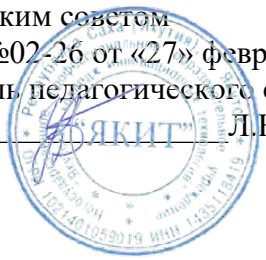
НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
педагогическим советом
(протокол №02-26 от «27» февраля 2026г.)
Председатель педагогического совета
Директор _____ Л.Н. Цой



Рабочая программа дисциплины

ОП.05 Основы информационной безопасности

ППССЗ по специальности

09.02.11 Разработка и управление программным обеспечением

Объем дисциплины - 72 час.

Якутск 2026

Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.11 Разработка и управление программным обеспечением. Укрупненная группа специальностей 09.00.00 Информатика и вычислительная техника.

Разработчики рабочей программы:	НПОУ «ЯКИТ»	преподаватель	Е.А. Соколова
	(место работы)	(должность)	(инициалы, фамилия)

Обсуждено на заседании отделения ИТ — 02 февраля 2026 г. — протокол № 06

Председатель заседания отделения — Зав. отделением —  — И.В. Пронин

Рассмотрено на заседании методического совета — «24» февраля 2026 г. — протокол № 02-26

Председатель методического совета — Директор НПОУ «ЯКИТ» —  — «24» февраля 2026 г. Цой Л.Н.

Заместитель директора по научно-методической работе —  — «24» февраля 2026 г. Зайцева Д.А.

№ п/п	Прилагаемый к Рабочей программе документ, содержащий текст обновления	Решение отделения		Подпись заведующего отделением	Фамилия И.О. заведующего отделением
		дата	Протокол №		
1.	Приложение № 1				
2.	Приложение № 2				
3.	Приложение № 3				
4.	Приложение № 4				
5.	Приложение № 5				

СОДЕРЖАНИЕ

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

1.1. Область применения рабочей программы

Рабочая программа дисциплины является частью образовательной программы в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением.

1.2. Место дисциплины в структуре ППССЗ:

ПП. Профессиональная подготовка

ОП. Общепрофессиональный цикл

ОП.05. Основы информационной безопасности

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

В результате освоения дисциплины обучающийся должен **уметь:**

– 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;

– шифровать данные и обеспечивать их конфиденциальность;

– анализ требований безопасности информационных систем;

– разрабатывать и реализовывать меры безопасности;

– реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.

В результате освоения дисциплины обучающийся должен **знать**:

– 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;

– 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;

– 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;

– отраслевая нормативная техническая документация;

– источники информации, необходимой для профессиональной деятельности;

– современный отечественный и зарубежный опыт в профессиональной деятельности;

– принципы и методы обеспечения 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;

– 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;

– 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.

ПК и ОК, которые актуализируются при изучении дисциплины:

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 Разрабатывать техническое задание на веб-приложение в соответствии с требованиями заказчика.

ПК 3.2 Разрабатывать веб-приложения в соответствии с техническим заданием.

ПК 3.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 3.5 Интегрировать информационную систему с существующими информационными системами заказчика.

ПК 3.7 Разрабатывать техническую документацию на эксплуатацию информационной системы.

1.4. Количество часов на освоение дисциплины:

Максимальной учебной нагрузки обучающегося 72 часов, в том числе:

– обязательная аудиторная учебная нагрузка (всего) – 24 часов; из них практические работы обучающихся (всего) – 12 часа.,

– самостоятельная работа обучающихся (всего)– 48 часов.

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

2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	72
Обязательная аудиторная учебная нагрузка (всего)	72
в том числе:	
Лекционные занятия *(если предусмотрено)*	12
лабораторные занятия *(если предусмотрено)*	-
практическая работа *(если предусмотрено)*	12
контрольные работы *(если предусмотрено)*	-
курсовая работа (проект) *(если предусмотрено)*	-
Самостоятельная работа обучающегося (всего)	48
Промежуточная аттестация	-
Промежуточная аттестация в форме	Зачет с оценкой

2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) *(если предусмотрено)*	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Основы информационной безопасности			
Тема 1.1. Введение в информационную безопасность	**Содержание**	1	1,2
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности		
	Практическая работа	1	-
Тема 1.2. Управление безопасностью информации	**Содержание**	1	1,2
	Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
	Практическая работа	2	-
Тема 1.3. Криптография	**Содержание**	1	1,2
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	Практическая работа	2	1,2

	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
Тема 1.4. Защита сетевой инфраструктуры	**Содержание**	1	1,2
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов		
	Практическая работа	1	1,2
	Организация защиты от атак Организация работы VPN и межсетевого экрана		
Тема 1.5. Безопасность приложений	**Содержание**	1	1,2
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
	Практическая работа	1	1,2
	Тестирование на проникновение и анализ уязвимостей.		
Тема 1.6. Защита данных	**Содержание**	1	1,2
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	Практическая работа	1	1,2
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным		
Тема 1.7. Безопасность облачных технологий	**Содержание**	2	1,2
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		
	Практическая работа	1	1,2
	Изучение модели облачных услуг и их безопасности		
Тема 1.8. Инциденты безопасности	**Содержание**	1	1,2
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		
	Практическая работа	1	1,2
	Работа с инцидентами.		
Тема 1.9. Социальная инженерия и человеческий фактор	**Содержание**	1	1,2
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности		
	Практическая работа	1	1,2
	Разработка политики информационной безопасности		
Тема 1.10.	**Содержание**	2	1,2

Будущее информационной безопасности	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
	Практическая работа	1	-
	Самостоятельная работа	**48**	
	ВСЕГО	**72**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Материально-техническое обеспечение

Лаборатория «Компьютерных сетей и основ информационной безопасности»

Технические средства обучения:

Занятия проводятся в учебной аудитории и компьютерном классе, оснащенных необходимым учебным, методическим, информационным, программным обеспечением.

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет – ресурсов, дополнительной литературы.

Основные источники:

1. 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, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587457

2. 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, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458

Дополнительные источники:

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебник для вузов / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2026. — 352 с. — (Высшее образование). — ISBN 978-5-534-19386-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/586060

2. Черпаков, И. В. Основы программирования : учебник и практикум для среднего профессионального образования / И. В. Черпаков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 196 с. — (Профессиональное образование). — ISBN 978-5-534-18760-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561922

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

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

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 программное обеспечение в профессиональной деятельности	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	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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;	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 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;	

- 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 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;	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; Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-	

-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;	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 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;	

- разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	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.	