Министерство образования и науки Самарской области
государственное автономное профессиональное
образовательное учреждение Самарской области
"Жигулевский государственный колледж"

УТВЕРЖДЕНО
Приказом № 100-од от 02.05.2024 г.

Подписан: ГАПОУ СО "ЖГК"
DN: OID.1.2.643.100.4=6345004462, СНИЛС=00967415365, ОГРН=1036301730508, ИНН=632302578862, E=zrt_buh@mail.ru, C=RU, S=63 Самарская область, L=ГОРОД ЖИГУЛЕВСК, STREET="МИРА УЛ,22", O="ГАПОУ СО ""ЖГК""", CN="ГАПОУ СО ""ЖГК""", T=ДИРЕКТОР, G=Александр Эдуардович, SN=Птицын
Основание: Я являюсь автором этого документа
Местоположение: Самарская область, г. Жигулевск, ул. Мира, 22
Дата: 2024.11.19 14:45:08+04'00'

Рабочая программа

учебной дисциплины:

ОПЦ.12 Информационная безопасность

для специальности

09.02.01 Компьютерные системы и комплексы

2024 год

ОДОБРЕНА
Предметной (цикловой)
комиссией
_____ЭВЭТП_____
Протокол № ____9_____
от “24” __апреля_____ 2024 г.
Председатель_____ Л.В. Форсюк

СОГЛАСОВАНО
заместитель директора по
учебно-методической работе
_____ М.Н. Тусинова
“25” _апреля_____ 2024 г.

Составитель: Ханмурзина Е.В., преподаватель ГАПОУ СО «ЖГК»

Эксперты:

Техническая экспертиза: Орешина Н.А., методист ГАПОУ СО «ЖГК»

Содержательная экспертиза: Форсюк Л.В., председатель П(Ц)К ГАПОУ СО «ЖГК»

_____

_____

Рабочая программа учебной дисциплины разработана на основе Федерального государственного стандарта среднего профессионального образования по специальности 09.02.01 Компьютерные системы и комплексы, утвержденного приказом Министерства просвещения Российской Федерации от «25» мая 2022 г. № 362.

Рабочая программа разработана с учетом квалификационных запросов со стороны предприятий/организаций.

Рабочая программа разработана в соответствии с требованиями к оформлению, установленными в ГАПОУ СО «ЖГК».

Содержание программы реализуется в процессе освоения обучающимися программы подготовки специалистов среднего звена по специальности 09.02.01 Компьютерные системы и комплексы.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОПЦ.12 Информационная безопасность

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.01 Компьютерные системы и комплексы.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании.

Рабочая программа составлена для очной формы обучения.

1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена: является вариативной частью общепрофессионального цикла.

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

Основная часть: не предусмотрена.

Вариативная часть:

В результате освоения учебной дисциплины обучающийся должен уметь:

УВ 01. Применять правовые, организационные, технические и программные средства защиты информации;

УВ 02. Создавать программные средства защиты информации.

В результате освоения учебной дисциплины обучающийся должен знать:

ЗВ 01. Источники возникновения информационных угроз;

ЗВ 02. Модели и принципы защиты информации от несанкционированного доступа;

ЗВ 03. Методы антивирусной защиты информации;

ЗВ 04. Состав и методы организационно-правовой защиты информации.

В результате освоения учебной дисциплины должны формироваться общие компетенции (ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности;

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

В результате освоения учебной дисциплины должны формироваться профессиональные компетенции (ПК):

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

Рабочая программа дисциплины реализуется в единстве учебной и воспитательной деятельности в соответствии с рабочей программой воспитания с учётом направлений воспитания:

− гражданское воспитание/ГН;

− патриотическое воспитание/ПатН;

− духовно-нравственное воспитание/ДНН;

− эстетическое воспитание/ЭстН;

− физическое воспитание, формирование культуры здорового образа жизни и эмоционального благополучия/ФН;

− профессионально-трудовое воспитание/ТН;

− экологическое воспитание/ЭкН;

− ценности научного познания/ПознН.

1.4. Количество часов на освоение рабочей программы учебной дисциплины:
Объем образовательной программы 80 часов, в том числе:

самостоятельной работы обучающегося 4 часа.

2. СТРУКТУРА СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Объем образовательной программы (всего)	*80*
в том числе:	
теоретическое обучение	*40*
лабораторные занятия **в форме практической подготовки**	-
практические занятия **в форме практической подготовки**	*30*
контрольные работы	-
курсовая работа (проект) (*если предусмотрено)*	-
Самостоятельная работа обучающегося (всего)	*4*
в том числе:	
внеаудиторная самостоятельная работа	*4*
Консультации (*если предусмотрено)*	-
Промежуточная аттестация в форме *экзамена*	*6*

2.2. Тематический план и содержание учебной дисциплины ОПЦ.12 Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*		Объем часов	Код образовательного результата	Направления воспитательной работы
1	2		3	4	5
Введение	**Содержание учебного материала**		**2**	ЗВ 01- ЗВ 04, УВ 01, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Предмет и задачи информационной безопасности.	1		
	2	Эволюция подходов к обеспечению информационной безопасности.	1		
	Самостоятельная работа обучающихся (внеаудиторная)		-		
Раздел 1. Борьба с угрозами несанкционированного доступа к информации			***37***		
Тема 1.1. Актуальность проблемы обеспечения безопасности информации	**Содержание учебного материала**		***4***	ЗВ 01- ЗВ 04, УВ 01, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации.	*1*		
	2	Угрозы информационной безопасности: классификация, источники возникновения и пути реализации.	*2*		
	3	Определение требований к уровню обеспечения информационной безопасности.	*1*		
	Самостоятельная работа обучающихся (внеаудиторная)		-		
Тема 1.2. Виды мер обеспечения информационной безопасности	**Содержание учебного материала**		**10**	ЗВ 01- ЗВ 04, УВ 01, УВ 02, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Виды мер обеспечения информационной безопасности.	1		
	2	Специфические приемы управления техническими средствами.	1		
	3	Методы защиты от копирования. Не копируемые метки.	2		
	4	Защита от средств отладки. Защита от средств дисассемблирования.	2		
	5	Защита от трассировки по заданному прерыванию.	2		
	6	Защита программ в оперативной памяти.	2		
	Практические занятия		**12**		
	Практическая работа №1. Защита информации от копирования.		4		
	Практическая работа №2. Защита программ в оперативной памяти.		4		
	Практическая работа №3. Механизмы контроля целостности данных.		4		
	Самостоятельная работа обучающихся (внеаудиторная)				

	1. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите.		2		
Тема 1.3. Основные принципы построения систем защиты информации	**Содержание учебного материала**		***4***	ЗВ 01- ЗВ 04, УВ 01, УВ 02, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Основные защитные механизмы: идентификация и аутентификация.	*2*		
	2	Криптографические механизмы защиты информации.	*2*		
	Практические занятия		***4***		
	Практическая работа №4. Криптографические методы закрытия данных.		*4*		
	Самостоятельная работа обучающихся (внеаудиторная)				
	2. Электронная цифровая подпись: анализ и перспективы.		*1*		
Раздел 2. Борьба с вирусным заражением информации			***22***		
Тема 2.1. Проблема вирусного заражения и структура современных вирусов	**Содержание учебного материала**		***10***	ЗВ 01- ЗВ 04, УВ 01, УВ 02, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Структура современных вирусов. Компьютерный вирус: понятие, пути распространения, проявление действия вируса.	*2*		
	2	Воздействия на программно-аппаратные средства защиты информации.	*2*		
	3	Разрушение программ защиты, схем контроля.	*2*		
	4	Программы-шпионы. Взлом парольной защиты.	*2*		
	5	Защита от воздействия вирусов.	*2*		
	Практические занятия		***6***		
	Практическая работа №5. Алгоритмы поведения вирусных и других вредоносных программ.		*4*		
	Практическая работа №6. Алгоритмы предупреждения и обнаружения вирусных угроз.		*2*		
	Самостоятельная работа обучающихся (внеаудиторная)		*-*		
Тема 2.2. Классификация антивирусных программ	**Содержание учебного материала**		***2***	ЗВ 01- ЗВ 04, УВ 01, УВ 02, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Классификация антивирусных программ: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры.	*2*		
	Практические занятия		***4***		
	Практическая работа №7. Пакеты антивирусных программ.		*4*		
	Самостоятельная работа обучающихся (внеаудиторная)		*-*		
Раздел 3. Организационно			***13***		

-правовое обеспечение информационной безопасности					
Тема 3.1. Организационно -правовое обеспечение информационной безопасности	**Содержание учебного материала**		***8***	ЗВ 01- ЗВ 04, УВ 01, ОК 01- ОК 09, ПК 3.1	ГН, ПатН, ДНН, ЭстН, ФН, ТН, ЭкН, ПозН
	1	Международные, российские и отраслевые правовые документы.	*1*		
	2	Стандарты и нормативно-методические документы в области обеспечения информационной безопасности.	*2*		
	3	Государственная система обеспечения информационной безопасности.	*2*		
	4	Международные правовые акты по защите информации.	*1*		
	5	Порядок создания, состав и назначение должностных инструкций.	*2*		
	Практические занятия		***4***		
	Практическая работа №8. Законодательство РФ в борьбе с компьютерными преступлениями.		*4*		
	Самостоятельная работа обучающихся (внеаудиторная)				
	3. Международные правовые акты по защите информации.		*1*		
Консультации			-		
Промежуточная аттестация - экзамен			***6***		
		Всего:	***80***		
		в том числе вариативная часть:	*80*		

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличия лаборатории Информационных технологий.

Оборудование лаборатории и рабочих мест лаборатории:

- автоматизированные рабочие места обучающихся (процессор не ниже i5, оперативная память объемом не менее 16 Гб или аналоги);
- автоматизированное рабочее место преподавателя (процессор не ниже i5, оперативная память объемом не менее 32 Гб или аналоги);
- демонстрационные стенды;
- принтеры;
- МФУ;
- интерактивная доска;
- аудиосистема;
- проектор и экран;
- маркерная доска.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189328 (дата обращения: 19.04.2024). – Режим доступа: по подписке.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2130242 (дата обращения: 19.04.2024). – Режим доступа: по подписке.

3. Сычев, Ю. Н. Основы информационной безопасности : учебное пособие / Ю. Н. Сычев. — Москва : ИНФРА-М, 2024. — 337 с. — (Среднее профессиональное образование). - ISBN 978-5-16-019432-5. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2118689 (дата обращения: 19.04.2024). – Режим доступа: по подписке.

Дополнительные источники:

1. Гришина, Н. В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 239 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-545-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/1001363 (дата обращения: 19.04.2024)

2. Ищейнов В.Я. Основные положения информационной безопасности: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум, НИЦ ИНФРА-М, 2015. – 208с. (электронный ресурс)

Интернет-ресурсы:

1. Национальный открытый университет Интуит https://www.intuit.ru
2. Ведущий образовательный портал Росии Инфоурок https://infourok.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения тестирования, а также выполнения обучающимися самостоятельной работы, индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Умения УВ 01. Применять правовые, организационные, технические и программные средства защиты информации; УВ 02. Создавать программные средства защиты информации.	Текущий контроль в форме: - устного и письменного опроса; - защиты практических работ; - выполнения индивидуальных тестовых заданий. Промежуточная аттестация -экзамен
Знания: ЗВ 01. Источники возникновения информационных угроз; ЗВ 02. Модели и принципы защиты информации от несанкционированного доступа; ЗВ 03. Методы антивирусной защиты информации; ЗВ 04. Состав и методы организационно-правовой защиты информации.	

5. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ

№ изменения, дата внесения изменения; № страницы с изменением; .	
БЫЛО	**СТАЛО**
Основание: Подпись лица внесшего изменения	

Рассмотрено на заседании
предметной (цикловой) комиссии
Председатель П(Ц)К
_____ (Ф.И.О.)

Протокол № _____
от _____ 202__ г.

ПРИЛОЖЕНИЕ 1

к рабочей программе учебной дисциплины ОПЦ.12 Информационная безопасность

ПЛАНИРОВАНИЕ УЧЕБНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ АКТИВНЫХ И ИНТЕРАКТИВНЫХ ФОРМ И МЕТОДОВ ОБУЧЕНИЯ СТУДЕНТОВ

№ п/п	Тема учебного занятия	Активные и интерактивные формы и методы обучения	Код формируемых компетенций
1.	Угрозы информационной безопасности: классификация, источники возникновения и пути реализации.	Дискуссия	ОК 01- ОК 09, ПК 3.1
2.	Виды мер обеспечения информационной безопасности.	«Мозговой штурм»	ОК 01- ОК 09, ПК 3.1
3.	Криптографические механизмы защиты информации	Имитационные МАО (анализ конкретных ситуаций)	ОК 01- ОК 09, ПК 3.1
4.	Структура современных вирусов. Компьютерный вирус: понятие, пути распространения, проявление действия вируса.	Дискуссия	ОК 01- ОК 09, ПК 3.1
5.	Защита от воздействия вирусов.	Дискуссия	ОК 01- ОК 09, ПК 3.1
6.	Классификация антивирусных программ: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры.	«Мозговой штурм»	ОК 01- ОК 09, ПК 3.1
7.	Международные, российские и отраслевые правовые документы.	Групповая работа с нормативными материалами	ОК 01- ОК 09, ПК 3.1
8.	Практическая работа №8. Законодательство РФ в борьбе с компьютерными преступлениями.	Имитационные МАО (анализ конкретных ситуаций)	ОК 01- ОК 09, ПК 3.1

ПРИЛОЖЕНИЕ 2

к рабочей программе учебной дисциплины ОПЦ.12 Информационная безопасность

ИСПОЛЬЗОВАНИЕ ЧАСОВ ВАРИАТИВНОЙ ЧАСТИ

№ п/п	Конкретизированные образовательные результаты (умения, знания)	№, наименование темы	Количество часов	Формируемые компетенции (код)	Обоснование выбора
1	*Умения:* УВ 01. Применять правовые, организационные, технические и программные средства защиты информации; УВ 02. Создавать программные средства защиты информации. *Знания:* ЗВ 01. Источники возникновения информационных угроз; ЗВ 02. Модели и принципы защиты информации от несанкционированного доступа; ЗВ 03. Методы антивирусной защиты информации; ЗВ 04. Состав и методы организационно-правовой защиты информации.	Введение	2	ОК 01 - ОК 09, ПК 3.1	Дисциплина введена в соответствии с запросом работодателей. Освоенные умения будут способствовать навыкам применения правовых, организационных, технических и программных средств защиты информации; созданию программных средства защиты информации.
2		**Раздел 1. Борьба с угрозами несанкционированного доступа к информации** Тема 1.1. Актуальность проблемы обеспечения безопасности информации. Тема 1.2. Виды мер обеспечения информационной безопасности. Тема 1.3. Основные принципы построения систем защиты информации.	37		
3		**Раздел 2. Борьба с вирусным заражением информации.** Тема 2.1. Проблема вирусного заражения и структура современных вирусов.	22		

		Тема 2.2. Классификация антивирусных программ.			
4		**Раздел 3. Организационно-правовое обеспечение информационной безопасности.** Тема 3.1. Организационно-правовое обеспечение информационной безопасности.	13		
5		Экзамен	6		