МИНИСТЕРСТВО ОБРАЗОВАНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ
Государственное автономное профессиональное образовательное учреждение Архангельской области
«Архангельский политехнический техникум»
(ГАПОУ АО «Архангельский политехнический техникум»)

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ А.В. Афанасьева
«__» ноября 20 25 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОПОП специальности 09.02.11 Разработка и управление программным обеспечением

Уровень образования – основное общее

Преподаватель ФИО

Распределение часов	Количество часов						Промежуточная аттестация без взаимодействия с преподавателем	Вид промежуточной аттестации
	всего	в т.ч. на теорию	в т.ч. на практич. занятия	в т.ч. на курсовой проект (работу)	в т.ч. на самостоятельную работу	в т.ч. на промежуточную аттестацию (во взаимодействии с преподавателем)		
на всю дисциплину по учебному плану	36	16	16		2	2		ДЗ
на 1 семестр								
на 2 семестр								
на 3 семестр	36	16	16		2	2		ДЗ
на 4 семестр								
на 5 семестр								
на 6 семестр								
на 7 семестр								
на 8 семестр								

Программа учебной дисциплины ОП.05 «Основы информационной безопасности» разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее ФГОС СПО) 09.02.11 Разработка и управление программным обеспечением, утверждённого приказом Министерства просвещения Российской Федерации от 24 февраля 2025 г. № 138.

Организация-разработчик: ГАПОУ АО «Архангельский политехнический техникум»

Разработчик:

Козьмина О.Г., преподаватель _____
Ф.И.О., ученая степень, звание, должность подпись

Рассмотрено и одобрено на заседании предметно-цикловой комиссии преподавателей и мастеров производственного обучения строительного профиля, машиностроения, наземного транспорта и беспилотных летательных аппаратов

Протокол № 3 от «12 ноября» 2025 г.

Председатель Машанова М.В. _____
подпись

СОДЕРЖАНИЕ

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 ОП.05 «Основы информационной безопасности» является обязательной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности 09.02.11 Разработка и управление программным обеспечением.

Особое значение учебная дисциплина имеет при формировании и развитии:

Код	Наименование общих 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 03	Планировать и реализовывать собственное профессиональное и личностное развитие
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	Собирать исходные данные для разработки проектной документации на информационную систему
ПК 3.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика
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
ПК 4.5	Осуществлять аудит безопасности веб-приложения в соответствии с регламентом по безопасности
ПК 5.7	Осуществлять защиту данных в мобильных приложениях
ПК 8.7	Осуществлять безопасность ИТ-инфраструктуры

1.2. Цель и планируемые результаты освоения учебной дисциплины:

В рамках программы **учебной дисциплины** обучающимися осваиваются умения и знания

Умения	Знания
− 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.	− 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; - принципы 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.

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины максимальная учебная нагрузка	36

в т. ч.:	
теоретическое обучение	16
практические занятия	16
самостоятельная работа	2
Промежуточная аттестация в форме дифференцированного зачета	2

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Номер учебного занятия	Содержание учебного материала и формы организации деятельности обучающихся	Объем, час.	Коды ПК, ОК и ЛР, формированию которых способствует элемент программы
1	2	3	4	5
Тема 1. Введение в информационную безопасность. Управление безопасностью информации	**Содержание учебного материала**		**2**	**ОК 01 ОК 02 ОК 03 ОК 09 ПК 1.5 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК 3.7 ПК 4.5 ПК 5.7 ПК 8.7**
	1	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности. Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)	2	
Тема 3. Криптография	**Содержание учебного материала**		**2**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	2	**Практическое занятие №1.** Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография. Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения	2	
Тема 4. Защита сетевой инфраструктуры	**Содержание учебного материала**		**6**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	3	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	2	
	4	**Практическое занятие №2.** Организация защиты от атак	2	
	5	**Практическое занятие №3.** Организация работы VPN и межсетевого экрана	2	
Тема 5. Безопасность приложений	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	6	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей	2	
	7	**Практическое занятие №4.** Тестирование на проникновение и анализ уязвимостей	2	
Тема 6. Защита данных	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 ОК 09 ПК 1.1 ПК 1.4 ПК 1.5 ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.5 ПК**
	8	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным	2	
	9	**Практическое занятие №5.** Выполнение резервного копирования и восстановления данных. Управление доступом к данным	2	

				3.7 ПК 4.5 ПК 5.7 ПК 8.7
Тема 7. Безопасность облачных технологий	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	10	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	2	
	11	**Практическое занятие №6.** Изучение модели облачных услуг и их безопасности	2	
Тема 8. Инциденты безопасности	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	12	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	2	
	13	**Практическое занятие №7.** Работа с инцидентами	2	
Тема 9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	14	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	2	
	15	**Практическое занятие №8.** Разработка политики информационной безопасности	2	
Тема 10. Будущее информационной безопасности	**Содержание учебного материала**		**4**	**ОК 01 ОК 02 ОК 03 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 ПК 4.5 ПК 5.7 ПК 8.7**
	16	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности	2	
	17	**Самостоятельная работа №1.** Будущее биометрической аутентификации. Искусственный интеллект в безопасности. Угрозы безопасности в мире «Интернета вещей»	2	
Промежуточная аттестация в виде дифференцированного зачёта			**2**	
Всего (включая самостоятельную работу), час.			**36**	

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Материально-техническое обеспечение:

- лаборатория «Компьютерных сетей и основ информационной безопасности», оснащенная:

1) посадочными местами по количеству обучающихся (столы, стулья);

2) рабочим местом преподавателя;

3) шкафом или полками для хранения учебной и методической литературы;

4) доской маркерной;

5) ПК преподавателя (системный блок, монитор, клавиатура, мышь);

6) ПК (системный блок, монитор, клавиатура, мышь) по количеству обучающихся;

7) мультимедийным проектором;

8) аудио- и видеооборудованием;

9) комплектом учебно-методических материалов.

3.2 Информационное обеспечение реализации программы

3.2.1 Основные печатные и/или электронные издания

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547 (дата обращения: 16.11.2025).

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950 (дата обращения: 16.11.2025).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 16.11.2025)

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 16.11.2025)

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	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 в том числе с использованием цифровых средств; - лексический минимум, относящийся к описанию	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 профессиональной деятельности в том числе с	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

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;	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 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; -анализировать задачу и/или проблему и выделять её составные части;	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-	

- 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;	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; 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;	

- разрабатывать и реализовывать меры безопасности; - реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию	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.	
Промежуточная аттестация в форме дифференцированного зачета		