Государственное автономное профессиональное
образовательное учреждение
«Мамадышский политехнический колледж»

УТВЕРЖДАЮ
Зам. директора по ТО
_____ Файзреева В.В.
«_01_» _сентября_ 2022 г.

РАБОЧАЯ ПРОГРАММА
дисциплины ОП.11 Основы информационной безопасности
по специальности 09.02.01 Компьютерные системы и комплексы

2022 г.

Рабочая программа учебной дисциплины ОП. 11 Основы информационной безопасности разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, приказ Министерства образования и науки от 28 июля 2014 г. № 849 (Зарегистрировано в Минюсте России 21.08.2014 г. №33748).

Обсуждена и одобрена на заседании предметно-цикловой комиссии преподавателей и мастеров производственного обучения общепрофессиональных дисциплин

Протокол № 1

«29» августа 2022 г.

Председатель ПЦК:

_____ В.В. Мирзаянова

Разработчик: Искандарова Раушания Зиннуровна, преподаватель

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 Основы информационной безопасности

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.11 Основы информационной безопасности является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы, входящей в состав укрупненной группы 09.00.00 Информатика и вычислительная техника.

1.2. Место учебной дисциплины в структуре ППССЗ: дисциплина входит в дисциплины профессионального цикла.

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

В результате освоения дисциплины обучающийся должен уметь:

– распознавать задачу и/или проблему в профессиональном и/или социальном контексте;

– реализовать задачу и/или проблему и выделять её составные части;

– определять этапы решения задачи;

– определять актуальность нормативно-правовой документации в профессиональной деятельности;

– применять современную научную профессиональную терминологию;

– выбирать сетевые топологии;

– использовать программно-аппаратныесредства технического контроля;

В результате освоения дисциплины обучающийся должен знать:

– содержание актуальной нормативно-правовой

– документации;

– современная научная и профессиональная терминология;

– значимость профессиональнойдеятельности специальности.

Знания и умения по дисциплине ОП.11 Основы информационной безопасности ориентированы на формирование общих и профессиональных компетенций:

общих:

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 инести 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.

профессиональных:

ПК 3.1. Проводить контроль параметров, диагностику и восстановление работоспособности компьютерных систем и комплексов.

1.4. Количество часов на освоение программы учебной дисциплины:

максимальная учебная нагрузка обучающихся – 72 часа, в том числе:

обязательной аудиторной учебной нагрузки обучающихся – 48 часов;

самостоятельной работы обучающихся – 24 час.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**72**
Обязательная аудиторная учебная нагрузка (всего)	**48**
в том числе:	
лабораторные работы	
практические занятия	**20**
контрольные работы	
Самостоятельная работа обучающегося (всего)	**24**
Итоговая аттестация в форме дифференцированного зачета.	*2*

1.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объемв часах	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Понятие национальной безопасности. Понятие информационной безопасности.	**Содержание учебного материала**	**24**	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ПК 1.2, ПК 1.3,
	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.	4	
	В том числе, практических занятий	**10**	
	Практическое занятие №1		
	Нормативно – правовое обеспечение информационной безопасности. Анализтерминов и определений	6	
	Практическое занятие №2		
	Угрозы информационной безопасности	4	
	Самостоятельная работа обучающихся	**10**	
	Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.		

Тема 2. Угрозы информационной безопасности	**Содержание учебного материала**	**27**	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10, ПК 1.2, ПК 1.3, ПК 3.5
	Национальные интересы и угрозы информационной безопасности Российской Федерации в информационной сфере и их обеспечение. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Угрозы конституционным правами свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка и ее продукции и выходу этой продукций на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональнойинформационной безопасности. Содержание информационного противоборства на межгосударственном уровне.Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и	12	

	возможности. Содержание информационного противоборства на военном уровне. Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационного воздействия.		
	В том числе, практических занятий	**5**	
	Практическое занятие №3		
	Допуск должностных лиц и граждан к государственной тайне		
	Самостоятельная работа обучающихся	**10**	
	Угрозы конституционным правами свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России. Угрозы информационному обеспечению государственной политики Российской Федерации.		
	Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка и ее продукции и выходу этой продукций на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.		
	Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.		
	Содержание информационного противоборства на межгосударственном		

	уровне.Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели и-формационного противоборства. Составные части и методы информационного противоборства.		
	Информационное оружие, его классификация и возможности.		
Тема 3. Методы и средства обеспечения информационной безопасности компьютерных систем.	**Содержание учебного материала**	**19**	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10, ПК 1.2, ПК 1.3, ПК 3.5
	Методы и средства обеспечения информационной безопасности компьютерных систем. Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности. Методы оценки защищенности компьютерных систем от несанкционированного доступа (НСД). Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общие критерии. Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем (АС). Методы защиты информации, обрабатываемой в АС, от технических разведок.Генераторы электромагнитных импульсов. Эффекты, возникающие от внешнего электромагнитного воздействия на АС исистемы вычислительной техники (СВТ). Методы защиты АС и СВТ от внешнего электромагнитного воздействия.	**12**	
	Итоги изучения курса. Методические рекомендации по применению полученныхзнаний, умений и навыков при изучении последующих курсов.		
	В том числе, практических занятий	**3**	
	Практическое занятие №4.		
	Симметричное шифрование. Блочные и потоковые шифры		
	Самостоятельная работа обучающихся	**4**	
	Методы и средства обеспечения информационной безопасности		

	компьютерныхсистем.		
	Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.		
	Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Общие критерии.		
	Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированныхсистем (АС).		
Промежуточная аттестация в форме дифференцированного зачета		***2***	
Всего:		***72***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия учебного кабинета информатики.

3.1.1. Оборудование кабинета информатики:

№ п/п	Наименование	Инвентарный номер	Дата	
			принятия к учету	ввода в эксплуатацию
1	Арм преподавателя Algorithm-I	222101040416	30.09.2011	01.10.2011
2	Жалюзи вертикальные тканевые	222101042127	29.04.2014	29.04.2014
3	Жалюзи вертикальные тканевые	222101042128	29.04.2014	29.04.2014
4	Жалюзи вертикальные тканевые	222101042129	29.04.2014	29.04.2014
5	Программно-аппаратный комплекс RAY S222Mi	222101043073	03.10.2014	03.10.2014
6	Программно-аппаратный комплекс RAY S222Mi	222101043074	03.10.2014	03.10.2014
7	Программно-аппаратный комплекс RAY S222Mi	222101043075	03.10.2014	03.10.2014
8	Программно-аппаратный комплекс RAY S222Mi	222101043076	03.10.2014	03.10.2014
9	Программно-аппаратный комплекс RAY S222Mi	222101043077	03.10.2014	03.10.2014
10	Программно-аппаратный комплекс RAY S222Mi	222101043078	03.10.2014	03.10.2014
11	Программно-аппаратный комплекс RAY S222Mi	222101043079	03.10.2014	03.10.2014
12	Программно-аппаратный комплекс RAY S222Mi	222101043080	03.10.2014	03.10.2014
13	Программно-аппаратный комплекс RAY S222Mi	222101043081	03.10.2014	03.10.2014
14	Программно-аппаратный комплекс RAY S222Mi	222101043082	03.10.2014	03.10.2014
15	Программно-аппаратный комплекс RAY S222Mi	222101043083	03.10.2014	03.10.2014
16	Программно-аппаратный комплекс RAY S222Mi	222101043084	03.10.2014	03.10.2014
17	Программно-аппаратный комплекс RAY S222Mi	222101043085	03.10.2014	03.10.2014
19	шкаф для одежды	222101040687	05.08.2013	05.08.2013
20	Шкаф 2-створчатый со	222101042515	2019	2019

№ п/п	Наименование	Инвентарный номер	Дата	
			принятия к учету	ввода в эксплуатацию
	стеклянными дверями			
21	Шкаф 2-створчатый со стеклянными дверями	222101042516	2019	2019
22	Интерактивный комплект	222101045608	13.12.2017	13.12.2017
23	Ноутбук Портативный ПЭВМ RAYbook Bi1010 ICL	222101045661	19.07.2018	19.07.2018

Материальные ценности

№ п/п	Наименование	Единица измерения	Количество
1	Компьютерный стол	шт.	13,00
2	В стул ученический регулируемый	шт	15,00
3	Доска школьная	шт.	1,00
5	Кресло "Визитор" №1 ч/м	шт.	1,00
6	Огнетушитель ОП-5(з)	шт.	1,00
7	сетевой Switch Trendnet	шт.	1,00
8	Стол ученический (лак)	шт.	7,00
9	Стол учителя	шт.	1,00
10	Стул ученический (лак)	шт.	14,00
11	Колонка USB Genius SP-HF160 Wooden 2x2W	шт.	1

Программное обеспечение компьютеров

1. Операционная система Microsoft Windows 10;
2. Компилятор языка программирования Free Pascal;
3. Пакет программ Microsoft Office 2007:
 − текстовый редактор MS Word 2007;
− электронные таблицы MS Excel 2007;
− программа MS Power Point 2007;
4. Антивирусные программы USB Disk Security

Инвентарная ведомость технических средств обучения кабинета № 303

№ п/п	Наименование ТСО	Марка	Год при-обретения	Инв. №
1.	Интерактивная доска	TRUBOARD	13.12.2017	222101045608

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

3.2.1. Основная литература

1. Клочко, И. А. Информационные технологии в профессиональной деятельности [Электронный ресурс] : учебное пособие для СПО / И. А. Клочко. — 2-е изд. — Электрон. текстовые данные. — Саратов: Профобразование, Ай Пи Эр Медиа, 2019. — 292 c. — 978-5-4486-0407-2, 978-5-4488-0219-5. — Режим доступа: http://www.iprbookshop.ru/80327.html

2. Косиненко Н.С. Информационные технологии в профессиональной деятельности [Электронный ресурс] : учебное пособие для СПО / Н.С. Косиненко, И.Г. Фризен. — 2-е изд. — Электрон. текстовые данные. — Саратов: Профобразование, Ай Пи Эр Медиа, 2018. — 308 c. — 978-5-4486-0378-5, 978-5-4488-0193-8. — Режим доступа: http://www.iprbookshop.ru/76992.html

3.2.2. Дополнительная литература

3. Пахомова, Н. А. Информационные технологии в менеджменте [Электронный ресурс]: учебно-методическое пособие / Н. А. Пахомова. — Электрон. текстовые данные. — Саратов : Ай Пи Эр Медиа, 2018. — 93 c. — 978-5-4486-0033-3. — Режим доступа: http://www.iprbookshop.ru/70765.html

4. Петров, С. В. Информационная безопасность [Электронный ресурс] : учебное пособие / С. В. Петров, П. А. Кисляков. — Электрон. текстовые данные. — Саратов : Ай Пи Ар Букс, 2015. — 326 c. — 978-5-906-17271-6. — Режим доступа: http://www.iprbookshop.ru/33857.html

5. Журнал «Вопросы защиты информации»

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Формы и методы оценки***
Перечень знаний, осваиваемых в рамках дисциплины:	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Оценка в рамках текущего контроля результатов выполнения индивидуальных контрольных заданий, результатов выполнения практических работ, устный индивидуальный опрос. Письменный опрос в форме тестирования
Содержание актуальной нормативно-правовой документации; Современная научная и профессиональная терминология; Значимость профессиональной деятельности специальности.		
Перечень умений, осваиваемых в рамках дисциплины:		
Распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Реализовать задачу и/или проблему и выделять её составные части; Определять этапы решения задачи; Определять актуальность нормативно-правовой документации в профессиональнойдеятельности; Применять современную научную профессиональную терминологию; Выбирать сетевые топологии; Использовать программно-аппаратные средства технического контроля; Использовать программно-аппаратные средства технического контроля;		Экспертное наблюдениеи оценивание выполнения практических работ. Текущий контроль в форме защиты практических работ