. Методы борьбы с компьютерными вирусами		

Наименование разделов и тем	Содержание учебного материала, практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Раздел 4. Защита от утечки информации по техническим причинам.		**14**	
Тема 4.1. Безопасность компьютерных сетей	**Содержание учебного материала**		**1**
	Лекция № 18. Элементы сети. Возможности угрозы целостности информации сети	2	
	Практические занятия		
	Практическое занятие №10. Защита информации в компьютерных сетях.	**2**	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 сети.	**Содержание учебного материала**	**2**	
	Лекция № 19. Программные и технические средства защиты информации в сети.		**1**
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Криптографические методы защиты информации», «Модели и системы криптографической защиты информации».	**4**	
Раздел 5. Организационно правовое обеспечение информационной безопасности.		**6**	
Тема 5.1. Правовые основы защиты информации.	**Содержание учебного материала**	**2**	
	Лекция № 20. Правовые основы защиты информации.		1
	Самостоятельная работа обучающихся написание рефератов, докладов на темы: «Правовые и законодательные меры по защите информации», «Административные и организационные мероприятия информационной безопасности».	**4**	2
Всего		**80**	

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

№ п/п	Наименование учебных изданий, Интернет -ресурсов, дополнительной литературы
	Основные источники
1	Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова.
2	Петренко, С. А. Аудит безопасности Intranet [Электронный ресурс] / С. А. Петренко, А. А. Петренко.
3	Шаньгин, В. Ф.Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин.
	Дополнительные источники
4	Байбурин В.Б., Бровков М.Б., Пластун И.Л. Введение в защиту информации: учебное пособие – М: Инфра-М, 2007
5	Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А./ Основы информационной безопасности/М.: Телеком – Горячая линия, 2007
6	Домарев В.В./ Безопасность информационных технологий(системный подход)/ Диасофт, 2009
7	Воронцова Л.В., Фролов Л.Б./ История и современность современного противоборства/ Горячая линия – телеком, 2009
8	Лукацкий А.В./ Обнаружение атак/ СПб: БХВ, 2007
9	Манойло А.В., Петренко А.И., Фролов Д.Б./Государственная информационная политика в условиях информационно-психологической войны/ М.: Горячая линия – Телеком, 2007
10	Мельников В.В. Безопасность информации в автоматизированных системах – М: Финансы и статистика, 2008
11	Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008

12	Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие – М.:ФОРУМ: ИНФА – М, 2008. – 386 с.: ил.
13	Петренко С.А., Курбатов В.А./Политики информационной безопасности/ДМК-Пресс, 2009
14	Расторгуев С.П./ Информационная война. Проблемы и модели/ Гелиос АРВ, 2008
15	Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: учебное пособие – СПб: Питер, 2008
16	Стрельцов А.А./ Обеспечение информационной безопасности России/ МЦНМО, 2009
17	Устинов Г.Н. Основы информационной безопасности систем передачи данных: учебное пособие – Б.м. СИНТЕГ, 2008
18	Тихонов В.А., Райх В.В./ Информационная безопасность: концептуальные, правовые, организационные и технические аспекты/ М.: Гелиос – АРВ, 2007
19	Филин С.А. Информационная безопасность: учебное пособие – М: Альфа-Пресс, 2006
20	Ярочкин В.И. Информационная безопасность: учебное пособие – М: Международные отношения, 2007
	Интернет-источники
21	http://std.mesi.ru/exact/Glove/viewer.asp?packId=MANIFEST-AA6B677D-B59D-68EA-9FAF-2E5AD9CDC839
22	http://www.bibliofond.ru/view.aspx?id=565176
23	http://www.k2x2.info/uchebniki/informacija_sbor_zashita_analiz_uchebnik_po_informacionno_analiticheskoi_rabote/p6.ph
24	http://nashol.com/20100513532/osnovi-informacionnoi-bezopasnosti-uchebnoe-posobie-dlya-vuzov-belov-e-b-los-v-p-mescheryakov-r-v-shelupanov-a-a-2006.html

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, КОС) 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
Умения	
- 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 выполнение заданий практических работ № 6-7, 8-9 Итоговое тестирование
Знания	
-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)

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
более 85	5	отлично
от 70 до 84	4	хорошо
от 55 до 69	3	удовлетворительно
менее 54	2	неудовлетворительно

Разработчик:
Серебрякова Н.А., преподаватель ПИ (ф) РЭУ им. Г.В. Плеханова