Краевое государственное бюджетное профессиональное образовательное учреждение
«Приморский индустриальный колледж»

УТВЕРЖДАЮ
Зам. директора по УПР
_____Е.Н. Золотарева
«__09__» ____06_____ 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 ЗАЩИТА ИНФОРМАЦИИ

Программа подготовки специалистов среднего звена
по специальности среднего профессионального образования технологического профиля
09.02.04 Информационные системы (по отраслям)

Рабочая программа утверждена
на заседании методического объединения
профессиональных дисциплин
Протокол № __4__ от «__8__» ____06_____2020 г.
_____И.В. Мироненко

Программа составлена
«__4__» _____июня_____2020 г.

Преподаватель:
_____ А.Ю. Сережкина

г. Арсеньев

Рабочая программа разработана на основе Федерального государственного образовательного стандарта по специальности 09.02.04 Информационные системы (по отраслям), утвержденного приказом Министерства образования и науки Российской Федерации от 14 мая 2014 № 525 (ред. от 21.10.2019) "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.04 Информационные системы (по отраслям)" (Зарегистрировано в Минюсте России 03.07.2014 N 32962)

В рабочей программе раскрывается содержание дисциплины, указываются тематика практических работ, темы самостоятельных работ, формы и методы текущего контроля учебных достижений и промежуточной аттестации обучающихся, рекомендуемые учебные пособия.

Организация-разработчик: КГБПОУ «Приморский индустриальный колледж»

Разработчик: Сережкина А.Ю., преподаватель общепрофессиональных и профессиональных дисциплин технологического профиля.

СОДЕРЖАНИЕ

ОП.14 Защита информации

1. Паспорт рабочей программы учебной дисциплины

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности 09.02.04 Информационные системы (по отраслям)

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке.

1.2 Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина ОП.14 «Защита информации» входит в профессиональный цикл и относится к общепрофессиональным дисциплинам. Дисциплина обеспечивается знаниями полученными студентами на первом курсе при освоении дисциплины УПВ.03 «Информатика». ОП.14 «Защита информации» является обеспечивающей дисциплиной для ПМ.03. «Выполнение работ профессии».

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

В результате изучения обязательной части учебного цикла обучающийся по общепрофессиональным дисциплинам должен:

уметь:

• применять организационно-правовые методы защиты информации в информационных системах;

• обеспечивать антивирусную защиту информации;

• использовать криптостойкие алгоритмы защиты данных;

• выполнять аутентификацию информации.

знать:

• сущность информационной безопасности информационных систем;

• состав и методы организационно-правовой защиты информации;

• источники возникновения информационных угроз;

• методы антивирусной защиты информации;

• алгоритмы традиционных методов шифрования данных;

• современные методы криптозащиты информации;

• протоколы идентификации и проверки подлинности пользователя;

• процедуры аутентификации данных и постановки электронной цифровой подписи.

В результате изучения учебной дисциплины ОП.14 «Защита информации» формируются следующие компетенции:

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.

Техник по информационным системам должен обладать профессиональными компетенциями, соответствующими видам деятельности:

ПК 1.1. Собирать данные для анализа использования и функционирования информационной системы, участвовать в составлении отчетной документации, принимать участие в разработке проектной документации на модификацию информационной системы.

ПК 1.5 Разрабатывать фрагменты документации по эксплуатации информационной системы.

ПК 1.10 Обеспечивать организацию доступа пользователей информационной системы в рамках своей компетенции.

ПК 2.6 Использовать критерии оценки качества и надёжности функционирования информационной системы.

Процесс изучения дисциплины направлен на формирование личностных результатов реализации программы воспитания:

ЛР 1. Осознающий себя гражданином и защитником великой страны.

ЛР 2. Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций.

ЛР 3. Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 5. Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России.

ЛР 6. Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях.

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 8. Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

ЛР 12. Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания.

Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности:

ЛР 13. Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации.

ЛР 14. Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм.

ЛР 15. Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.

1.4 Количество часов на освоение программы дисциплины

максимальной учебной нагрузки обучающегося **84** часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося **56** часов;

в т.ч. лабораторные и практические 28 часов;

самостоятельной работы обучающегося **28** 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)	**84**
Обязательная аудиторная учебная нагрузка (всего)	**56**
в том числе:	
практические	28
Самостоятельная работа обучающегося (всего)	**28**
Итоговая аттестация	***Дифференцированный зачет***

2.2 Тематический план и содержание учебной дисциплины ОП.14 «Защиты информации»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студентов, курсовая работа (проект)	Объем часов	Осваиваемые компетенции
РАЗДЕЛ 1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ			
Тема 1.1 Понятие "информационная безопасность"	***Содержание учебного материала:*** 1. Введение 2. Проблема информационной безопасности общества	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Подготовка проекта: этапы развития информационной безопасности в обществе	3	
Тема 1.2 Составляющие информационной безопасности	***Содержание учебного материала:*** 1. Доступность информации. Целостность информации 2. Конфиденциальность информации 3. Уровни информационной безопасности объектов 4. Уровни информационной безопасности объектов 5. Обнаружение и противодействие атакам. 6. Криптографические механизмы конфиденциальности, целостности и аутентичности информации 7. Основные возможности криптографических методов защиты информации 8. Человеческий фактор в безопасности.	8	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Проанализировать профессионально-значимые источники информации с точки зрения основных аспектов: конфиденциальности, целостности и доступности	3	
Тема 1.3 Система формирования режима информационной безопасности	***Содержание учебного материала:*** 1. Задачи информационной безопасности общества	1	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: 1. Параметры безопасности программы Microsoft Outlook	1	
	Содержание учебного материала:		ОК 01-ОК 09

Тема 1.4 Нормативно-правовые основы информационной безопасности в РФ	1. Правовые основы информационной безопасности общества 2. Государственная система обеспечения информационной безопасности. 3. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации 4. Ответственность за нарушения в сфере информационной безопасности	4	ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: 1. Права на использование директории для определенного пользователя	1	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Составить перечень основных понятий и определений, используемых в нормативно-правовых документах	2	
РАЗДЕЛ 2 СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ			
Тема 2.1 Стандарты информационной безопасности: "Общие критерии"	***Содержание учебного материала:*** 1. Требования безопасности к информационным системам 2. Принцип иерархии: класс – семейство – компонент – элемент	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: ***1.*** Проверка компьютера на предмет наличия уязвимостей ***2.*** Исследование угроз доступности ***3.*** Использование средств администрирования Windows для анализа и настройки безопасности системы ***4.*** Использование шифрующей файловой системы	6	
	Самостоятельная работа: Чтение и анализ литературы. Домашнее задание: работа с конспектом лекций.	2	
Тема 2.2 Стандарты информационной безопасности распределенных систем	***Содержание учебного материала:*** 1. Сервисы безопасности в вычислительных сетях 2. Администрирование средств безопасности	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Чтение и анализ литературы. Домашнее задание: работа с конспектом лекций.	3	
Тема 2.3 Стандарты информационной безопасности в РФ	***Содержание учебного материала:*** ***1.*** Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ ***2.*** Документы по оценке защищенности автоматизированных систем в РФ	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10,

			ПК 2.6.
	Самостоятельная работа: Чтение и анализ литературы. Домашнее задание: работа с конспектом лекций.	2	
Тема 2.4 Административный уровень обеспечения информационной безопасности	***Содержание учебного материала:*** 1. Цели, задачи и содержание административного уровня 2. Политика безопасности и меры противодействия. 3. Разработка политики информационной безопасности	3	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Чтение и анализ литературы. Домашнее задание: работа с конспектом лекций.	2	
Тема 2.5 Классификация угроз "информационной безопасности	***Содержание учебного материала:*** 1. Классы угроз информационной безопасности 2. Каналы несанкционированного доступа к информации	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: 1. Разграничение доступа к системам 2. Аварийное восстановление 3. Защита и восстановление данных на компьютере, используя систему архивации.	3	
	Самостоятельная работа: Чтение и анализ литературы. Домашнее задание: работа с конспектом лекций.	2	
РАЗДЕЛ 3 КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ			
Тема 3.1 Вирусы как угроза информационной безопасности	***Содержание учебного материала:*** 1. Компьютерные вирусы и информационная безопасность 2. Воздействия на программно-аппаратные средства защиты информации 3. Характерные черты компьютерных вирусов	3	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Самостоятельная работа: Разработать контролирующий, диагностирующий или демонстрационный материал по теме	3	

Тема 3.2 Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям	***Содержание учебного материала:*** 1. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям	1	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: 1. Использование антивирусных программ 2. Настройка антивирусной программы, обновление сигнатур. 3. Борьба с рекламными и шпионскими программами	3	
	Самостоятельная работа: Построить схему системы антивирусной защиты корпоративной сети	2	
Тема 3.3 Характеристика "вирусоподобных" программ	***Содержание учебного материала:*** 1. Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. "Intended"-вирусы. Способы заражения программ. Признаки проявления вируса. Методы защиты.	2	ОК 01-ОК 09 ПК 1.1, ПК 1.5, ПК 1.10, ПК 2.6.
	Практические работы: 1. Исследование реестра, на предмет возможных уязвимостей для вирусов 2. Приемы работы с защищенными программами 3. Использование брэндмауэров 4. Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки AVZ.». 5. Очистка системы 6. Оптимизация антивирусной программы под определенную систему 7. Задание исключений и требований доверия 8. Настройка межсетевого экрана	8	
	Самостоятельная работа: Составить презентацию в программе Power Point по теме: Характеристика "вирусоподобных" программ	3	
Дифференциальный зачет		**2**	
ВСЕГО:		**84**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1 Требования к минимальному материально-техническому обеспечению

Программа реализуется в учебной мастерской специальности «Информационные системы (по отраслям)».

Оборудование рабочих мест мастерской:

- рабочие места по количеству обучающихся, оборудованные персональными компьютерами с необходимым программным обеспечением общего и профессионального назначения;
- комплект учебно-методической документации;
- наглядные пособия: демонстрационные плакаты, макеты, раздаточный материал, электронные учебники, видеоматериалы;
- мультимедийный проектор;
- сканер;
- принтер.

Оборудование учебного кабинета:

- персональный компьютер;
- мультимедийный проектор;
- интерактивная доска;
- комплект учебно-методической документации; - наглядные пособия (стенды, стандарты ЕСКД).

Технические средства обучения:

- электронные учебники, плакаты, видеоматериалы;
- персональный компьютер; - мультимедийный проектор.

Программные средства обучения:

ОС Windows; Google Chrome, IntelliJ IDEA Community Edition, Java SE Microsoft Visual Studio Code, PascalABC.Net, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Мельников В.П. Информационная безопасность: учебное пособие для студентов учреждений среднего профессионального образования. / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под редакцией С.А. Клейменова. - 10-е изд., стер. - М.: Издательский центр «Академия», 2019. - 336 с.

Дополнительные источники:

1. Конституция Российской Федерации. – 1993 г.
2. Концепция национальной безопасности Российской Федерации (в редакции Указа Президента РФ от 10 января 2000 года № 24).
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
4. Закон РФ от 5 мая 1992 года № 2446-1 «О безопасности».
5. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Партыка Т. Л., Попов И. И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФРА-М, 2005. – 368 с.: ил. – (Профессиональное образование).

Интернет ресурсы

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. http://www.bnti.ru/dbtexts/analmat/1_2008/ershov.pdf
2. Шнайер Брюс. Прикладная криптография. 2-е издание, Протоколы, алгоритмы и исходные тексты на языке С. http://4444kf.110mb.com/upload/files/lection/shifr/shnaer.zip

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП. 14 «ЗАЩИТА ИНФОРМАЦИИ»

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения:	
• применять организационно-правовые методы защиты информации в информационных системах; • обеспечивать антивирусную защиту информации; • использовать криптостойкие алгоритмы защиты данных; • выполнять аутентификацию информации.	Устный опрос Тестирование Выполнение и оценка практических занятий и самостоятельных работ
Знания:	
• сущность информационной безопасности информационных систем; • состав и методы организационно-правовой защиты информации; • источники возникновения информационных угроз; • методы антивирусной защиты информации; • алгоритмы традиционных методов шифрования данных; • современные методы криптозащиты информации; • протоколы идентификации и проверки подлинности пользователя; • процедуры аутентификации данных и постановки электронной цифровой подписи.	Устный опрос Тестирование Выполнение и оценка практических занятий и самостоятельных работ;

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