МИНИСТЕРСТВО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ
«ЕКАТЕРИНБУРГСКИЙ МОНТАЖНЫЙ КОЛЛЕДЖ»

Рабочая программа учебной дисциплины
«ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
для специальности
09.02.11 «Разработка и управление программным обеспечением»

Екатеринбург

2025

Чистяков Валерий Николаевич

Подписан: Чистяков Валерий Николаевич
DN: C=RU, S=Свердловская область, L=Екатеринбург, T=директор, O="ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СВЕРДЛОВСКОЙ ОБЛАСТИ ЕКАТЕРИНБУРГСКИЙ МОНТАЖНЫЙ КОЛЛЕДЖ"", СНИЛС=12733562351, ИНН=666401166129, E=bulr1@ya.ru, G=Валерий Николаевич, SN=Чистяков, CN=Чистяков Валерий Николаевич
Основание: я подтверждаю этот документ своей квалифицированной подписью
Местоположение: место подписания
Дата: 2025.07.11 16:58:32+05'00'
Foxit Reader Версия: 10.1.1

Рабочая программа учебной дисциплины **«Основы информационной безопасности»** разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности **09.02.11 «Разработка и управление программным обеспечением».**

Организация-разработчик: ГАПОУ СО «Екатеринбургский монтажный колледж»

Разработчик Кузьмин В.П., преподаватель ГАПОУ СО «Екатеринбургский монтажный колледж».

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности является частью основной образовательной программы в соответствии с ФГОС СПО 09.02.11 «Разработка и управление программным обеспечением»

1.2. Место дисциплины в структуре основной образовательной программы:

Общепрофессиональная дисциплина профессионального цикла (ОП.05)

1.3. Цель и планируемые результаты освоения дисциплины:

Код ОК, ПК	*Умения*	*Знания*
ОК 1, ОК 3, ОК 5, ОК 6, ОК 9, ПК 1.5, ПК 3.3	– Определение угроз объекта информатизации и их классификация – Определение путей распространения и форм проявления компьютерных вирусов – Поддержание групп мер процедурного уровня и дать оценку уровню поддержания безопасности – Определение программно-технических методов защиты информационной безопасности по условию	– Основные понятия и задачи информационной безопасности Состав, структуру, принципы реализации и функционирования информационных технологий. – Понятие угрозы. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности. Классификация атак. Сетевые атаки. Окно опасности. Социальная инженерия. Компьютерная преступность. – Вредоносное ПО. Компьютерные вирусы и средства защиты от них. – Политика безопасности. Программа безопасности. Концепция информационной безопасности – Процедурный уровень информационной безопасности – Программно- технические методы защиты информационной безопасности

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.

ОК 09. Использовать информационные технологии в профессиональной деятельности.
ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации
ПК 3.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы	58
в том числе:	
теоретическое обучение	32
практические занятия	16
Самостоятельная работа	10
Промежуточная аттестация проводится в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работаобучающихся, курсовая работа (проект) *(если предусмотрены)*	Объем часов	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1 Основные понятия и задачи информационной безопасности	**Содержание**	**8**	ОК 01, ОК 03, ОК 05, ОК 06, ОК 09, ПК 1.5, ПК 3.3
	Основные понятия и определения, относящиеся к ИБ. Необходимость защиты информации.	2	
	Основные задачи обеспечения защиты информации.	2	
	Объекты, цели и задачи защиты информации.	2	
	Целостность, доступность и конфиденциальность информации.	2	
Тема 2 Угрозы безопасности защищаемой информации	**Содержание**	**6**	ОК 01, ОК 03, ОК 05, ОК 06, ОК 09, ПК 1.5, ПК 3.3
	Понятие угрозы. Классификация видов угроз ИБ по различным признакам.	2	
	Угрозы доступности, целостности и конфиденциальности. Классификация атак.	2	
	Сетевые атаки. Окно опасности. Социальная инженерия. Компьютерная преступность.	2	
Тема 3 Вредоносное ПО. Компьютерные вирусы и средства защиты от них.	**Содержание**	**6**	ОК 01, ОК 03, ОК 05, ОК 06, ОК 09, ПК 1.5, ПК 3.3
	Понятие компьютерного вируса. Признаки появления вируса.	2	
	Классификация вирусов. Вирусная сигнатура.	2	
	Антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины.	2	
	Тематика практических занятий и лабораторных работ	**6**	
	1. Идентификация признаков заражения вирусом	2	
	2. Анализ вирусной сигнатуры	2	
	3. Сравнение антивирусных программ	2	
	Самостоятельная работа обучающихся	**2**	
	Подготовить сообщение по тему «Антивирусное программное обеспечение: принципы работы, методы обнаружения и удаления вредоносного ПО».	2	
Тема 4 Административный уровень информационной безопасности	**Содержание**	**4**	ОК 01, ОК 03, ОК 05, ОК 06, ОК 09, ПК 1.5, ПК 3.3
	Административный уровень информационной безопасности: основные понятия.	2	
	Политика безопасности. Программа безопасности. Концепция информационной безопасности	2	
Тема 5 Процедурный уровень	**Содержание**	**4**	ОК 01, ОК 03, ОК 05, ОК 06,
	Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на	2	

информационной безопасности	нарушения режима безопасности.		ОК 09, ПК 1.5, ПК 3.3
	Планирование восстановительных работ. Защита информации при работе с посетителями. Организация работы с документами.	2	
	Тематика практических занятий и лабораторных работ	**2**	
	1. Разработка фрагмента процедур информационной безопасности для офиса.	2	
	Самостоятельная работа обучающихся	**4**	
	Создание набора документов, регламентирующих основные аспекты защиты информации в небольшой организации	4	
Тема 6 Программно- технические методы защиты информационной безопасности	**Содержание**	**4**	ОК 01, ОК 03, ОК 05, ОК 06, ОК 09, ПК 1.5, ПК 3.3
	Основные понятия программно- технического уровня ИБ. Парольная аутентификация. Одноразовые пароли. Идентификация/ аутентификация с помощью биометрических данных.	2	
	Протоколирование. Активный аудит. Криптография. Стеганография. Управление доступом.	2	
	Тематика практических занятий и лабораторных работ	**8**	
	1. Реализация и анализ парольной аутентификации	2	
	2. Генерация и использование одноразовых паролей (OTP)	2	
	3. Исследование методов протоколирования и активного аудита	2	
	4. Практическое применение криптографии для защиты данных	2	
	Самостоятельная работа обучающихся	**4**	
	Подготовить сообщения по темам «Криптографические методы защиты информации: алгоритмы шифрования, хеширования и электронной подписи.», «Безопасность беспроводных сетей: протоколы, методы защиты и аудит безопасности».	4	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие лаборатории разработки баз данных и информационной безопасности;

Оборудование лаборатории и рабочих мест лаборатории:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся;
- компьютер с лицензионным программным обеспечением;
- мультимедиа проектор;

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд ГАПОУ СО «ЕМК» обладает следующим перечнем используемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Баранова, Е. К. Основы информационней безопасности : учебник / Е.К. Баранова, А.В. Бабаш. — Москва : РИОР : ИНФРА- М, 2022. — 202 с.
2. Бубнов А. А. Основы информационной безопасности : учеб. для студ. учреждений сред. проф. образования / А.А.Бубнов, В.Н.Пржегорлинский, О.А.Савинкин. — 3- е изд., стер. — М. : Издательский центр «Академия», 2020. — 256 с.
3. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 135 с.

3.2.2. Дополнительные источники

1. www.osp.ru (Издат. Открытые системы)
2. www.compres.ru (Журнал Компьютер-пресс)
3. www.ibxt.ru (Новости вычислительной техники)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Перечень знаний, осваиваемых в рамках дисциплины: –Основные понятия и задачи информационной безопасности Состав, структуру, принципы реализации и функционирования информационных технологий. –Понятие угрозы. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности. Классификация атак. Сетевые атаки. Окно опасности. Социальная инженерия. Компьютерная преступность. –Вредоносное ПО. Компьютерные вирусы и средства защиты от них. –Политика безопасности. Программа безопасности. Концепция информационной безопасности –Процедурный уровень информационной безопасности –Программно- технические методы защиты информационной безопасности	«5» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «4» - теоретическое содержание курса освоено полностью, без некоторые пробелов, умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «3» - 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. «2» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Компьютерное тестирование на знание терминологии по теме; Наблюдение за выполнением практического задания. (деятельностью студента) Оценка выполнения практического задания(работы)
Перечень умений, осваиваемых в рамках дисциплины: –Определение угроз объекта информатизации и их классификация –Определение путей распространения и форм проявления компьютерных вирусов Поддержание групп мер процедурного уровня и дать оценку уровню поддержания безопасности –Определение программно-технических методов защиты информационной безопасности по условию		