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.14 Информационная безопасность**

код, специальность: **09.02.01 Компьютерные системы и комплексы**

квалификация: **техник по компьютерным системам**

форма обучения: очная

Москва
2018

СОГЛАСОВАНА:
Цикловой методической комиссией «Профессиональных модулей 09.02.01»

Протокол № __1__

от «31» августа 2018 года
Председатель ЦМК

О.Л. Мещеринова
Подпись Инициалы Фамилия

Разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, квалификация техник по компьютерным системам

Заместитель директора по учебной работе

Д.А.Клопов
Подпись

УТВЕРЖДЕНА:

Директор техникума **А.В.Чурилов**
Подпись

Составители (авторы): Мотыльков К.В., преподаватель
ФГБОУ ВО РЭУ имени Г.В. Плеханова
Ф.И.О., ученая степень, звание, должность, наименование ФГБОУ
Московский приборостроительный техникум

Рецензент: Прищеп М.С., преподаватель ФГБОУ ВО РЭУ имени Г.В. Плеханова
Ф.И.О., ученая степень, звание, должность, наименование ФГБОУ

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Программа учебной дисциплины является частью программы подготовки специалистов среднего звена по специальности среднего профессионального образования 09.02.01 Компьютерные системы и комплексы, базовой подготовки

1.2. Место дисциплины в структуре ППССЗ: учебная дисциплина ОП.14 Информационная безопасность входит в общепрофессиональный цикл

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

В результате освоения дисциплины обучающийся должен

уметь:

- выполнять анализ способов нарушения информационной безопасности;
- использовать методы и средства защиты данных;
- применять алгоритмы криптографии;
- пользоваться средствами защиты, предоставляемыми СУБД;
- создавать дополнительные средства защиты;
- проводить анализ и оценивание механизмов защиты;
- выбирать формы и критерии информационной безопасности;
- разрабатывать предложения по совершенствованию политики безопасности.

знать:

- терминологию в сфере безопасности информационного контента;
- понятия политики безопасности, существующие типы политик безопасности;
- существующие стандарты информационной безопасности;
- виды угроз информационной безопасности;
- средства борьбы с угрозами информационной безопасности;
- о современных концепциях безопасности программного обеспечения и баз данных;
- методы защиты информации;
- критерии защищенности программного обеспечения и баз данных;
- угрозы безопасности программного обеспечения и баз данных;
- критерии и методы оценивание механизмов защиты;
- организационно-правовое обеспечение информационной безопасности.

Результатом освоения программы дисциплины является овладение обучающимися профессиональными (ПК) и общими (ОК) компетенциями:

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 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. Разрабатывать схемы цифровых устройств на основе интегральных схем разной степени интеграции.
ПК 1.5. Выполнять требования нормативно-технической документации.
ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов.

1.4. Рекомендуемое количество часов на освоение учебной дисциплины:

Максимальная учебная нагрузка обучающего	96	часов
Включая:		
Обязательная аудиторная нагрузка	64	часа
Самостоятельная работа	28	часов
Консультации	4	часа
ВСЕГО	**96**	**часов**

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем нагрузки учебной дисциплины

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	*96*
Обязательная аудиторная учебная нагрузка (всего)	*64*
в том числе:	
лекционные занятия	*32*
практические занятия	*32*
Самостоятельная работа обучающегося	*28*
Консультации	*4*
Промежуточная аттестация 5 семестр - экзамен	

2.2. Тематический план и содержание тем учебной дисциплины ОП.13 «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Информация как объекта защиты		**14**	
Тема 1.1. Основные виды информационной защиты. Защита человека как собственника информации.	**Содержание учебного материала**	2	1
	Понятие об опасной информации. Виды опасной информации. Способы защиты человека от излишней, назойливой, недобросовестной информации. Вредная информация в формах обмана и злоупотребления доверием. Ценность информации.		
	Самостоятельная работа Формирование прав собственности на информацию.	2	
Тема 1.2. Уровни представления информации и особенности ее защиты**.**	**Содержание учебного материала**	2	1
	Виды и общая характеристика информационных угроз. Уязвимости информационных систем. Виды ущерба от информационных атак. Носители информационных угроз.		
Тема 1.3. Классификация и категории информационных нарушителей.	**Содержание учебного материала**	2	1
	Информационные нарушители. Цели нарушителей. Оценка опасности нарушителя на основании его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя.		
	Практическая работа	4	
	Оценка агентов угроз и угроз		
	Разработка классификации агентов угроз		
	Упорядочивание угроз и механизмов угроз в соответствии с классификацией агентов угроз		
	Оценка вероятности угроз, инициируемых преднамеренными агентами		
	Оценка уязвимости		
	Самостоятельная работа обучающихся	2	
	Создание перечня информационного контента, агентов угроз и угроз на индивидуальном предприятии. Выполнение анализа угроз и уязвимости.		
Раздел 2. Направления информационной защиты		**18**	
Тема 2.1. Нормативно-правовое регулирование защиты информации**.**	**Содержание учебного материала**	2	1
	Характеристика нормативно-правовой защиты. Виды информации по категории доступа. Правовой режим защиты государственной тайны. Правовой режим защиты конфиденциальной информации. Виды конфиденциальной информации и режимы ее защиты. Ответственность за право нарушения в сфере защиты конфиденциальной информации.		

	Самостоятельная работа обучающихся Используя Интернет – ресурсы ознакомиться со статьями 23,24 Конституции РФ, статьями 272, 273, 274, 138, 146, 283, 284 главы 28 Уголовного кодекса РФ.	2	
Тема 2.2. Организационно-распорядительная защита.	**Содержание учебного материала**	2	1
	Работа с кадрами и внутри объектовый режим. Основные принципы организационно-распорядительной защиты: изоляция носителей информации, минимальная информированность исполнителей, производственная дисциплина, регламентация служебного времени, минимизация неслужебных контактов, объединение и разделение полномочий. Формы контроля и надзора за персоналом. Дезинформация и легендирование. Допуск к работе с конфиденциальной информацией. Режим учета и хранения вещественных носителей информации. Права и обязанности системного администратора. Функции подразделений безопасности.		
	Самостоятельная работа обучающихся Используя Интернет – ресурсы ознакомиться Кодексом РФ об административных нарушениях № 195-ФЗ от 30.12.2001 (с изм. и доп. от 4.07.2003), Гражданским кодексом РФ. Часть четвертая, ФЗ «О персональных данных», № 152-ФЗ от 27.07.2006, ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006.	2	
Тема 2.3. Инженерно-техническая защита от физического вторжения.	**Содержание учебного материала**	2	1
	Защита информации от утечки по техническим каналам. Защита от внедрения и использования автономных средств технической разведки. Управление доступом к информации. Защита компьютерных систем от вредоносного программного воздействия. Семантическое скрытие информации. Обеспечение нормальных условий эксплуатации информационных систем и машинных носителей информации.		
	Самостоятельная работа обучающихся Используя Интернет – ресурсы ознакомиться ФЗ «О персональных данных», № 152-ФЗ от 27.07.2006, ФЗ «О связи», № 126-ФЗ от 07.07.2003.	2	
	Практическая работа Определение шагов для формального анализа риска. Определение активов для включения в список при анализе риска. Разработка качественных шкал для оценки активов. Определение значений суммарного влияния для качественного анализа риска.	4	
	Самостоятельная работа	2	
	Создание перечня подразделений безопасности на индивидуальном предприятии. Создание перечня организационно-распорядительных и инженерно-технических мероприятий на индивидуальном предприятии.		
Раздел 3. Методы и средства защиты программного обеспечения		**16**	

Тема 3.1. Описание типовых политик безопасности.	**Содержание учебного материала**	2	1
	Понятие политики безопасности. Модель политики безопасности.		
	Практическая работа	4	
	Оценка политик безопасности		
Тема 3.2. Модель защищенного канала связи.	**Содержание учебного материала**	2	1,2
	Виды информационных угроз для канала связи и передаваемой информации. Незаконное использование канала. Деструктивные действия. Фальсификация передаваемых данных. Подключение к каналу связи своих передатчиков и приемников. Виды перехвата информации в канале связи. Использование побочных каналов утечки информации. Способы защиты передаваемой информации от характерных атак.		
	Самостоятельная работа Технические характеристики устройств(передатчиков и приемников), подключаемых к каналу связи.	2	
Тема 3.3. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.	**Содержание учебного материала**	2	1
	Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.		
Тема 3.4. Угрозы безопасности компьютерных систем.	**Содержание учебного материала**	1	1,2
	Методы и средства ограничения доступа к компонентам вычислительных систем. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы и средства хранения ключевой информации.		
	Самостоятельная работа Создание перечня методов и средств защиты ПО на индивидуальном предприятии.	2	
Тема 3.5. Защита программ	**Содержание учебного материала**	1	1,2
	Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий**.** Защита программ от изменения и контроль целостности.		
Раздел 4. Механизмы обеспечения информационной безопасности программного обеспечения и баз данных		**24**	
Тема 4.1.	**Содержание учебного материала**	1	1,2

Анализ существующих средств и методов защиты программного обеспечения	Классификация системы защиты программного обеспечения по методу установки, по используемым механизмам защиты. Методы для защиты ПО: Алгоритмы запутывания, Алгоритмы мутации, Алгоритмы компрессии данных, Алгоритмы шифрования данных, Вычисление сложных математических выражений в процессе отработки механизма защиты, Методы затруднения дизассемблирования, Нестандартные методы работы с аппаратным обеспечением. Классификация системы защиты по принципу функционирования системы защиты. Достоинства и недостатки методов.		
	Самостоятельная работа Методы затруднения отладки, Эмуляция процессоров и операционных систем. Достоинства и недостатки методов.	2	
	Практическая работа Создание системы защиты ПО, применяя к программному обеспечению алгоритмы мутации.	4	
	Создание системы защиты ПО, применяя к программному обеспечению методы затруднения дизассемблирования.		
Тема 4.2. Классификация угроз конфиденциальности СУБД.	**Содержание учебного материала**	1	1,2
	Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.		
Тема 4.3. Методы противодействия.	**Содержание учебного материала**	1	1,2
	Особенности применения криптографических методов. Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.		
	Самостоятельная работа обучающихся Этапы развития криптографии. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа.	2	
	Практическая работа Создание системы защиты ПО, применяя криптографические методы.	4	
	Модификация системы, разделяя группы пользователей, привилегии, роли и представления информации.		
Тема 4.4. Метки безопасности.	**Содержание учебного материала**	1	1,2
	Использование представлений для обеспечения конфиденциальности информации в СУБД.		

	Самостоятельная работа обучающихся Произвести сравнительный анализ достоинств и недостатков изученных ранее СУБД.	2	
Тема 4.5. Аудит и подотчетность.	**Содержание учебного материала**	1	
	Подотчетность действий пользователя и аудит связанных с безопасностью событий. Журнализация. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.		
Тема 4.6. Оценка эффективности систем защиты	**Содержание учебного материала**	1	1,2
	Набор показателей применимости и критериев оценки систем защиты программного обеспечения. Показатели применимости: Технические, Экономические, Организационные. Критерии оценки: Защита как таковая, Стойкость к исследованию/взлому, Отказоустойчивость (надёжность), Независимость от конкретных реализаций ОС, Совместимость, Неудобства для конечного пользователя ПО, Побочные эффекты, Стоимость, Доброкачественность.		
	Практическая работа Произвести технический, экономический и организационный анализ показателей применимости программного обеспечения отраслевой направленности Произвести оценку критериев системы защиты программного обеспечения отраслевой направленности.	4	
Раздел 5. Обеспечение информационной безопасности компьютерных сетей		**10**	
Тема 5.1. Программно-аппаратные средства защиты информации в сетях передачи данных.	**Содержание учебного материала**	2	1,2
	Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.		
Тема 5.2. Межсетевые экраны.	**Содержание учебного материала**	2	1,2
	Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов.		
	Самостоятельная работа обучающихся Создание перечня систем идентификации и аутентификации на индивидуальном предприятии. Аудит журналов брандмауэра.	2	
	Практическая работа Создание модели политики безопасности индивидуального предприятия на основе собранных данных	4	
Раздел 6. Организационно-правовое обеспечение информационной безопасности		**14**	
Тема 6.1. Правовое	**Содержание учебного материала**	1	1

обеспечение информационной безопасности.	Правовое обеспечение информационной безопасности. Российские документы по защите информации. Организационное обеспечение информационной безопасности		
Тема 6.2. Состав и назначение должностной инструкции.	**Содержание учебного материала**	1	1,2
	Состав и назначение должностной инструкции.		
	Самостоятельная работа обучающихся Методы контроля за исполнением должностных инструкций. Методы и формы организационной защиты информации. Методы организационной защиты информации. Виды перекрытия каналов утечки информации	4	
	Практическая работа Составление должностной инструкции	4	
	Консультации	4	
	Всего:	**96**	

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.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной дисциплины требует наличия Лаборатории информационных технологий

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	Парты 16 шт	проектор	28
2	стулья 28 шт		
3	доска маркерная		
4	стол преподавателя 1 шт		
5	8 автоматизированных рабочих мест учащихся		

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 реализации программы

Печатные издания не используются. Дисциплина полностью обеспечена электронными изданиями.

№ п/п	Наименование учебных изданий, Интернет-ресурсов, дополнительной литературы
I	**Основные источники**
1.1	Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 416 с. — (Профессиональное образование). - Режим доступа: http://znanium.com/catalog/product/775200
1.2	Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. — М.: ИД «ФОРУМ»: ИНФРА-М, 2017. — 592 с. — (Высшее образование: Бакалавриат). - Режим доступа: http://znanium.com/catalog/product/546679
II	**Электронно библиотечная система (ЭБС)**
2.1	http://znanium.com/
2.2	http://biblioclub.ru
2.3	https://biblio-online.ru/
2.4	https://www.book.ru/
III	**Профессиональные базы данных и справочные системы**
3.1	Федеральная служба государственной статистики - https://rosstat.gov.ru/
3.2	Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
3.3	Информационно-справочная система "КонсультантПлюс"

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.14 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:	
- выполнять анализ способов нарушения информационной безопасности; - использовать методы и средства защиты данных; - применять алгоритмы криптографии; - пользоваться средствами защиты, предоставляемыми СУБД; - создавать дополнительные средства защиты; - проводить анализ и оценивание механизмов защиты; - выбирать формы и критерии информационной безопасности; - разрабатывать предложения по совершенствованию политики безопасности.	Устный опрос Тестирование Практическая работа Внеаудиторная самостоятельная работа Экзамен
Знания:	
- терминологию в сфере безопасности информационного контента; **-** понятия политики безопасности, существующие типы политик безопасности; - существующие стандарты информационной безопасности; - виды угроз информационной безопасности; - средства борьбы с угрозами информационной безопасности; - о современных концепциях безопасности программного обеспечения и баз данных; - методы защиты информации; - критерии защищенности программного обеспечения и баз данных; - угрозы безопасности программного обеспечения и баз данных; - критерии и методы оценивание механизмов защиты; - организационно-правовое обеспечение информационной безопасности.	Устный опрос Тестирование Практическая работа 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: Мотыльков К.В.., преподаватель ФГБОУ ВО "РЭУ им. Г.В. Плеханова"

Эксперт: