МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ НИЖЕГОРОДСКОЙ ОБЛАСТИ

ГБПОУ ЛЫСКОВСКИЙ АГРОТЕХНИЧЕСКИЙ ТЕХНИКУМ

ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЛЫСКОВО
2026 г.

ОДОБРЕНА

Предметной (цикловой) комиссией

Протокол №1 от 01 сентября 2026г.

Председатель П(Ц)К ППССЗ СПО

_____Егорова В.А

Программа разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (СПО):

09.02.11 Разработка и управление программным обеспечением

Заместитель директора по УПР _____ Гуляева Т.В.

Организация-разработчик: ГБПОУ Лысковский агротехнический техникум

Разработчики:

Андреева Наталья Александровна - преподаватель ГБПОУ Лысковский агротехнический техникум

Анучина Марина Дмитриевна - преподаватель ГБПОУ Лысковский агротехнический техникум

Царегородцева Ольга Владимировна - преподаватель ГБПОУ Лысковский агротехнический техникум

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

1.1 Область применения программы

Рабочая программа учебной дисциплины ОП.05 Основы информационной безопасности предназначена для реализации требований Федерального государственного образовательного стандарта и является частью программы подготовки специалистов среднего звена по специальности 09.02.11 Разработка и управление программным обеспечением, входящей в состав укрупнённой группы специальностей 09.00.00 Информатика и вычислительная техника.

Программа учебной дисциплина разработана в рамках образовательной программы по специальности среднего профессионального образования 09.02.11 Разработка и управление программным обеспечением, утвержденного приказом Минпросвещения Российской Федерации от 24 февраля 2025 года № 138 (зарегистрировано в Минюсте России 31.03.2025 г. № 81696) и с учетом профессионального стандарта «Программист», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 года №679н, интересов работодателей в части освоения дополнительных видов профессиональной деятельности, обусловленных требованиями к компетенции «Разработка программного обеспечения».

Рабочая программа учебной дисциплины может быть использована для базовой подготовки в дополнительном профессиональном образовании и в программах профессиональной подготовки (программах повышения квалификации и переподготовке) обучающихся по специальности укрупненной группы 09.00.00 Информатика и вычислительная техника.

1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

Учебная дисциплина принадлежит общепрофессиональному учебному циклу программы подготовки специалистов среднего звена.

1.3. Цели и задачи дисциплины - требования к результатам освоения дисциплины:

В результате изучения дисциплины студент должен освоить соответствующие общие компетенции:

Код	Наименование общих и профессиональных компетенций
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 09.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 1.1	Проектировать базы данных.
ПК 1.4	Администрировать базы данных.
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 3.1	Выполнять техническое проектирование бизнес-приложений и сопровождение проектных решений.
ПК 3.2	Разрабатывать бизнес-приложения.
ПК 3.3	Модифицировать бизнес-приложения.
ПК 3.5	Выполнять внедрение бизнес-приложений и их интеграцию с информационными системами (сервисами).
ПК 3.6	Осуществлять поддержку и обслуживание бизнес-приложений.

В результате освоения дисциплины студент должен освоить следующие:

Код ПК, ОК	Умения	Знания
ОК.01,ОК.02, ОК.09,ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3, ПК 3.5, ПК 3.7	– Классифицировать защищаемую информацию по видам тайны и степеням секретности – классифицировать основные угрозы безопасности информации;	– сущность и понятие информационной безопасности, характеристику ее составляющих – место информационной безопасности в системе национальной безопасности страны – виды, источники и носители защищаемой информации – источники угроз безопасности информации и меры по их предотвращению – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи – современные средства и способы обеспечения информационной безопасности – основные методики анализа угроз и рисков информационной безопасности

Дескрипторы сформированности компетенций по разделам профессиональной дисциплины ОП.05 Основы информационной безопасности

Спецификация ПК (ОК) / разделов профессиональной дисциплины

Код	ПК, ОК	Дискрипторы (показатели сформированности)	Умения	Знания
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в	–

	контекстам	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)	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.	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	Выполнять техническое проектирование бизнес-приложений и сопровождение проектных решений.	– использования типовых бизнес-приложений для автоматизации бизнес-процессов; – сбора, анализа и обработки требований заказчика; – подготовки проектной документации; – эффективной коммуникации с участниками процесса проектирования бизнес-приложений.	– применять типовые бизнес-приложения для автоматизации бизнес-процессов; – осуществлять сбор исходных данных для проектирования бизнес-приложений и описания деятельности, подлежащей автоматизации; – осуществлять логическое проектирование бизнес-приложений; – осуществлять разработку и сопровождения требований и технических; – применять заданные стандарты и шаблоны для составления и оформления проектной документации; – осуществлять коммуникацию с заинтересованными сторонами.	– предметные области автоматизации и ключевых бизнес-процессов: управление продажами, планирование и организация производства, управление материальными потоками, управление кадрами, электронный документооборот, основы управленческого и регламентированного учета; – возможности типовых бизнес-приложений; – возможности программно-технической архитектуры; – возможности средств разработки бизнес-приложений, баз данных, технических средств; – методологию и технологии проектирования и использования баз данных; – методы моделирования и описания устройства и функционирования информационных систем, их частей, обеспечения и окружения;

				− методы функциональной декомпозиции информационных систем; − формальную логику; − основы защиты информации при построении взаимодействия систем и компонентов; − основные стандарты оформления проектной документации.
ПК 3.2	Разрабатывать бизнес-приложения.	− ведения разработки бизнес-приложений, включая клиент-серверные, кроссплатформенные, мобильные, облачные; − создания пользовательских интерфейсов; − работы с нормативно-справочной документацией; − документирования разработки бизнес-приложений; − эффективной коммуникации с участниками процесса разработки бизнес-приложений.	− разрабатывать клиент-серверные, кроссплатформенные, мобильные, облачные бизнес-приложения; − отлаживать и оптимизировать структуры и код бизнес-приложений; − документировать разработку; − осуществлять коммуникацию с заинтересованными сторонами.	− методологии разработки информационных систем и технологий программирования; − бизнес-ориентированные языки программирования и платформ (сред) разработки, реализующих современные подходы к автоматизации бизнес-процессов; − стандарты разработки; − принципы обеспечения качества бизнес-приложений; − основные требования к документированию разработки бизнес-приложений.
ПК 3.3	Модифицировать бизнес-приложения.	− модификации бизнес-приложения (типовых решений) и информационных систем, эксплуатируемых у пользователей; − работы с нормативно-справочной документацией; − документирования разработки бизнес-приложений; − эффективной коммуникации с участниками процесса разработки бизнес-приложений.	− выбирать типовые бизнес-приложения в качестве основы проекта автоматизации бизнес-процессов; − определять область и объем необходимой модификации; − проводить разработку дополнительного функционала; − документировать разработку и тестовые испытания; − осуществлять коммуникацию с заинтересованными сторонами.	− функциональность типовых бизнес-приложений; − принципы обеспечения качества бизнес-приложений; − стандарты поддержки и расширения функциональности типовых бизнес-приложений; − основные требования к документированию разработки бизнес-приложений.
ПК 3.5	Выполнять внедрение бизнес-приложений и их интеграцию с информационными системами (сервисами).	− развертывания бизнес-приложения на рабочих местах пользователей; − развертывания серверной части; − интеграции бизнес-приложений с информационными системами, сервисами, программно-аппаратных обеспечением; − настройки рабочих мест и пользовательского интерфейса; − управления списком и ролями пользователей; − миграции и преобразования данных; − проведения интеграционного тестирования; − документирования ввода в эксплуатацию; − разработки эксплуатационной документации; − эффективной коммуникации с участниками процесса внедрения и интеграции с используемыми информационными системами.	− развертывать бизнес-приложения; − управлять правами доступа; − выбирать сервисы и программно-аппаратное обеспечение для расширения функциональности бизнес-приложений и поддержки цифровой трансформации бизнес-процессов; − применять заданные требования к документированию ввода в эксплуатацию; − применять заданные стандарты и шаблоны для составления и оформления эксплуатационной документации; − осуществлять коммуникации с заинтересованными сторонами.	− стандарты сопровождения и эксплуатации бизнес-приложений; − современные стандарты информационного взаимодействия информационных систем; − механизмы интеграции; − сервисы, расширяющие функциональность бизнес-приложений; − программно-аппаратное обеспечение, используемое в бизнес-процессах при цифровой трансформации.
ПК 3.6	Осуществлять поддержку и обслуживание бизнес-приложений.	− сохранения, восстановления и обновления бизнес-приложения; − выполнения сохранения и резервного копирования данных; − обучения и инструктажа пользователей бизнес-приложений; − эффективной коммуникации с участниками процесса поддержки и обслуживания.	− проверять и контролировать работоспособность бизнес-приложений; − применять заданные требования к процессам поддержки и обслуживания; − осуществления коммуникации с заинтересованными сторонами.	− возможности бизнес-приложений, автоматизирующих задачи организационного управления и бизнес-процессы; − особенности программно-технической архитектуры; − стандарты сопровождения; возможности средств разработки, обновления и модернизации бизнес-приложений.

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	***Объем часов***
Максимальная учебная нагрузка (всего)	
Обязательная аудиторная учебная нагрузка (всего)	*36*
в том числе:	
практические занятия	*16*
Самостоятельная (внеаудиторная) работа обучающегося (всего)	*0*
Итоговая аттестация в форме ***экзамен***	

2.2. Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	***Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся.***		***Объем в часах***	***Коды компетенций, формированию которых способствует элемент программы***
1	*2*		*3*	*4*
Раздел 1. Основы информационной безопасности			***36***	
Тема 1.1. Введение в информационную безопасность	***Содержание учебного материала***	***Уровень освоения***	***1***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	*1,2*	*1*	
Тема 1.2. Управление безопасностью информации	***Содержание учебного материала***	***Уровень освоения***	***1***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	*1,2*	*1*	
Тема 1.3. Криптография	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	*1,2*	*2*	
	Практические занятия		***2***	
	Практическая работа №1. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		*2*	
Тема 1.4. Защита сетевой инфраструктуры	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	*1,2*	*2*	
	Практические занятия		***4***	
	Практическая работа №2. Организация защиты от атак		*2*	
	Практическая работа №3. Организация работы VPN и межсетевого экрана		*2*	
Тема 1.5.	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1,*

Безопасность приложений	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	*1,2*	*2*	*ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Практические занятия		***2***	
	Практическая работа №4. Тестирование на проникновение и анализ уязвимостей.		*2*	
Тема 1.6. Защита данных	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	*1,2*	*2*	
	Практические занятия		***2***	
	Практическая работа №5. Выполнение резервного копирования и восстановления данных. Управление доступом к данным		*2*	
Тема 1.7. Безопасность облачных технологий	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	*1,2*	*2*	
	Практические занятия		***2***	
	Практическая работа №6. Изучение модели облачных услуг и их безопасности		*2*	
Тема 1.8. Инциденты безопасности	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	*1,2*	*2*	
	Практические занятия		***2***	
	Практическая работа №7. Работа с инцидентами.		*2*	
Тема 1.9. Социальная инженерия и человеческий фактор	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	*1,2*	*2*	
	Практические занятия		***2***	
	Практическая работа №8. Разработка политики информационной безопасности		*2*	
Тема 1.10. Будущее информационной безопасности	***Содержание учебного материала***	***Уровень освоения***	***2***	*ОК.01,ОК.02, ОК.09, ПК1.1, ПК1.4,ПК1.5, ПК 3.1,ПК 3.2, ПК 3.3,ПК 3.5, ПК 3.7*
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	*1,2*	*2*	
	Дифференцированный зачет		***2***	

	Всего:	***36***	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1 – ознакомительный (воспроизведение информации, узнавание (распознавание), объяснение ранее изученных объектов, свойств и т.п.);
2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3 – продуктивный (самостоятельное планирование и выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1 Требования к минимальному материально-техническому обеспечению

Реализация учебной дисциплины требует наличие лабораторий «Вычислительной техники, архитектуры персонального компьютера и периферийных устройств», «Программирования и баз данных» оснащенных необходимым для реализации программы учебной дисциплины оборудованием.

Оборудование кабинета

Комплект учебной мебели:

- столы;
- стулья;
- столы компьютерные;

Технические средства обучения:

- компьютеры;
- ноутбуки;
- мультимедийный проектор;
- доска интерактивная;
- доска магнитно-маркерная;
- сканер; плоттер; принтер;
- микрофон с наушниками;
- программное обеспечение общего и профессионального назначения.
- Сервер.

3.2 Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основной источник:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668 (дата обращения: 15.05.2025).978-5-8199-0754-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1910870

Интернет-ресурсы:

http://www.lessons-tva.info/edu/inf-access/access.html
http://kafiitbgau.narod.ru/Metod/Access/Access.htm
http://www.bestbookit.net/database/access.html

3.3. Организация образовательного процесса

Программа дисциплины имеет практикоориентированную направленность. Реализация программы дисциплины предусматривает выполнение обучающимися заданий для лабораторных и практических занятий с использованием персонального компьютера с лицензионным программным обеспечением и с подключением к информационно-телекоммуникационной сети «Интернет».

Для повышения качества знаний студентов в процессе обучения используются следующие педагогические технологии: лично-ориентированного, познавательно-поискового обучения, метод проектов, технология проблемного обучения, здоровьесберегающие технологии. При использовании проблемных учебных занятий, отмечаются повышение познавательной активности студентов, развитие элементарной аналитической деятельности, взаимоуважение и другие образовательные эффекты.

В соответствии с требованиями ФГОС для специальности СПО реализация компетентностного подхода должна предусматривать использование активных и интерактивных форм проведения занятий: компьютерных симуляций – использование электронных образовательных ресурсов, групповых дискуссий, деловых и ролевых игр, разбор конкретных ситуаций, психологических тренингов, индивидуальных и групповых проектов с целью формирования и развития требуемых компетенций студентов.

Реализация программы дисциплины обеспечивается доступом каждого обучающегося к библиотечным фондам, укомплектованным печатными изданиями и (или) электронными изданиями по каждой дисциплине цикла и по каждому профессиональному модулю профессионального цикла из расчета одно печатное издание и (или) электронное издание по каждой дисциплине, модулю на одного обучающегося. Библиотечный фонд должен быть укомплектован печатными изданиями и (или) электронными изданиями основной и дополнительной учебной литературы, вышедшими за последние 5 лет.

В случае наличия электронной информационно-образовательной среды допускается замена печатного библиотечного фонда предоставлением права одновременного доступа не менее 25% обучающихся к электронно-библиотечной системе (электронной библиотеке).

Обучающиеся с ограниченными возможностями здоровья и инвалиды должны быть обеспечены печатными и (или) электронными образовательными ресурсами, адаптированными к ограничениям их здоровья.

Текущий контроль знаний и умений можно осуществлять в форме различных видов опросов на занятиях и во время инструктажа перед лабораторными и практическими занятиями, контрольных работ, различных форм тестового контроля и др. Текущий контроль освоенных умений осуществляется в виде экспертной оценки результатов выполнения лабораторных, практических занятий.

Промежуточная аттестация обучающихся осуществляется в рамках освоения цикла в соответствии с разработанными образовательной организацией фондами оценочных средств, позволяющими оценить достижение запланированных по отдельным дисциплинам результатов обучения. Завершается освоение программы в рамках промежуточной аттестации экзаменом или дифференцированным зачётом, включающем как оценку теоретических знаний, так и практических умений.

При реализации программы дисциплины могут проводиться консультации для обучающихся. Формы проведения консультаций (групповые, индивидуальные, письменные, устные) определяются образовательной организацией.

При реализации образовательной программы образовательная организация вправе применять электронное обучение и дистанционные образовательные технологии.

При обучении лиц с ограниченными возможностями здоровья электронное обучение и дистанционные образовательные технологии должны предусматривать возможность приема-передачи информации в доступных для них формах.

3.4. Кадровое обеспечение образовательного процесса

Реализация образовательной программы обеспечивается руководящими и педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового

договора, в том числе из числа руководителей и работников организаций, деятельность которых связана с направленностью реализуемой образовательной программы (имеющих стаж работы в данной профессиональной области не менее 3 лет).
Квалификация педагогических работников образовательной организации должна отвечать квалификационным требованиям, указанным в профессиональных стандартах «Педагог профессионального обучения, профессионального образования и дополнительного профессионального образования».
Педагогические работники получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях, направление деятельности которых соответствует области профессиональной деятельности не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.
Доля педагогических работников (в приведенных к целочисленным значениям ставок), обеспечивающих освоение обучающимися профессиональных модулей, имеющих опыт деятельности не менее 3 лет в организациях, направление деятельности которых соответствует области профессиональной деятельности в общем числе педагогических работников, реализующих образовательную программу, должна быть не менее 25 процентов.

3. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	– 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;	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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	– 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 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	

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; - законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - основные принципы безопасности информации и методов ее защиты; - стандартные криптографические	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; – 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;	

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. ***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;	– 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; – 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;	

- 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.	– 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 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.	