Приложение
к ППССЗ по специальности
09.02.11 Разработка и управление
программным обеспечением

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности

09.02.11 РАЗРАБОТКА И УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Базовая подготовка

среднего профессионального образования

(год начала подготовки 2026)

СОДЕРЖАНИЕ

1.ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 Основы информационной безопасности

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью основной образовательной программы подготовки специалистов среднего звена (далее – ППССЗ) в соответствии с ФГОС по специальности (специальностям) СПО
09.02.11 Разработка и управление программным обеспечением **квалификации выпускника** Программист.

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании в рамках реализации программ переподготовки кадров в учреждениях СПО.

1.2. Место учебной дисциплины в структуре ППССЗ:

Учебная дисциплина *«Основы информационной безопасности»* относится к общему профессиональному циклу основной профессиональной образовательной программы.

1.3. Цель и планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Уметь	Знать	Владеть навыками
ОК.01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	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	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	-

	действий (самостоятельно или с помощью наставника)	задач профессиональной деятельности	
ОК.02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	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	номенклатура информационных источников, 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 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.1 Проектировать базы данных.	-	принципы безопасности хранения данных	-
ПК 1.4 Администрировать базы данных	-	методы защиты баз данных от внешних угроз	-
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации.	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 Собирать исходные данные для разработки проектной документации на информационную систему.	-	отраслевая нормативная техническая документация источники информации, необходимой для профессиональной деятельности	-
		современный отечественный и зарубежный опыт в профессиональной деятельности	-
ПК 3.2 Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.	-	принципы и методы обеспечения безопасности информационных систем	-
ПК 3.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	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 Интегрировать	-	источники угроз	-

информационную систему с существующими информационными системами заказчика.		информационной безопасности и меры по их предотвращению	
ПК 3.7 Разрабатывать техническую документацию на эксплуатацию информационной системы.	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 понимание различных уязвимостей и угроз безопасности, а также способов их	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

		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

2.1Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**44**
в том числе:	
теоретическое обучение	16
практические занятия	16
Самостоятельная работа	12

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 программы
1	2	3	
Раздел 1. Информационная безопасность и уровни ее обеспечения 30/6/16/8			
Тема 1.1. Составляющие информационной безопасности	**Содержание учебного материала**	**10/2/6/2**	
	Составляющие информационной безопасности	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практические занятия		
	Практическое занятие №1. Анализ источников, каналов распространения и каналов утечки информации	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие №2. Проведение анализа информации на предмет целостности	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие №3. Оценка уязвимости информации	2	ОК 1, ОК 2, ОК 9, 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		
	Концепция информационной безопасности	2	
Тема 1.2. Стандарты информационной безопасности: "Общие критерии"	**Содержание учебного материала**	12/2/6/4	
	Стандарты информационной безопасности	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие		
	Практическое занятие №4. Требования к безопасности информационных систем	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие№5. Требования к безопасности информационных систем в России	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие№6. Оценка состояния безопасности ИС	2	ОК 1, ОК 2, ОК 9, 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		
	Политики безопасности в компьютерных сетях	4	
Тема 1.3. Стандарты информационной безопасности распределенных систем	**Содержание учебного материала**	8/2/4/2	
	Стандарты информационной безопасности распределенных систем	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК

			3.3, ПК 3.5, ПК 3.7
	Практические занятия		
	Практическое занятие№7. Определение классов защищенности средств вычислительной техники от несанкционированного доступа	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Практическое занятие№8. Определение требований к защите информации	2	ОК 1, ОК 2, ОК 9, 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		
	Угрозы информационной безопасности в компьютерных системах	2	
Раздел 2. Компьютерные вирусы и защита от них		14/10/-/4	
Тема 2.1. Вирусы как угроза информационной безопасности	**Содержание учебного материала**	6/4/-/2	
	Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов.	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Трудности в определении отличий вирусов от обычных программ.	2	ОК 1, ОК 2, ОК 9, 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:		
	Защита информации от несанкционированного доступа	2	
Тема 2.2.	**Содержание учебного материала**	4/2/-/2	

Классификация компьютерных вирусов	Классификация компьютерных вирусов по среде обитания. Классификация по особенностям алгоритма работы.	2	ОК 1, ОК 2, ОК 9, 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		
	Криптографические методы защиты информации	2	
Тема 2.3. Антивирусные программы	**Содержание учебного материала**	4/4/-/-	
	Особенности работы антивирусных программ. Классификация антивирусных программ.	2	ОК 1, ОК 2, ОК 9, ПК 1.1, ПК 1.4, ПК 1.5, ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7
	Антивирусные сканеры. Блокировщики и иммунизаторы.	2	ОК 1, ОК 2, ОК 9, 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		**12**	
Всего:		**44**	

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение реализации учебной дисциплины:

Учебная дисциплина реализуется в учебном кабинете №302 «Информационно-коммуникационные системы».

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2. Информационное обеспечение обучения

1. Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2022. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118234

2. Долозов, Н. Л. Программные средства защиты информации : учебное пособие / Н. Л. Долозов, Т. А. Гультяева. — Новосибирск : НГТУ, 2023. — 63 с. — ISBN 978-5-7782-2753-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118200

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Освоение содержания учебной дисциплины ОП.05 Основы информационной безопасности обеспечивает достижение студентами определенных результатов**.**

Результаты обучения	Показатели освоенности компетенций	Методы оценки
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	Ориентируется в профессиональном и социальном контексте, в котором приходится работать и жить; Владеет основными источниками информации и ресурсами для решения задач и проблем в профессиональном и/или социальном контексте; Знает алгоритмы выполнения работ в профессиональной и смежных областях; Знает методы работы в профессиональной и смежных сферах; Знает структуру плана для решения задач; Может произвести оценку результатов решения задач профессиональной деятельности Владеет номенклатурой информационных источников, применяемых в профессиональной деятельности; Знает приемы структурирования информации; Знает формат оформления результатов поиска информации, современные средства и устройства информатизации; Может применять современные средства и устройства информатизации и программное обеспечение в	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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;	профессиональной деятельности в том числе с использованием цифровых средств; Владеет лексическим минимумом, относящимся к описанию предметов, средств и процессов профессиональной деятельности; Знает принципы безопасности хранения данных; Владеет методами защиты баз данных от внешних угроз Знает принципы криптографии и методов шифрования данных; Ориентируется в стандартах и протоколах безопасности, таких как SSL/TLS, SSH, Kerberos и др.; Знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы 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; - 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;	Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений;	

- 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. ***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;	Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы. Может распознавать задачу и/или проблему в профессиональном и/или социальном контексте; Анализирует задачу и/или проблему и может выделить её составные части; Умеет определять этапы решения задачи; Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять необходимые ресурсы; Владеет актуальными методами работы в профессиональной и смежных сферах; Может реализовывать составленный план; Оценивает результат и последствия своих действий (самостоятельно или с помощью наставника); Умеет определять задачи для	

- 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.	поиска информации; Умеет определять необходимые источники информации; Планирует процесс поиска; Умеет структурировать получаемую информацию; Может выделить наиболее значимое в перечне информации; Умеет оценивать практическую значимость результатов поиска; Оформляет результаты поиска и применяет средства информационных технологий для решения профессиональных задач; Может использовать современное программное обеспечение; Может использовать различные цифровые средства для решения профессиональных задач; Понимает тексты на базовые профессиональные темы; Умеет шифровать данные и обеспечивать их конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	

5. Перечень используемых методов обучения:

5.1 Пассивные:

- лекции традиционные без применения мультимедийных средств и безраздаточного материала;
- демонстрация учебных фильмов;
- рассказ;
- семинары, преимущественно в виде обсуждения докладов студентов по темили иным вопросам;
- самостоятельные и контрольные работы;
- тесты;
- чтение и опрос.

(взаимодействие преподавателя как субъекта с обучающимся как объектомпознавательной деятельности).

5.2 Активные и интерактивные:

- активные и интерактивные лекции;
- работа в группах;
- учебная дискуссия;
- деловые и ролевые игры;
- игровые упражнения;
- творческие задания;
- круглые столы (конференции) с использованием средств мультимедиа;
- решение проблемных задач;
- анализ конкретных ситуаций;
- метод модульного обучения;
- практический эксперимент;
- обучение с использованием компьютерных обучающих программ.

(*взаимодействие преподавателя как субъекта с обучающимся как субъектом познавательной деятельности).*