Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

РАБОЧАЯ ПРОГРАММА

учебной дисциплины **ОП.10 Информационная безопасность**

код, специальность **09.02.03 Программирование в компьютерных системах**

квалификация: **техник-программист**

форма обучения: очная

Москва
2018

СОГЛАСОВАНА:
Предметной комиссией
Общепрофессиональных дисциплин (программное обеспечение)

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
09.02.03 Программирование в компьютерных системах
Квалификация: техник-программист

Протокол № 1-17/18 ЗК

от «28» августа 2017г

Председатель предметной (цикловой) комиссии

Г.Ю. Волкова
Подпись Инициалы Фамилия

Заместитель директора по учебной работе

Д.А. Клопов
Подпись Инициалы Фамилия

УТВЕРЖДЕНА:

Директор техникума

А.В. Чурилов
Подпись Инициалы Фамилия

Составители (авторы): А.С. Дубовик, преподаватель ФГБОУ ВО "РЭУ им. Г.В.Плеханова"

Лист актуализации

рабочей программы учебной дисциплины

В рабочую программу учебной дисциплины на 2018/19 уч. год внесены следующие изменения:

1. На основании Указа Президента РФ от 15.01.2018 года №215 на титульном листе исправлено Министерство образования и науки Российской Федерации на Министерство науки и высшего образования Российской Федерации

Дата актуализации: 30.08.2018 г

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена по специальности 09.02.03 «Программирование в компьютерных системах».

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы: общепрофессиональная дисциплина профессионального цикла

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

В результате освоения учебной дисциплины обучающийся должен

уметь:

- анализировать угрозы информационной безопасности;
- анализировать угрозы сетевой безопасности;
- анализировать трафик, циркулирующий по каналам связи;
- составлять политику безопасности;
- использовать системы и алгоритмы криптографической защиты;
- использовать системы и алгоритмы электронно-цифровой подписи (ЭЦП);
- использовать системы и алгоритмы идентификации, аутентификации и авторизации;
- обеспечивать безопасность операционных систем;
- работать с межсетевыми экранами и защищёнными сетями VPN;
- обеспечивать безопасность на всех уровнях модели OSI;

знать:

- основные понятия информационной безопасности;
- основные правовые законы информационной безопасности;
- доктрину информационной безопасности Российской Федерации;
- модель ISO/OSI и стек протоколов TCP/IP;
- семантику основных протоколов прикладного уровня;
- проблемы безопасности IP сетей;
- угрозы и уязвимости проводных и беспроводных сетей;
- стандарты информационной безопасности сетей;
- основные понятия политики безопасности;
- структуру политики безопасности, базовые и специализированные политики безопасности, процедуры безопасности;
- основные понятия криптографической защиты информации;
- симметричные и асимметричные криптосистемы шифрования;
- комбинированные криптосистемы шифрования;
- электронно-цифровую подпись и функцию хеширования;
- управление криптоключами;
- классификацию криптографических алгоритмов;
- симметричные и блочные алгоритмы шифрования данных;
- асимметричные алгоритмы шифрования данных, алгоритмы цифровой подписи;

- методы аутентификации;
- проблемы обеспечения безопасности операционных систем;
- угрозы безопасности операционных систем, понятие защищенной операционной системы
- функции межсетевых экранов;
- виртуальные защищенные сети VPN;
- особенности функционирования межсетевых экранов и виртуальных защищенных сетей на различных уровнях модели OSI;
- основы защиты на различных уровнях моделей OSI;
- основные технологии обнаружения вторжений.

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.
ПК 2.3. Решать вопросы администрирования базы данных.
ПК 2.4. Реализовывать методы и технологии защиты информации в базах данных.

1.4. Рекомендуемое количество часов на освоение программы дисциплины:

Максимальная учебная нагрузка обучающего	117	часов
Включая:		
Обязательная аудиторная нагрузка	78	часов
Самостоятельная работа	9	часов
Консультации	30	часов
ВСЕГО	**117**	**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)	**117**
Обязательная аудиторная учебная нагрузка (всего)	**78**
В том числе:	
практические занятия	20
Самостоятельная работа обучающегося (всего)	**39**
в том числе:	
тематика внеаудиторной самостоятельной работы	9
консультации	30
Итоговая аттестация 6 семестр – другие формы контроля 7 семестр - экзамен	

2.2. Тематический план и содержание учебной дисциплины ОП.10 «Информационная безопасность»

Наименование тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Тема 1. Введение.	Информационная безопасность. Основные понятия. Виды защищаемой информации.	2	1
	Модели информационной безопасности. Виды защищаемой информации.	2	
	Самостоятельная работа Основные модели информационной безопасности	2	
Тема 2. Правовое обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Федеральное законодательство.	2	2
	Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны	2	
	Самостоятельная работа Анализ угроз информационной безопасности и их;	2	
Тема 3. Вредоносное программное обеспечение, защита от вредоносного ПО	Вредоносное ПО. Классификация вредоносного ПО.	2	1
	Методы защиты от вредоносного ПО. Антивирусные программы	2	
	Практическая работа «Работа с антивирусными пакетами»	2	
	Самостоятельная работа Сравнительные характеристики антивирусного ПО	2	
Тема 4. Проблемы информационной безопасности сети	Введение в сетевой информационный обмен. Использование сети Internet и Ethernet.	2	2
	Модели ISO/OSI и стек протоколов TCP/IP	2	
	Анализ угроз сетевой безопасности	2	
	Обеспечение информационной безопасности сетей.	2	
	Практическая работа «Анализ циркулирующего трафика в сети» «Обеспечение информационной безопасности локальной сети»	4	
	Самостоятельная работа	8	

	Стандарты информационной безопасности сетей Проблемы безопасности IP сетей. Угрозы и уязвимости проводных и беспроводных сетей		
Тема 5. Политика безопасности	Основные понятия политики безопасности	2	2
	Структура политики безопасности. Базовые и специализированные политики безопасности. Процедуры безопасности.	2	
	Основные стандарты информационной безопасности.	2	
	Практическая работа «Разработка политики безопасности»	4	
	Самостоятельная работа ГОСТ Р ИСО/МЭК 17799-2005	2	
Тема 6. Принципы криптографической защиты информации	Основные понятия криптографической защиты информации	2	2
	Симметричные и асимметричные криптосистемы шифрования	2	
	Комбинированная криптосистема шифрования	2	
	Электронная цифровая подпись Хеширование. Управление криптоключами.	2	
	Самостоятельная работа Метод распределения ключей Диффи-Хеллмана	4	
Тема 7. Криптографические алгоритмы	Классификация криптографических алгоритмов. Симметричные и блочные алгоритмы шифрования данных	2	2
	Асимметричные алгоритмы шифрования данных. Алгоритмы цифровой подписи	2	
	Практическая работа «Реализация системы шифрования»	4	
	Самостоятельная работа Подготовка к практической работе	2	
Тема 8. Технологии аутентификации	Методы аутентификации, использующие пароли и PIN-коды	2	2
	Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах	2	
	Практическая работа «Разработка системы аутентификации»	4	
	Самостоятельная работа	4	

	Подготовка к практической работе		
Тема 9. Обеспечение безопасности операционных систем	Проблемы обеспечения безопасности операционных систем.	2	2
	Угрозы безопасности операционных систем. Понятие защищенной операционной системы.	2	
	Архитектура подсистемы защиты операционной системы.	2	
	Самостоятельная работа Безопасность NT систем при обмене данных. Обеспечение безопасности хранения данных в ОС Microsoft	2	
Тема 10. Технологии межсетевых экранов. Виртуальные защищенные сети	Функции межсетевых экранов.	2	2
	Виртуальные защищенные сети VPN	2	
	Особенности функционирования межсетевых экранов и виртуальных защищенных сетей на различных уровнях модели OSI	2	
	Самостоятельная работа Настройка VPN оборудования	2	
Тема 11. Технология электронной подписи	Назначение и применение электронных подписей в IT	2	2
	Подделка подписей. Управление ключами	2	
	Практическая работа «Создание электронной подписи в Microsoft Outlook»	2	
	Самостоятельная работа Социальные атаки Подготовка к практической работе	5	
Консультации	Перехват TCP/UDP пакетов в проводных и беспроводных сетях	2	2
	Биометрическая аутентификация	2	
	Всего:	117	

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 ОП.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной дисциплины требует наличия Лаборатории информационно-коммуникационных систем

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	Парты 12 шт	проектор 1 шт	15
2	стулья 40 шт	компьютер 15 шт	
3	доска маркерная		
4	стол преподавателя 1 шт •		
5	шкаф 4 шт •		

Программное обеспечение:

Androind Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition, Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

3.2. Информационное обеспечение обучения

Печатные издания не используются. Дисциплина полностью обеспечена электронными изданиями.

№ п/п	Наименование учебных изданий, Интернет-ресурсов, дополнительной литературы
I	**Основные источники**
1.1	Т. Л. Партыка, И. И. Попова «Информационная безопасность» (5-е издание) Москва, Издательство «Форум: НИЦ ИНФРА-М» 2018. Режим доступа: http://www.znanium.com/bookread.php?book=420047
1.2	В. Ф. Шаньгин, «Информационная безопасность компьютерных систем и сетей» (учебное пособие) Москва, Издательство «Форум: НИЦ ИНФРА-М» 2014. Режим доступа: http://www.znanium.com/bookread.php?book=335362book=335362
1.3	Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2017. Режим доступа: http://http://http://znanium.com/bookread2.php?book=882007 В. Г. Спицын «Информационная безопасность вычислительной техники» (учебное пособие) Томск, Издательство «Эль Контент» 2011. Режим доступа: http://biblioclub.ru/index.php?page=book&id=208694&sr=1
1.4	Е.В. Глинская, Н.В. Чичварин Информационная безопасность конструкций ЭВМ и систем. — М. : ИНФРА-М, 2018 Режим доступа: http://znanium.com/bookread2.php?book=925825
II	**Дополнительные источники**
2.1	Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016 Режим доступа: http://znanium.com/bookread2.php?book=544554
2.2	Программно-аппаратные средства обеспечения информационной безопасно-

	сти: Учебное пособие для вузов / Душкин А.В., Барсуков О.М., Кравцов Е.В. - М.:Гор. линия-Телеком, 2016 Режим доступа: http://znanium.com/ bookread2.php?book=973806
2.3	В. Ф. Шаньгин «Защита информации в компьютерных системах и сетях» (учебник) Москва, Издательство «ДМК Пресс» 2016. Режим доступа: http:// biblioclub.ru/index.php?page=book&id=231889&sr=1
2.4	В. И. Аверченков, М. Ю. Рытов «Служба защиты информации: организация и управление» (учебное пособие) Москва, Издательство «Флинта» 2015. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93356&sr=1
III	**Электронно библиотечная система (ЭБС)**
3.1	http://znanium.com/
3.2	http://biblioclub.ru
3.3	https://biblio-online.ru/
3.4	https://www.book.ru/
IV	**Профессиональные базы данных и справочные системы**
4.1	Федеральная служба государственной статистики - https://rosstat.gov.ru/
4.2	Наукометрическая и реферативная база данных SCOPUS - https:// www.scopus.com
4.3	Информационно-справочная система "КонсультантПлюс"

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.10 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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.

Текущий контроль проводится преподавателем.

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

Итоговой формой контроля является экзамен

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 обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
– анализировать угрозы информационной безопасности; – анализировать угрозы сетевой безопасности; – анализировать трафик, циркулирующий по каналам связи; – составлять политику безопасности; – использовать системы и алгоритмы криптографической защиты; – использовать системы и алгоритмы электронно-цифровой подписи (ЭЦП);	Устный опрос Наблюдение и оценка результата выполнения практических работ Тестирование Внеаудиторная самостоятельная работа Экзамен

– использовать системы и алгоритмы идентификации, аутентификации и авторизации; – обеспечивать безопасность операционных систем; – работать с межсетевыми экранами и защищёнными сетями VPN; – обеспечивать безопасность на всех уровнях модели OSI;	
Знания:	
– основные понятия информационной безопасности; – основные правовые законы информационной безопасности; – доктрину информационной безопасности Российской Федерации; – модель ISO/OSI и стек протоколов TCP/IP; – семантику основных протоколов прикладного уровня; – проблемы безопасности IP сетей; – угрозы и уязвимости проводных и беспроводных сетей; – стандарты информационной безопасности сетей; – основные понятия политики безопасности; – структуру политики безопасности, базовые и специализированные политики безопасности, процедуры безопасности; – основные понятия криптографической защиты информации; – симметричные и асимметричные криптосистемы шифрования; – комбинированные криптосистемы шифрования; – электронно-цифровую подпись и функцию хеширования; – управление криптоключами; – классификацию криптографических алгоритмов; – симметричные и блочные алгоритмы шифрования данных; – асимметричные алгоритмы шифрования данных, алгоритмы цифровой подписи; – методы аутентификации; – проблемы обеспечения безопасности операционных систем; – угрозы безопасности операционных систем, понятие защищенной операционной системы – функции межсетевых экранов; – виртуальные защищенные сети VPN; – особенности функционирования межсетевых экранов и виртуальных защищенных сетей на различных уровнях модели OSI; – основы защиты на различных уровнях моделей OSI; – основные технологии обнаружения вторжений.	Устный опрос Наблюдение и оценка результата выполнения практических работ Тестирование Внеаудиторная самостоятельная работа Экзамен

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 90	5	отлично
от 70 до 89	4	хорошо
от 50 до 69	3	удовлетворительно
менее 49	2	неудовлетворительно

Разработчик:
Дубовик А.С., преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

Эксперт: