

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОСТОВСКОЙ ОБЛАСТИ

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
РОСТОВСКОЙ ОБЛАСТИ**

«КАМЕНСКИЙ ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ:

Директор ГБПОУ РО «КамПК»

Н.А. Гайдаенко

« 16 » декабря 2025 г.

ГАЙДАЕН
КО
НАТАЛЬЯ
АЛЕКСАН
ДРОВНА

Подписано
цифровой
подписью:
ГАЙДАЕНКО
НАТАЛЬЯ
АЛЕКСАНДРОВНА
Дата: 2026.03.10
13:39:29 +03'00'

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

в рамках профессиональной образовательной программы среднего профессио-
нального образования (ППССЗ)

по специальности **09.02.11 Разработка и управление программным
обеспечением**

Форма обучения: очная

г. Каменск – Шахтинский
2025г.

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Минпросвещения России от 24 февраля 2025 года № 138, учебного плана, примерной рабочей программы учебной дисциплины «Основы информационной безопасности», Положения о разработке рабочих программ учебных дисциплин.

Организация-разработчик: ГБПОУ РО «Каменский педагогический колледж»

Разработчики: Губа И.М., преподаватель информатики высшей квалификационной категории, Пашкевич А.А., преподаватель информатики

Программа рассмотрена на заседании ПЦК информатики и математики

Протокол № 3 от 07 ноября 2025 г.

Председатель ПЦК информатики и математики  И.М. Губа

Рабочая программа одобрена Методическим Советом колледжа

Протокол № 2 от 12 ноября 2025 г.

Председатель Методического Совета колледжа  Г.В. Звездунова

СОДЕРЖАНИЕ

	Стр.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ <i>ОП.05. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</i> ..4	
2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ7	
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ 10	
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ..... 11	

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

1.1. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «Основы информационной безопасности» принадлежит к общепрофессиональному циклу (ОП.00) образовательной программы и включена в обязательную часть образовательной программы.

1.2. Цель и планируемые результаты освоения учебной дисциплины.

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

В рамках освоения программы учебной дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01	– распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; – составлять план действия; определять необходимые ресурсы; – владеть актуальными методами работы в профессиональной и смежных сферах – реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	– актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; – алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	
ОК.02	– определять задачи для поиска информации; определять необходимые источ-	– номенклатура информационных источников,	

Код ОК, ПК	Уметь	Знать	Владеть навыками
	ники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	
ОК.09	– понимать тексты на базовые профессиональные темы	– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	
ПК 1.1		– принципы безопасности хранения данных	
ПК 1.4		– методы защиты баз данных от внешних угроз	
ПК 1.5	– шифровать данные и обеспечивать их конфиденциальность	– принципы криптографии и методов шифрования данных – стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др. – методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных – законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.	
ПК 3.1		– отраслевая нормативная техническая документация	
		– источники информации, необходимой для профессиональной деятельности	
		– современный отечественный и зарубежный опыт в профессиональной деятельности	

Код ОК, ПК	Уметь	Знать	Владеть навыками
ПК 3.2		– принципы и методы обеспечения безопасности информационных систем	
ПК 3.3	– анализ требований безопасности информационных систем	– принципов безопасности информационных систем – современных методов и технологий в области безопасности информационных систем – законодательных и нормативных актов в области безопасности информационных систем	– применение современных методов и технологий в области безопасности информационных систем
ПК 3.5		– источники угроз информационной безопасности и меры по их предотвращению	
ПК 3.7	– разрабатывать и реализовывать меры безопасности – реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	– основные угрозы безопасности мобильных приложений – принципы криптографии и шифрования данных. – стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect – законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA – основные принципы безопасности информации и методов ее защиты. – стандартные криптографические алгоритмы для шифрования данных – принципы обеспечения безопасности передачи данных по сети – основы безопасности приложений и инфраструктуры – методы анализа на уязвимости и мониторинга безопасности – знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений	– использование шифрования данных для защиты конфиденциальной информации, такой как пароли, персональные данные пользователей и другие чувствительные данные. – применение механизмов хеширования для защиты паролей пользователей от несанкционированного доступа. – обеспечение безопасности передачи данных между клиентскими устройствами и серверами с использованием протоколов шифрования, таких как SSL/TLS – соблюдение законодательства и регуляций в области защиты данных

<i>Код ОК, ПК</i>	Уметь	Знать	Владеть навыками
		– понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения – знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы	

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем рабочей программы учебной дисциплины:	82
в том числе в форме практической подготовки	42
в том числе:	
теоретическое обучение	28
практические занятия	42
курсовая работа (проект)	-
<i>Самостоятельная работа</i>	4
Промежуточная аттестация в форме экзамена	8
в т.ч. консультации	2

2.2. Тематический план и содержание учебной дисциплины «ОП. 05. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Наименование разделов и тем	Содержание учебного материала практические занятия, самостоятельная работа обучающихся		Объем часов	Коды компетенций, формированию которых способствует элемент	
1	2		3	4	
Раздел 1. Основы информационной безопасности			74	ОК. 01, ОК.02, ОК.09, ПК. 1.1, ПК.1.4, ПК.1.5, ПК.3.1, ПК.3.2, ПК.3.3, ПК.3.5, ПК.3.7	
Тема 1.1. Правовое и организационное обеспечение информационной безопасности	<i>Содержание</i>		8		
	1	Введение в безопасность веб-приложений.			
	2	Понятие защиты информации, безопасности веб-приложений.			
	3-4	Законодательство РФ в сфере защиты информации			
	5-6	Источники права на доступ к информации. Уровни доступа к информации			
	7-8	Организационное обеспечение информационной безопасности.			
	Практические занятия 1. Изучение международных стандартов информационного обмена. 2. <i>Обзор стандартов в области информационной безопасности</i> 3. Анализ ФЗ и норм законодательства, обеспечивающих безопасность информации 4. Изучение ответственности за нарушение законодательства в информационной сфере 5. Изучение проекта системы информационной безопасности в организации		10		
Самостоятельная работа обучающихся: 1. Составление схемы по уровням доступа информации. 2. Составление таблицы «Ответственность за нарушение законодательства		2			
Тема 1.2. Криптографическое закрытие информации	<i>Содержание</i>		6		ОК. 01, ОК.02, ОК.09, ПК. 1.1, ПК.1.4, ПК.1.5, ПК.3.1, ПК.3.2, ПК.3.3, ПК.3.5, ПК.3.7
	1	Введение в криптографию.			
	2	Методы криптографического преобразования данных. Шифрование. Кодирование			
	3-4	Типы криптографических систем: симметричные криптосистемы			
	5-6	Типы криптографических систем. Системы с открытым ключом, электронная цифровая подпись	10		
	Практические занятия 1. Криптология и этапы ее развития. 2. Шифрование заменой (подстановка) 3. Шифрование методом перестановки 4. Цифр Цезаря 5. Шифрование с помощью алгебраических преобразований				
	Самостоятельная работа обучающихся: 1. Подготовка сообщения по теме «Шифрование методом гаммирования».			1	
	Контрольная работа по темам 1.1 и 1.2		1		
Тема 1.3. Защита информации в автома-	<i>Содержание</i>		14	ОК. 01, ОК.02, ОК.09, ПК. 1.1,	
	1-2	Понятие угрозы. Источники угроз информационной безопасности и меры по их предотвращению			

тизированных си- стемах обработки данных (АСОД)	3-4	Предотвращение несанкционированного доступа. Основные этапы допуска к компьютер- ным ресурсам		ПК.1.4, ПК.1.5, ПК.3.1, ПК.3.2, ПК.3.3, ПК.3.5, ПК.3.7
	5-6	Идентификация пользователей при доступе к компьютерным ресурсам. Использование па- роля		
	7-8	Понятие компьютерного вируса. Классификация компьютерных вирусов.		
	9-10	Методы защиты от компьютерных вирусов Антивирусные программы		
	11	Информационная безопасность в вычислительных сетях.		
	12	Угрозы информационно-программному обеспечению, характерные только для рас- пределенной вычислительной среды		
	13	Проблемы обеспечения безопасности в сетях Межсетевые экраны		
	14	Контроль информационного наполнения (контента) электронной почты и Web- трафика		
	Практические занятия 1. Функции и методы защиты информации в АСОД. Механизмы защиты информации. 2. Изучение методов и систем защиты информации. 3. Способы разграничения доступа к компьютерным ресурсам. 4. Организация разграничения доступа пользователей средствами операционной системы. 5. Анализ пароля на его устойчивость к подбору. 6. Организация парольной защиты ПК. 7. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. 8. Изучение антивирусного пакета. 9. Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспе- чения информационной безопасности. 10.Изучение работы брандмауэра.		20	ОК. 01, ОК.02, ОК.09, ПК. 1.1, ПК.1.4, ПК.1.5, ПК.3.1, ПК.3.2, ПК.3.3, ПК.3.5, ПК.3.7
	Самостоятельная работа обучающихся: 1. Составление таблицы по компьютерным ресурсам		1	
	<i>Контрольная работа по теме 1.3</i>		1	
Консультации к промежуточной аттестации			2	
Промежуточная аттестация (экзамен)			6	
Всего			82	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенный оборудованием и техническими средствами обучения:

- рабочее место преподавателя;
- рабочие места обучающихся (по количеству обучающихся);
- шкаф или полки для хранения учебной и методической литературы
- учебные наглядные пособия (таблицы, плакаты);
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся;
- ПК преподавателя (системный блок, монитор, клавиатура, мышь);
- мультимедийный проектор.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Печатные издания

- 1) Партыка Т.Л., Попов И.И. Информационная безопасность. – М: ФОРУМ: ИНФРА-М, 2021. – 432с.
- 2) Алябышева Ю.А., Данько Е.В. и др. Введение в безопасность Web-приложений: учебное пособие / Ю.А. Алябышева, Е.В. Данько, О.В. Константинова, Т.В. Михеева, О.Н. Половикова, Л.Л. Смолякова, О.С. Терновой; Барнаул – АлтГУ, 2021

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Формы и методы оценки</i>
Знает: - актуальный профессиональный и социальный контекст, в котором приходится работать и жить; - основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; - алгоритмы выполнения работ в профессиональной и смежных областях; - методы работы в профессиональной и смежных сферах; - структуру плана для решения задач; - порядок оценки результатов решения задач профессиональной деятельности - номенклатуру информационных источников, применяемых в профессиональной деятельности; - приемы структурирования информации; - формат оформления результатов поиска информации, современные средства и устройства информатизации; - порядок применения современных средств и устройств информатизации и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств; - лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; - принципы безопасности хранения данных; - методы защиты баз данных от внешних угроз - принципы криптографии и методов шифрования данных; - стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; - отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; - современный отечественный и зарубежный опыт в профессиональной деятельности; - принципы и методы обеспечения безопасности информационных систем; - принципы безопасности информационных систем; - современные методы и технологии в области безопасности информационных систем; - законодательные и нормативные акты в области безопасности информационных систем; - источники угроз информационной безопасности и меры по их предотвращению; - основные угрозы безопасности мобильных приложений; - принципы криптографии и шифрования данных; - стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;	«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 гру-	• Компьютерное тестирование на знание терминологии по теме. • Наблюдение за выполнением практического задания (деятельностью студента). • Оценка выполнения практического задания(работы). • Подготовка тезисов по теме. • Оценка выполнения индивидуального задания.

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Формы и методы оценки</i>
- законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на уязвимости и мониторинга безопасности; - знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.	бые ошибки.	
Умеет: -распознавать задачу и/или проблему в профессиональном и/или социальном контексте; -анализировать задачу и/или проблему и выделять её составные части; - определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; -составлять план действия; - определять необходимые ресурсы; - владеть актуальными методами работы в профессиональной и смежных сферах; - реализовывать составленный план; - оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); - определять задачи для поиска информации; - определять необходимые источники информации; - планировать процесс поиска; - структурировать получаемую информацию; - выделять наиболее значимое в перечне информации; - оценивать практическую значимость результатов поиска; - оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; - использовать современное программное обеспечение; - использовать различные цифровые средства для решения профессиональных задач; - понимать тексты на базовые профессиональные темы; - шифрование данных и обеспечивает их конфиденциальность; - анализировать требования безопасности информационных систем; - разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.		

