Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Куижева Саида Казбековна
Должность: Ректор
Дата подписания: 15.10.2026 22:37:43
Уникальный программный ключ:
71183e1134ef9cfa69b206d480271b3c1a975e6f

МИНОБРНАУКИ РОССИИ
политехнический колледж филиала федерального государственного бюджетного образовательного учреждения высшего образования
«Майкопский государственный технологический университет»
в поселке Яблоновском

Предметная (цикловая) комиссия информационных и математических дисциплин

УТВЕРЖДАЮ
Врио директора филиала МГТУ
в поселке Яблоновском
_____ З.Х. Тляшок
«14» 05 2026 г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Наименование дисциплины ОП.05 Основы информационной безопасности

Наименование специальности 09.02.11 Разработка и управление программным обеспечением

Квалификация выпускника программист

Форма обучения очная (на базе основного общего образования)

Яблоновский, 2026

Рабочая программа составлена на основе ФГОС СПО и учебного плана филиала МГТУ в поселке Яблоновском по специальности 09.02.11 Разработка и управление программным обеспечением

Составитель рабочей программы:

преподаватель _____ (подпись) П.В. Николаев

Рабочая программа утверждена на заседании предметной (цикловой) комиссии информационных и математических дисциплин

Председатель предметной
(цикловой) комиссии

«24» 03 2026 г. _____ (подпись) Р.Я. Шартан

СОГЛАСОВАНО:

Начальник УМО филиала МГТУ
в поселке Яблоновском
«24» 03 2026 г. _____ (подпись) З. И. Воронцова

СОДЕРЖАНИЕ

		Стр.
1.	ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	4
2.	СТРУКТУРА И СОДЕРЖАНИЕ ОБРАЗОВАТЕЛЬНОЙ И ВОСПИТАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ ПО РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	6
3.	КАЛЕНДАРНЫЙ ГРАФИК ВОСПИТАТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ	12
4.	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	12
5.	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	14
6.	АДАПТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ	16
7.	ЛИСТ ВНЕСЕННЫХ ИЗМЕНЕНИЙ В ПРОГРАММУ	18

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП 05 Основы информационной безопасности

1.1. Область применения программы

Рабочая программа учебной дисциплины ОП 05 Основы информационной безопасности (далее – программа) является составной частью основной профессиональной образовательной программы филиала МГТУ в поселке Яблоновском в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) по специальности 09.02.11Разработка и управление программным обеспечением

1.2. Место дисциплины в структуре основной образовательной программы

Дисциплина ОП. 05 Основы информационной безопасности входит в перечень дисциплин общепрофессионального цикла.

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

-формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях.

Задачи дисциплины: - способствовать освоению терминологического и понятийного аппарата теории информационной безопасности; - изучить российское и зарубежное законодательство, а также особенности стандартов и спецификаций в области информационной безопасности; - способствовать формированию знаний о возможных информационных угрозах и возможных средств защиты от них; - изучить методологию и основные методы защиты информации от базовых угроз; - способствовать формированию навыков оценки защищенности объектов и эффективности систем обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен:

уметь:

У1-распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части;

У2-определять этапы решения задачи;

У3-выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;

У4-составлять план действия; определять необходимые ресурсы;

У5-владеть актуальными методами работы в профессиональной и смежных сферах

У6-реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)

У7-определять задачи для поиска информации; определять необходимые источники информации;

У8- планировать процесс поиска;

У9- структурировать получаемую информацию; выделять наиболее значимое в перечне информации;

У10-оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач;

У-11использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач

У12-понимать тексты на базовые профессиональные темы

У13-шифровать данные и обеспечивать их конфиденциальность

У14-разрабатывать и реализовывать меры безопасности

У15-реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификаци

знать:

З1-актуальный профессиональный и социальный контекст, в котором приходится работать и жить;

З2-основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте;

З3-алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах;

З4-структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности

З5-номенклатура информационных источников, применяемых в профессиональной деятельности;

З6-приемы структурирования информации;

З7-формат оформления результатов поиска информации, современные средства и устройства информатизации;

З8-порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств;

З9-лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;

З10-принципы безопасности хранения данных;

З11-методы защиты баз данных от внешних угроз;

З12-принципы криптографии и методов шифрования данных;

З13-стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.;

З14-методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных;

З15-законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.;

З16-отраслевая нормативная техническая документация;

З17-источники информации, необходимой для профессиональной деятельности;

З18-современный отечественный и зарубежный опыт в профессиональной деятельности;

З19-принципы и методы обеспечения безопасности информационных систем;

принципов безопасности информационных систем;

З20- 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;

З21-принципы криптографии и шифрования данных;

З22-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;

З23-стандартные криптографические алгоритмы для шифрования данных;

З24-принципы обеспечения безопасности передачи данных по сети;

З25-основы безопасности приложений и инфраструктуры;

З26-методы анализа на уязвимости и мониторинга безопасности;

З27-знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений;

З28-понимание различных уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения;

З29-знание инструментов и технологий для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы

1.4. Компетенции обучающегося, формируемые в результате освоения дисциплины

Образовательная и воспитательная деятельность направлена на формирование у обучающих следующих 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. 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.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП. 05 Основы информационной безопасности
2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Количество часов (всего)	3 семестр
Обязательная аудиторная учебная нагрузка	**32**	**32**
в том числе		
теоретические занятия (Л)	16	16
практические занятия (ПЗ)	16	16
Самостоятельная работа обучающихся (СРС) (всего)	**-**	**-**
Форма промежуточной аттестации -экзамен	**экзамен**	**экзамен**
Общая трудоемкость	**32**	**32**

2.2. Тематический план дисциплины ОП 05 Основы информационной безопасности

2	Шифр и № занятия	Наименование тем	Макс. учебная нагрузка на студента, час.	Количество часов		
				Теоретические занятия	Практические занятия	Промежуточная аттестация
Раздел 1. Основы информационной безопасности						
1.	Л1	Введение в информационную безопасность	1	1	-	-
2.	Л2	Управление безопасностью информации	1	1	-	-
3.	Л3	Криптография	2	2	-	-
4.	ПЗ1	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	-	2	-
5.	Л4	Защита сетевой инфраструктуры	2	2	-	-
6.	ПЗ2	Организация защиты от атак	2	-	2	-
7.	ПЗ3	Организация работы VPN и межсетевого экрана	2	-	2	-
8.	Л5	Безопасность приложений	2	2	-	-
9.	ПЗ4	Тестирование на проникновение и анализ уязвимостей.	2	-	2	-
10.	Л6	Защита данных	2	2	-	-
11.	ПЗ5	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	2	-	2	-
12.	Л7	Безопасность облачных технологий	2	2	-	-
13.	ПЗ6	Изучение модели облачных услуг и их безопасности	2	-	2	-
14.	Л8	Инциденты безопасности	2	2	-	-
15.	ПЗ7	Работа с инцидентами.	2	-	2	-
16.	Л9	Социальная инженерия и человеческий фактор	1	1	-	-
17.	Л10	Будущее информационной безопасности	1	1	-	-
18.	ПЗ8	Разработка политики информационной безопасности	2	-	2	-
ИТОГО			**32**	**16**	**16**	-

2.3. Содержание учебной дисциплины ОП. 05 Основы информационной безопасности

Наименование разделов дисциплины	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Коды формируемых компетенций, осваиваемых знаний и умений
Раздел 1. Основы информационной безопасности			
	Содержание учебного материала		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
Тема 1. Введение в информационную безопасность Тема2.Управление безопасностью информации	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.)		
	Теоретические занятия		
	Введение в информационную безопасность	1	
	Управление безопасностью информации	1	
Тема 1.3. Криптография	**Содержание учебного материала** Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Криптография	2	
	Практические занятия		
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.	2	
Тема 1.4. Защита сетевой инфраструктуры	**Содержание учебного материала** Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Защита сетевой инфраструктуры	2	
	Практические занятия		
	Организация защиты от атак	2	
	Организация работы VPN и межсетевого экрана	2	
Тема 1.5. Безопасность приложений	**Содержание учебного материала** Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Безопасность приложений	2	

	Практические занятия		
	Тестирование на проникновение и анализ уязвимостей	2	
Тема 1.6. Защита данных	**Содержание учебного материала** Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Защита данных	2	
	Практические занятия		
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным	2	
Тема 1.7. Безопасность облачных технологий	**Содержание учебного материала** Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Безопасность облачных технологий	2	
	Практические занятия		
	Изучение модели облачных услуг и их безопасности	2	
Тема 1.8. Инциденты безопасности	**Содержание учебного материала** Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		
	Инциденты безопасности	2	
	Практические занятия		
	Работа с инцидентами	2	
Тема 1.9. Социальная инженерия и человеческий фактор **Тема 1.10. Будущее информационной безопасности**	**Содержание учебного материала** Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности. Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Теоретические занятия		У1-У15, З1-З29, ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7
	Социальная инженерия и человеческий фактор	1	
	Будущее информационной безопасности	1	
	Практические занятия		
	Разработка политики информационной безопасности	2	
Итого		**32**	

3. КАЛЕНДАРНЫЙ ГРАФИК ВОСПИТАТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

Модуль 1. Проектная и проектно-исследовательская деятельность обучающихся

Дата, место, время и формат проведения	Название мероприятия и организатор	Форма проведения мероприятия	Ответственный	Достижения обучающихся
март 2028г. Политехнический колледж филиала МГТУ в поселке Ябloновском	Мастер-класс «Работа с инцидентами»	Групповая	Т.А. Елизарова	Сформированность ОК.05

4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.05 Основы информационной безопасности

4.1. Требования к материально-техническому обеспечению

Лаборатория программирования и баз данных:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- шкаф для хранения раздаточного дидактического материала и др.;
- маркерная доска;
- персональные компьютеры обучающихся – 10 шт.;
- персональный компьютер преподавателя;
- МФУ;
- переносное мультимедийное оборудование;
- программное обеспечение общего и профессионального назначения.

4.2. Информационное обеспечение обучения

Перечень учебных изданий основной и дополнительной литературы, Интернет-ресурсов

Основные электронные издания

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для СПО / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 84 с. — URL: https://e.lanbook.com/book/515089

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для СПО / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 284 с. — URL: https://e.lanbook.com/book/463001

3. Нестеров, С. А. Основы информационной безопасности : учебник для СПО / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2026. — 324 с. — URL: https://e.lanbook.com/book/518575

4. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 7-е изд., стер. — Санкт-Петербург : Лань, 2026. — 124 с. — URL: https://e.lanbook.com/book/515187

Дополнительная литература

1. Мельников, В. П. Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2026. — 267 с.— URL: https://book.ru/book/963258

2. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — 2-е изд. — Саратов : Профобразование, 2024. — 135 с. URL: https://profspo.ru/books/142816

3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с.— URL: https://profspo.ru/books/142285

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОБУЧЕНИЯ И ВОСПИТАНИЯ ПО ДИСЦИПЛИНЕ

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	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)

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	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	

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 алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети; - основы безопасности приложений и инфраструктуры; - методы анализа на	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; 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	

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;	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; Может выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; Составляет план действия; Может определять	

- 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,	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	

сессионные токены и двухфакторную аутентификацию.	конфиденциальность; Умеет анализировать требования безопасности информационных систем; Может разрабатывать и реализовывать меры безопасности; Может реализовывать хэширование паролей, сессионные токены и двухфакторную аутентификацию.	

6. АДАПТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРИ ОБУЧЕНИИ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Адаптация рабочей программы дисциплины ОП. 05 Основы информационной безопасности проводится при реализации адаптивной образовательной программы – программы подготовки специалистов среднего звена по специальности 09.02.11 Разработка и управление программным обеспечением в целях обеспечения права инвалидов и лиц с ограниченными возможностями здоровья на получение профессионального образования, создания необходимых для получения среднего профессионального образования условий, а также обеспечения достижения обучающимися инвалидами и лицами с ограниченными возможностями здоровья результатов формирования практического опыта.

Оборудование лаборатории программирования и баз данных для обучающихся с различными видами ограничения здоровья.

Оснащение лаборатории программирования и баз данных должно отвечать особым образовательным потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья. Кабинет должен быть оснащен оборудованием и учебными местами с техническими средствами обучения для обучающихся с различными видами ограничений здоровья.

Кабинет, в котором обучаются лица с нарушением слуха, должен быть оборудован радиоклассом, компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

Для слабовидящих обучающихся в кабинете предусматриваются просмотр удаленных объектов при помощи видео увеличителей для удаленного просмотра, использование Брайлевской компьютерной техники, электронных луп, программ невизуального доступа к информации, технических средств приема-передачи учебной информации в доступных формах.

Для обучающихся с нарушением опорно-двигательного аппарата кабинет должен быть оборудован передвижной регулируемой партой.

Вышеуказанное оснащение устанавливается в кабинете при наличии обучающихся по адаптированной образовательной программе с учетом имеющегося типа нарушений здоровья у обучающегося.

Информационное и методическое обеспечение обучающихся.

Доступ к информационным и библиографическим ресурсам должен быть представлен в формах, адаптированных к ограничениям здоровья обучающихся инвалидов и лиц с ограниченными возможностями здоровья:

Для лиц с нарушениями зрения (не менее одного вида):

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла;
- в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

- в печатной форме;
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата (не менее одного вида):

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Для лиц с нервно-психическими нарушениями (расстройство аутического спектра, нарушение психического развития) (не менее одного вида):

- использование текста с иллюстрациями;
- мультимедийные материалы.

Во время самостоятельной подготовки обучающиеся инвалиды и лица с ограниченными возможностями здоровья должны быть обеспечены доступом к сети Интернет.

Формы и методы контроля и оценки результатов обучения.

Применяемые при реализации рабочей программы дисциплины ОП.05 Основы информационной безопасности формы и методы контроля проводятся с учетом ограничения здоровья обучающихся.

Целью текущего контроля является своевременное выявление затруднений и отставаний обучающегося с ограниченными возможностями здоровья и внесение коррективов в учебную деятельность.

Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей обучающихся инвалидов и лиц с ограниченными возможностями здоровья (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

При проведении промежуточной аттестации обучающемуся предоставляется время на подготовку к ответу, увеличенное не более чем в три раза, установленного для подготовки к ответу обучающимся, не имеющим ограничений в состоянии здоровья.

7. ЛИСТ ВНЕСЕННЫХ ИЗМЕНЕНИЙ

Дополнения и изменения в рабочей программе
за _____ / _____ учебный год

В рабочую программу дисциплины _____

_____

Специальности 09.02.11 Разработка и управление программным обеспечением

вносятся следующие дополнения и изменения

Дополнения и изменения внес _____ _____
подпись И.О. Фамилия

Рабочая программа пересмотрена и одобрена на заседании предметной (цикловой) комиссии _____

_____

« _____ » _____ 20 _____ г.

Председатель предметной
(цикловой) комиссии _____ _____
подпись И.О. Фамилия