МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»

Институт экономики

УТВЕРЖДЕНО
решением ученого совета ННГУ
протокол от 24.12.2025 г. № 15

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

Специальность среднего профессионального образования

09.02.12 «Техническая эксплуатация и сопровождение информационных систем»

Квалификация выпускника

Специалист по технической эксплуатации и сопровождению информационных систем

Форма обучения

Очная

2026

Программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности (специальностям) среднего профессионального образования (далее – СПО) 09.02.12 «Техническая эксплуатация и сопровождение информационных систем»

Автор
Преподаватель ИНЭК СПО Запольнова Н.Ю.

Программа дисциплины рассмотрена и одобрена на заседании методической комиссии протокол от 14.11.2025 г. № 5

Председатель методической комиссии ИНЭК
к.э.н., доцент Макарова С.Д.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОП.0.6 Основы информационной безопасности»

1.1 Место дисциплины в структуре образовательной программы:
Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.12 «Техническая эксплуатация и сопровождение информационных систем»
Учебная дисциплина «Основы информационной безопасности» обеспечивает формирование профессиональных и 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 09. Пользоваться профессиональной документацией на государственном и иностранном языках;
ПК 1.7. Обнаруживать инциденты информационной безопасности, связанные с работой информационных систем
ПК 2.5. Выявлять инциденты информационной безопасности при обеспечении функционирования баз данных

1.2 Цель и планируемые результаты освоения дисциплины:
В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Умения и знания учебной дисциплины

Таблица 1

Код ОК, ПК	**Умения**	**Знания**
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	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

	(самостоятельно или с помощью наставника)	
ОК.02	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации, современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности в том числе с использованием цифровых средств.
ОК.09	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

ПК 2.5	– идентифицировать инциденты ИБ при работе с БД – осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации) – управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ устанавливать и сопровождать антивирусное ПО	– понятие и классификация инцидентов ИБ – типичные угрозы ИБ при работе с БД – процедуры и регламенты передачи информации об инцидентах в службу ИБ организации – средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры) – основы работы со средствами антивирусной защиты – основы ИБ – основы деловой этики правила деловой переписки

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	48
В т.ч. в форме практической подготовки	
в том числе:	
теоретическое обучение	10
практические занятия	38
Промежуточная аттестация в форме дифференцированного зачета	

2.2 Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятий	Объем, акад. ч / в том числе в форме практической подготовки, акад. ч	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Тема 1. Введение в информационную безопасность	**Содержание учебного материала**		ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности	**1**	
	Практические занятия	**2**	
	1.Анализ угроз		
Тема 2. Управление безопасностью информации	**Содержание учебного материала**	**1**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)		
	Практические занятия	**2**	
	1. Нормативно-правовое регулирование в области информационной безопасности		
Тема 3. Криптография	**Содержание учебного материала**	**2**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1. Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография.		
	Практические занятия	**6**	
	1 Работа с симметричными и асимметричными алгоритмами. 2.Хэширование и создание цифровой подписи сообщения. 3.Стеганография.		
	Содержание учебного материала		

Тема 4. Защита сетевой инфраструктуры	1.Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов	**2**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	Практические занятия	**4**	
	1.Организация защиты от атак		
	2.Организация работы VPN и межсетевого экрана		
Тема 5. Безопасность приложений	**Содержание учебного материала**	**2**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей.		
	Практические занятия	**2**	
	1.Тестирование на проникновение и анализ уязвимостей.		
Тема 6. Защита данных	**Содержание учебного материала**	**2**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Шифрование данных в покое и в транзите. Резервное копирование и восстановление данных. Управление доступом к данным		
	Практические занятия	**4**	
	1.Выполнение резервного копирования и восстановления данных. 2.Управление доступом к данным		
Тема 7. Безопасность облачных технологий	**Содержание учебного материала**		ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Особенности безопасности в облачных средах. Модели облачных услуг (IaaS, PaaS, SaaS) и их безопасности	**1**	
	Практические занятия		
	1.Изучение модели облачных услуг и их безопасности	**2**	
Тема 8. Инциденты безопасности	**Содержание учебного материала**		

	1.Реакция на инциденты и управление ими. Анализ инцидентов и цифровая криминалистика. Восстановление после инцидента. Кибербезопасность. Промышленный шпионаж. OSINT. Форензика	**1**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	Практические занятия		
	1.Работа с инцидентами.	**2**	
Тема 9. Социальная инженерия и человеческий фактор	**Содержание учебного материала**		ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Психология атак: социальная инженерия. Обучение сотрудников информационной безопасности	**1**	
	Практические занятия	**2**	
	1.Оценка уязвимости организации перед методами социальной инженерии		
Тема 10. Будущее информационной безопасности	**Содержание учебного материала**	**1**	ОК 01.; ОК 02.; ОК 09.; ПК 1.7.; ПК 2.5.
	1.Тенденции и новые технологии в области безопасности (AI, ML, блокчейн). Этические аспекты информационной безопасности		
	Практические занятия	**2**	
	1.Анализ влияния новых технологий и этических аспектов в сфере информационной безопасности		
Промежуточная аттестация в форме дифференцированного зачета			

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатория «Компьютерные сети и основы информационной безопасности»:

– Автоматизированные рабочие места на 12-15 обучающихся: ЦПУ:Intel(R) Core(TM) i3-10100,- количество физических ядер – 4, количество потоков – 8, Сетевой адаптер: - технология Ethernet - 0/100/1000 mbps, ОЗУ: - 8 ГБ, Графический адаптер: - NVIDIA GeForce GT730, ПЗУ:- SSD 256 ГБ или аналоги;

– Автоматизированное рабочее место преподавателя: (ЦПУ:Intel(R) Core(TM) i3-10100,- количество физических ядер – 4, количество потоков – 8, Сетевой адаптер: - технология Ethernet - 0/100/1000 mbps, ОЗУ: - 8 ГБ, Графический адаптер: - NVIDIA GeForce GT730, ПЗУ:- SSD 256 ГБ или аналоги;

– Проектор и экран;

– Маркерная доска;

– Программное обеспечение общего и профессионального назначения: Операционная система (РЕД ОС 8.0 или аналог), клиент для работы с API (Postman или аналог), программное обеспечение для записи экрана (OBS Studio или аналог), эмулятор выполняемой среды (Genymotion, VirtualBox, VMWare Workstation или аналог), набор средств разработки (Node.js или аналог), ПО веб-браузер (Яндекс Браузер, Chromium, Google Chrome или аналоги), ПО Системы контроля версий (Git, GitKraken или аналоги), текстовый редактор (Sublime Text, Visual Studio Code или аналоги)

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации имеет электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

3.2.1. Основные 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: 03.03.2026).

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: 03.03.2026).

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: 03.03.2026)

3.2.1. Дополнительные источники

1. 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: 03.03.2026)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Методы оценки
Перечень знаний, осваиваемых в рамках дисциплины		
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	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;	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, собеседование, подготовка и выступление с докладом, сообщением, презентацией) Аттестация дифференцированный зачет

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 – 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 – понятие и классификация инцидентов ИБ – типичные угрозы ИБ при работе с БД – процедуры и регламенты передачи информации об	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,	

инцидентах в службу ИБ организации – средства электронной коммуникации (электронная почта, системы управления задачами, мессенджеры) – основы работы со средствами антивирусной защиты – основы ИБ – основы деловой этики правила деловой переписки	такие как GDPR, HIPAA, PCI DSS и др.; Знает отраслевую нормативную техническую документацию и источники информации, необходимые для профессиональной деятельности; Знает современный отечественный и зарубежный опыт в профессиональной деятельности; Владеет принципами и методами обеспечения безопасности информационных систем; Знает принципы безопасности информационных систем; Владеет современными методами и технологиями в области безопасности информационных систем; Знает законодательные и нормативные акты в области безопасности информационных систем; Знает источники угроз информационной безопасности и меры по их предотвращению; Имеет представление об основных угрозах безопасности мобильных приложений; Ориентируется в принципах криптографии и шифрования данных; Знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect;	

	Знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; Владеет основными принципами безопасности информации и методов ее защиты; Знает стандартные криптографические алгоритмы для шифрования данных; Имеет представление о принципах обеспечения безопасности передачи данных по сети; Знает основы безопасности приложений и инфраструктуры; Знает методы анализа на уязвимости и мониторинга безопасности; Знает основные принципы и методы обеспечения безопасности ИТ-инфраструктуры и веб-приложений; Понимает различные уязвимости и угрозы безопасности, а также способы их предотвращения и обнаружения; Знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.	
Перечень умений, осваиваемых в рамках дисциплины		

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	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;	Экспертное наблюдение выполнения практических работ и видов работ по практике Диагностика (тестирование, собеседование, подготовка и выступление с докладом, сообщением, презентацией) Аттестация дифференцированный зачет

решения профессиональных задач понимать тексты на базовые профессиональные темы – 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 – идентифицировать инциденты ИБ при работе с БД – осуществлять коммуникации с сотрудниками службы ИБ организации (в том числе с использованием электронных средств коммуникации) – управлять доступом пользователей к элементам БД при обнаружении инцидентов ИБ	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.	

устанавливать и сопровождать антивирусное ПО		

Шкала оценивания

Таблица 4

Индикаторы компетенции	неудовлетворительно	удовлетворительно	хорошо	отлично
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий