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.01 Основы информационной безопасности**

код, специальность**: 10.02.03 Информационная безопасность автоматизированных систем**

квалификация: **техник по защите информации**

форма обучения: очная

Москва

СОГЛАСОВАНА

цикловой методической комиссией «Профессиональных модулей 10.02.03»

Разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности

10.02.03 Информационная безопасность автоматизированных систем

код, наименование специальности

Протокол № 1-17/18

от «31» 08 2017 года

Председатель цикловой методической комиссии _____ М. С. Прищеп
подпись инициалы, фамилия

Заместитель директора техникума по учебной работе _____ Д. А. Клолов
подпись инициалы, фамилия

УТВЕРЖДЕНА

Директор техникума _____ А. В. Чурилов
подпись инициалы, фамилия

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.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена по специальности 10.02.03 Информационная безопасность автоматизированных систем

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:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации

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

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
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 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. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.
ПК 2.6. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности программно-аппаратными средствами.
ПК 3.3. Участвовать в мониторинге эффективности применяемых инженерно-технических средств обеспечения информационной безопасности.
ПК 3.5. Применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

1.4. Рекомендуемое количество часов на освоение учебной дисциплины:

максимальная учебная нагрузка обучающегося	162	часа
включая:		
обязательная аудиторная учебная нагрузка	108	часов
самостоятельная работа	48	часов
консультации	6	часов
ВСЕГО	**162**	**часа**

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	**162**
Обязательная аудиторная учебная нагрузка (всего)	**108**
в том числе:	
практические занятия	44
лабораторные работы	
контрольные работы	
Самостоятельная работа обучающегося (всего)	**48**
в том числе:	
тематика внеаудиторной самостоятельной работы	48
Консультации	**6**
Итоговая аттестация 3 семестр – другие формы контроля 4 семестр - дифференцированный зачет	

2.2. Тематический план и содержание тем учебной дисциплины ОП.01 Основы информационной безопасности

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		**24**	
Тема 1.1. Основные виды информационной защиты. Защита человека как собственника информации.	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.	4	1
	Самостоятельная работа Формирование прав собственности на информацию.	4	
Тема 1.2. Уровни представления информации и особенности ее защиты**.**	Виды и общая характеристика информационных угроз. Уязвимости информационных систем. Виды ущерба от информационных атак. Носители информационных угроз.	4	1
Тема 1.3. Классификация и категории информационных нарушителей.	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.	6	1
	Практическая работа	2	
	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	4	
	Создание перечня информационного контента, агентов угроз и угроз на индивидуальном предприятии. Выполнение анализа угроз и уязвимости.		
Раздел 2. Направления информационной защиты		**28**	

Тема 2.1. Нормативно-правовое регулирование защиты информации**.**	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.	4	1
	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.	4	
Тема 2.2. Организационно-распорядительная защита.	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.	4	1
	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.	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.	6	1
	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.	4	

	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.	2	
	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		**28**	
Тема 3.1. Описание типовых политик безопасности.	Понятие политики безопасности. Модель политики безопасности.	2	1
	Практическая работа	2	
	Оценка политик безопасности		
Тема 3.2. Модель защищенного канала связи.	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.	4	1,2
	Самостоятельная работа Технические характеристики устройств (передатчиков и приемников), подключаемых к каналу связи.	4	
Тема 3.3. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности.	Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем.	4	1
Тема 3.4. Угрозы безопасности компьютерных систем.	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.	4	1,2
	Самостоятельная работа Создание перечня методов и средств защиты ПО на индивидуальном предприятии.	4	

Тема 3.5. Защита программ	Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий**.** Защита программ от изменения и контроль целостности.	4	1,2
Раздел 4. Механизмы обеспечения информационной безопасности программного обеспечения и баз данных		**40**	
Тема 4.1. 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.	2	1,2
	Самостоятельная работа Методы затруднения отладки, Эмуляция процессоров и операционных систем. Достоинства и недостатки методов.	4	
	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.	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.	2	1,2
Тема 4.3. Методы противодействия.	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.	2	1,2
	Самостоятельная работа обучающихся Этапы развития криптографии. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа.	4	
	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.	Использование представлений для обеспечения конфиденциальности информации в СУБД.	2	1,2
	Самостоятельная работа обучающихся Произвести сравнительный анализ достоинств и недостатков изученных ранее СУБД.	6	
Тема 4.5. Аудит и подотчетность.	Подотчетность действий пользователя и аудит связанных с безопасностью событий. Журнализация. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.	4	1,2
Тема 4.6. Оценка эффективности систем защиты	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.	2	1,2
	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		**20**	
Тема 5.1. Программно-аппаратные средства защиты информации в сетях передачи данных.	Модели безопасного взаимодействия в КС. Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды.	6	1,2
Тема 5.2. Межсетевые экраны.	Свойства экранирующего субъекта. Классификация требований к классам межсетевых экранов.	6	1,2
	Самостоятельная работа обучающихся Создание перечня систем идентификации и аутентификации на индивидуальном предприятии. Аудит журналов брандмауэра.	6	
	Практическая работа Создание модели политики безопасности индивидуального предприятия на основе собранных данных	2	

Раздел 6. Организационно-правовое обеспечение информационной безопасности		**22**	
Тема 6.1.	Правовое обеспечение информационной безопасности. Российские документы по защите информации. Организационное обеспечение информационной безопасности	6	1,2
Тема 6.2.	Состав и назначение должностной инструкции.	6	1,2
	Самостоятельная работа обучающихся Методы контроля за исполнением должностных инструкций.	2	
	Самостоятельная работа обучающихся Методы и формы организационной защиты информации. Методы организационной защиты информации. Виды перекрытия каналов утечки информации	4	
	Практическая работа Составление должностной инструкции	4	
	Всего:	***162***	

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.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы учебной дисциплины требует наличия Лаборатории инженерно-технических средств обеспечения информационной безопасности

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	Стол преподавателя 1 шт	проектор 1 шт	32
2	парты 21 шт		
3	стулья 32 шт		
4	шкафы 12 шт		
5	автоматизированные рабочие места 11 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
Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

№ 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
1.4	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
1.5	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 безопасности: 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.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 дифференцированный зачет

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:	
• классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; • применять основные правила и документы системы сертификации Российской Федерации; • классифицировать основные угрозы безопасности информации	Устный опрос Наблюдение и оценка результата выполнения практических работ Тестирование Внеаудиторная самостоятельная работа Дифференцированный зачет
Знания:	
• сущность и понятие информационной безопасности, характеристику ее составляющих; • место информационной безопасности в системе национальной безопасности страны;	Устный опрос Наблюдение и оценка результата выполнения практических работ Тестирование

• 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	Внеаудиторная самостоятельная работа Дифференцированный зачет

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:
Прищеп М.С., преподаватель ФГБОУ ВО РЭУ им. Г.В. Плеханова

Эксперт: