

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Гаврилов Сергей Александрович
Должность: И.О. Ректора
Дата подписания: 31.07.2026 11:54:15
Уникальный программный ключ:
f17218015d82e3c1457d1df9e244def505047355

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет
«Московской институт электронной техники»»

УТВЕРЖДАЮ



Проректор по учебной работе

А.Г. Балашов

«18» *августа* 2026 г.

М.П.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОП. 06 «Основы информационной безопасности»

Специальность среднего профессионального образования:

09.02.12 Техническая эксплуатация и сопровождение информационных систем

Квалификация: специалист по технической эксплуатации и сопровождению
информационных систем

Форма обучения: очная

Нормативный срок обучения: 2 года 10 месяцев
на базе основного общего образования

2026 год

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ ОБЩЕПРОФЕССИОНАЛЬНОГО ЦИКЛА «ОП 06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «Основы информационной безопасности»: формирование у студентов знаний и представлений о смысле, целях и задачах информационной защиты, характерных свойствах защищаемой информации, основных информационных угрозах, существующих направлениях защиты и возможностях построения моделей, стратегий, методов и правил информационной защиты.

Дисциплина «ОП 06 Основы информационной безопасности» включена в обязательную часть общепрофессионального цикла образовательной программы СПО в соответствии с ФГОС СПО по специальности 09.02.12 «Техническая эксплуатация и сопровождение информационных систем».

Особое значение дисциплина имеет при формировании общих компетенций: ОК 01, ОК 02, ОК 09, профессиональных компетенций: ПК 1.7

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, информационные технологии для выполнения задач профессиональной деятельности.

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.7. Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем.

Воспитательный потенциал дисциплины реализуется сквозным методом через формирование общих компетенций 01, ОК 02, ОК 09 в формулировки которых интегрированы личностные результаты реализации рабочей программы Колледжа электроники и информатики.

Общий объем учебного времени на освоение дисциплины сохранен в рамках нормативных требований и составляет 72 академических часов, из которых на освоение теоретических дисциплин отведено 18 часов, на освоение практических занятий – 36 часов, 18 часов для самостоятельной работы.

Рабочая программа разработана с учетом требований ФГОС среднего профессионального образования по специальности 09.02.12 «Техническая эксплуатация и сопровождение информационных систем», профессиональных стандартов и профиля профессионального образования.

В программе теоретические сведения дополняются практическими занятиями в соответствии с учебным планом по специальности, которые изучаются в 4 семестре.

Программа содержит тематический план, отражающий количество часов, выделяемое на изучение разделов и тем в рамках дисциплины «Основы информационной безопасности».

Контроль качества освоения дисциплины проводится в процессе текущего контроля и промежуточной аттестации. Текущий контроль проводится в пределах учебного времени, отведенного на дисциплину, как традиционными, так и инновационными методами, включая компьютерное тестирование. Результаты контроля учитываются при подведении итогов по дисциплине.

1.2. Планируемые результаты освоения дисциплины.

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3 ОП СПО).

В результате освоения дисциплины обучающийся должен:

Код ОК/ ПК	Уметь	Знать	Владеть навыками
ОК 01	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)	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	-
ОК 02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать	номенклатуру информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации,	-

	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	современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.	
ОК 09	понимать тексты на базовые профессиональные темы	лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности	-
ПК 1.7	-идентифицировать инциденты ИБ при работе с ИС в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -осуществлять коммуникации с заинтересованными сторонами в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -разрабатывать документы в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -настраивать СУБД в рамках технической поддержки процессов создания (модификации) и сопровождения ИС	-основы ИБ организации модель угроз информационной безопасности ИС организации заказчика; -процедуры и регламенты передачи информации по инцидентам в службу ИБ заказчика; -основы администрирования СУБД; основы системного администрирования; -коммуникационное оборудование; -сетевые протоколы; -основы современных операционных систем -устройство и функционирование современных ИС; -основы архитектуры мультиарендного программного обеспечения	-распознавание инцидентов ИБ, связанных с работой ИС, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -передача информации об инцидентах в службу ИБ заказчика в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -информирование заинтересованных лиц заказчика и в своей организации об инцидентах ИБ, связанных с работой ИС, для принятия управленческих решений,

			минимизирующих ущерб от инцидента ИБ, в рамках технической поддержки процессов создания (модификации) и сопровождения ИС; -временное блокирование доступа к ИС (при необходимости) при обнаружении инцидентов ИБ в рамках технической поддержки процессов создания (модификации) и сопровождения ИС
--	--	--	---

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Трудоемкость освоения дисциплины

Наименование составных частей дисциплины	Объем в часах	В т.ч. в форме практ. подготовки
Учебные занятия	54	36
Из них:		
Самостоятельная работа	18	-
Практико-ориентированное содержание (Прикладной модуль)	-	-
Промежуточная аттестация	XX	XX
Всего	72	36

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала, практических занятий	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Основы информационной безопасности		54	
Тема 1.1. Введение в информационную безопасность.	Содержание	1	ОК 01, ОК 09
	Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и	1	

	риски в информационной безопасности.		
Самостоятельная работа		2	
Тема 1.2. Управление безопасностью информации.	Содержание	1	ОК 01, ПК 1.7
	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	
Самостоятельная работа		2	
Тема 1.3. Криптография.	Содержание	8	ОК 02, ПК 1.7
	Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.	2	
	В том числе практических занятий	6	
	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.		
Самостоятельная работа		2	
Тема 1.4. Защита сетевой инфраструктуры.	Содержание	12	ОК 02, ПК 1.7
	Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов.	2	
	В том числе практических занятий	10	
	Организация защиты от атак.	6	
	Организация работы VPN и межсетевого экрана.	4	
Самостоятельная работа		2	
Тема 1.5. Безопасность приложений.	Содержание	6	ОК 02, ПК 1.7
	Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.	2	
	В том числе практических занятий	4	
	Тестирование на проникновение и анализ уязвимостей.		
Самостоятельная работа		2	

Тема 1.6. Защита данных.	Содержание	6	ОК 02, ПК 1.7
	Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным.	2	
	В том числе практических занятий	4	
	Выполнение резервного копирования и восстановления данных. Управление доступом к данным.		
Самостоятельная работа		2	
Тема 1.7. Безопасность облачных технологий.	Содержание	6	ОК 02, ПК 1.7
	Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности.	2	
	В том числе практических занятий	4	
	Изучение модели облачных услуг и их безопасности.		
Самостоятельная работа		2	
Тема 1.8. Инциденты безопасности.	Содержание	6	ОК 01, ОК 02, ПК 1.7
	Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика.	2	
	В том числе практических занятий	4	
	Работа с инцидентами.		
Самостоятельная работа		2	
Тема 1.9. Социальная инженерия и человеческий фактор.	Содержание	6	ОК 01, ПК 1.7
	Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности.	2	
	В том числе практических занятий	4	
	Разработка политики информационной безопасности.		
Самостоятельная работа		2	
Тема 1.10. Будущее информационной безопасности.	Содержание	2	ОК 09, ПК 1.7.
	Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности.	2	
Промежуточная аттестация		**	
Всего		72	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория «Основ информационной безопасности», оснащенная в соответствии с приложением 5 настоящей образовательной программы.

№	Наименование оборудования	Техническое описание
I Специализированная мебель и системы хранения		
Основное оборудование		
1	Посадочные места	Стол на металлокаркасе ONIX-П О.МР-SP-1.7 белый бриллиант/белый Ш980 Кресло СН797 сетка, ткань черная (664024)
2	Рабочее место преподавателя	Стол на металлокаркасе ONIX-П П О.МР-SP-4.7 белый бриллиант/бел. Ш 1580 Кресло Бюрократ СН-695NLT ткань черная TW-11/сетка 4ерН.TW-01 пластик
3	Комплект документации, методическое обеспечение	Паспорт кабинета, инструкции по охране труда, журналы инструктажей
II Технические средства		
Основное оборудование		
4	Автоматизированные рабочие места на 17 обучающихся	Моноблок MSI Modem AM242P 12M-1071XRU (9s6- ae0711-1071) Black 23.8" {FHD i7 1255U/16G6/512G6 SSD/noOS с комплектом клавиатура + мышь Acer 0MW141 черный (ZL.MCEEE.01M) – на 17 автоматизированных рабочих мест.
5	Профессиональная панель	Lumien LS8650SD
6	Интерактивная панель	Geckotouch Interactive IP86SL
7	Комплект учебно-наглядных пособий и плакатов	Набор плакатов по тематике

Все виды учебной деятельности обучающихся, предусмотренные учебным планом, в рамках настоящей дисциплины общепрофессионального цикла, включая промежуточную аттестацию, обеспечены расходными материалами. Помещения для организации самостоятельной и воспитательной работы оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную образовательную среду Колледжа электроники и информатики.

Оснащение кабинета «Самостоятельная и воспитательная работа»:

Посадочные места по количеству обучающихся: секция стола складная мобильная CM1, Ш800, белый, кресло- трансформер RIVA CHAIR 1821 пластик белый.

Рабочее место преподавателя: стол на металлокаркасе ONIX-П П О.МР-SP-4.7 белый бриллиант/бел. Ш1580, стол на металлокаркасе ONIX-П О.МР-SP-1.7 белый бриллиант/белый Ш980, Кресло EChair-225 PTW_TW11 сетка/ткань черный.

Моноблок MSI PRO AM242P 14M-668XRU 23.8" Full HD i7 14700/16Gb/SSD512Gb UHDG 770/noOS/kb/m/белый.

Комплект клавиатура и мышь A4tech Fstyler F1010 белый/серый USB.

МФУ Kyocera M2540DN: Технология печати: лазерный. Тип печати: черно-белый. Формат печати: А4. Размещение: настольный. Цвет: белый/серый. Печать: Скорость печати А4 (ч/б): до 40 стр/мин. Время разогрева: 17 с. Время печати первой страницы А4 (ч/б): 6.4 с. Разрешение печати (ч/б): 1200 x 1200 dpi. Нагрузка (А4, в месяц): до 50000 листов. Стандартный лоток подачи: 250 листов. Стандартный выходной лоток: 150 листов. Лоток ручной подачи: 100 листов. Возможности печати: Автоматическая двусторонняя печать в стандартной комплектации. Тип сканера: планшетный/протяжный. Устройство автоподачи: двустороннее реверсивное. Емкость устройства автоподачи: 50 лист. Макс. формат оригинала сканирования: А4. Макс. размер сканирования: 216x297 мм. Разрешение сканера: 600x600 dpi. Объем памяти: 1024 Мб. Частота процессора: 1000 МГц. Лоток подачи: 250 лист. Интерфейсы: USB, Ethernet RJ-45.

Рельсовая система РС-75: Материал профиля - анодированный алюминий. Цвет профиля – серебристый. Количество рабочих поверхностей - 4. Количество неподвижных рабочих поверхностей - 2. Количество подвижных рабочих поверхностей – 2.

Интерактивная панель EDFLAT EDF75TP01: Android 13.0, Cortex A76*4+A55*4, 2.4ГГц, 32 ГБ, DDR4 256 ГБ, 75 дюймов.

Комплект документации, методическое обеспечение: стенды по охране труда, техники безопасности и правилам поведения в кабинете.

Лицензионное и свободно распространяемое программное обеспечение.

Перечень необходимого комплекта лицензионного и свободно распространяемого программного обеспечения: Операционная система (Microsoft Windows 10), ПО веб-браузер (Яндекс Браузер, Google Chrome), ПО Системы контроля версий (Git), Текстовый редактор (Sublime Text, Visual Studio Code), Клиент для работы с API (Postman), Программное обеспечение для записи экрана (OBS Studio), Эмулятор выполняемой среды (VirtualBox, VMWare Workstation), Набор средств разработки (Node.js).

3.2. Учебно-методическое обеспечение

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

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: 02.02.2026).

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: 02.02.2026).

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: 02.02.2026)

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: 02.02.2026).

ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ БАЗ ДАННЫХ, ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ

- 1.Znanium.com: Электронно-библиотечная система: [сайт]. – Москва, ООО «ЗНАНИУМ» 2011-2026 – URL:<https://new.znanium.com/>(дата обращения: 02.02.2026). - Режим доступа: для авториз. пользователей МИЭТ.
- 2.ЭБС Юрайт: образовательная платформа. – Москва, ООО «Электронное издательство Юрайт» 2020 – URL: <https://urait.ru/author/list?partner=450217DE-BE2D-46F5-BB25-9C69E84103EE> (дата обращения: 02.02.2026). - Режим доступа: для авториз. пользователей МИЭТ.
- 3.Электронно - библиотечная система Лань: [сайт]. – Санкт-Петербург, 2011-2026 – URL: <https://e.lanbook.com/>(дата обращения: 02.02.2026). - Режим доступа: для авториз. пользователей МИЭТ.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	Показатели освоённости 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	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,	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, контрольные работы)

- 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	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 биометрических данных законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для	
--	--	--

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 алгоритмы для шифрования данных; - принципы обеспечения безопасности передачи данных по сети;	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; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения	
--	---	--

- 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; - реализовывать составленный план;	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; 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;	
--	--	--

- 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 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.	
--	----------------------------------	--

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе реализации обучения используется смешанное обучение, основанное на интеграции технологий традиционного и электронного обучения, замещении части традиционных учебных форм занятий, формами и видами взаимодействия в электронной образовательной среде.

Применяются следующие модели обучения: перевернутый класс, когда студенты знакомятся с новым материалом при помощи электронных ресурсов самостоятельно дома, а на аудиторных занятиях происходит обсуждение изученного материала.

Освоение образовательной программы обеспечивается ресурсами электронной информационно - образовательной среды SDO.MIET.RU.

В процессе обучения при проведении занятий и для самостоятельной работы используются внутренние электронные ресурсы в различных формах.

При проведении занятий и для самостоятельной работы используются внешние электронные ресурсы в формах:

- электронных компонентов сервисов:

<https://resh.edu.ru/>

<https://mob-edu.ru/>

<https://www.mos.ru/city/projects/mesh/>

Рабочая программа дисциплины общепрофессионального цикла «ОП 06 Основы информационной безопасности» по специальности среднего профессионального образования 09.02.12 «Техническая эксплуатация и сопровождение информационных систем» разработана в колледже электроники и информатики НИУ МИЭТ 02.02.2026, протокол № 6.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа согласована с директором колледжа ЭИ НИУ МИЭТ

Директор колледжа /



/С.Н. Литвинова /