МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Казанский национальный исследовательский технологический университет»
КАЗАНСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
(ФГБОУ ВО "КНИТУ" КТК)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

УТВЕРЖДАЮ

Зам. директора по УР

_____ Р.А. Газизов

« 01» апреля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ОП.05 Основы информационной безопасности

(наименование предмета/дисциплины)

09.02.11 Разработка и управление программным обеспечением

(шифр, специальность/профессия)

Программист

(квалификация выпускника)

2 года 10 месяцев

(нормативный срок обучения)

Казань, 2026

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта по специальности 09.02.11 Разработка и управление программным обеспечением среднего профессионального образования, утвержденного приказом Минпросвещения России от 24.02.2025 № 138, и основной образовательной программы подготовки специалистов среднего звена.

Составитель (ли): _____

ФОС учебной дисциплины рассмотрен и утвержден на заседании предметно-цикловой комиссии общепрофессиональных дисциплин и профессиональных модулей специальности 09.02.11 Разработка и управление программным обеспечением КТК ФГБОУ ВО "КНИТУ", Протокол № 7 от «27» марта 2026 г.

Председатель ПЦК/З.Н. Гатятуллина

(ФИО)

СОДЕРЖАНИЕ

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

1.1 Общие положения

В результате освоения дисциплины ОП.05 «Основы информационной безопасности» обучающийся должен обладать предусмотренными ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением умениями, знаниями и компетенциями, подлежащими проверке средствами текущего и итогового контроля.

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

– распознавать и анализировать угрозы информационной безопасности, определять риски и каналы утечки информации;
– применять меры защиты информации, баз данных, приложений и сетевой инфраструктуры;
– использовать механизмы аутентификации, авторизации, резервного копирования, аудита и мониторинга безопасности;
– применять криптографические методы защиты данных, включая шифрование, хэширование и цифровую подпись;
– анализировать требования безопасности информационных систем и разрабатывать базовые меры защиты;
– собирать, систематизировать и документировать информацию о системе, подготавливать пользовательскую и проектную документацию.

знать:

– основные понятия информационной безопасности, виды угроз, уязвимостей и рисков;
– принципы безопасного хранения, обработки и передачи данных;
– методы защиты баз данных, приложений, сетевой инфраструктуры и информационных систем;
– основы криптографии, аутентификации, авторизации и резервного копирования;
– нормативно-правовые и этические основы работы с информацией и защитой данных;
– принципы анализа требований безопасности, проектирования мер защиты и документирования решений.

Общие (ОК) и профессиональные компетенции (ПК), формируемые в результате освоения дисциплины:

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

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

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

ПК 1.1 - Проектировать базы данных.

ПК 1.4 - Администрировать базы данных.

ПК 1.5 - Защищать информацию в базе данных с использованием технологии защиты информации.

ПК 3.1 - 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.

1.2 Результаты освоения дисциплины, подлежащие проверке

Форма аттестации по дисциплине - другие формы контроля.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПОДЛЕЖАЩИЕ ПРОВЕРКЕ

2.1 В результате аттестации по дисциплине осуществляется комплексная проверка умений, знаний и динамики формирования общих и профессиональных компетенций.

Таблица 1. Перечень профессиональных и общих компетенций и показатели результата

Результаты обучения: умения, знания и компетенции	**Показатели оценки результата**	**Форма контроля и оценивания**
Уметь: - анализировать угрозы и риски ИБ; - применять меры защиты данных, БД, приложений и сетевой инфраструктуры; - использовать аутентификацию, авторизацию, резервное копирование, аудит и мониторинг; - применять криптографические методы защиты; - разрабатывать и документировать базовые меры безопасности ИС.	Демонстрирует умение выявлять угрозы информационной безопасности, выбирать и применять меры защиты, использовать криптографические механизмы, настраивать базовые средства защиты и документировать результаты работы.	Текущий контроль: устный опрос, тестирование, практические работы, решение кейсов, наблюдение. Промежуточная аттестация: другие формы контроля.
Знать: - понятия, угрозы, уязвимости и риски информационной безопасности; - методы защиты данных, БД, приложений и сетей; - основы криптографии, аутентификации и авторизации; - нормативно-правовые основы защиты информации; - принципы проектирования и документирования мер защиты.	Демонстрирует знание терминологии и принципов ИБ, методов защиты информации, криптографических подходов, нормативных требований, правил безопасной эксплуатации и документирования информационных систем.	Текущий контроль: устный опрос, тестирование, контрольные задания. Промежуточная аттестация: другие формы контроля.
Общие и профессиональные компетенции		
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно	Обоснованно выбирает способы решения задач в области информационной безопасности, планирует	Наблюдение, анализ практических работ, решение ситуационных задач. Тестирование, практические

к различным контекстам	последовательность действий и оценивает результат.	работы, анализ кейсов. Устный опрос, работа с документацией, практические задания.
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Использует современные средства поиска, анализа и интерпретации информации, применяет цифровые инструменты и программное обеспечение для решения профессиональных задач.	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Понимает профессиональную документацию, корректно использует терминологию, умеет работать с инструкциями, регламентами и описаниями технологий.	
ПК 1.1. Проектировать базы данных.	Анализирует требования безопасности при проектировании баз данных, учитывает принципы безопасного хранения данных.	
ПК 1.4. Администрировать базы данных.	Применяет методы администрирования и обеспечения безопасности баз данных, использует резервное копирование и контроль доступа.	
ПК 1.5. Защищать информацию в базе данных с использованием технологии защиты информации.	Выбирает и применяет технологии защиты информации в базах данных, использует аудит, шифрование и механизмы безопасного доступа.	
ПК 3.1. Собирать исходные данные для разработки проектной документации на информационную систему.	Собирает и анализирует исходные данные по требованиям безопасности информационных систем.	
ПК 3.2. Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.	Документирует проектные решения и учитывает риски, нормативные требования и требования безопасности.	
ПК 3.3. Разрабатывать	Анализирует требования	

подсистемы безопасности информационной системы в соответствии с техническим заданием.	безопасности и предлагает меры по защите информационной системы.	
ПК 3.5. Интегрировать информационную систему с существующими информационными системами заказчика.	Понимает принципы защищенной интеграции информационных систем и интерфейсов обмена данными.	
ПК 3.7. Разрабатывать техническую документацию на эксплуатацию информационной системы.	Разрабатывает и оформляет пользовательскую и эксплуатационную документацию по вопросам безопасности и использования системы.	

3. ОЦЕНКА ОСВОЕНИЯ ДИСЦИПЛИНЫ

3.1 Формы и методы оценивания

Предметом оценки служат умения и знания, предусмотренные ФГОС по дисциплине ОП.05 Основы информационной безопасности, направленные на формирование общих и профессиональных компетенций

Таблица 2 Контроль и оценка освоения дисциплины по темам (разделам)

Элемент дисциплины	**Формы и методы контроля**					
	Текущий контроль		**Рубежный контроль**		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые ОК, ПК, У, З**	**Форма контроля**	**Проверяемые ОК, ПК, У, З**	**Форма контроля**	**Проверяемые ОК, ПК, У, З**
					Другие формы контроля	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.5, ПК3.7,
Раздел 1	Комплексная оценка освоения раздела по результатам текущего контроля	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.5, ПК3.7, У1-У4, З1-З5	Другие формы контроля: проверка освоения дисциплины в целом.	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7,		
Тема 1.1	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.5, ПК3.7, У1, У3, З1, З2, З3	Учет результатов текущего контроля			
Тема 1.2	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.5, ПК3.7, У3, У4, З2, З3	Учет результатов текущего контроля			

	работ.					
Тема 1.3	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.5, ПК3.7, У1, У4, З2	Учет результатов текущего контроля			
Раздел 2	Комплексная оценка освоения раздела по результатам текущего контроля	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, ПК3.1, ПК3.2, ПК3.3, ПК3.5, ПК3.7, У1-У4, З1-З5	Другие формы контроля: итоговое оценивание.			
Тема 2.1	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК1.5, У1, З1	Учет результатов текущего контроля			
Тема 2.2	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК3.1, ПК3.2, ПК3.3, У1, У4, З2, З5	Учет результатов текущего контроля			
Тема 2.3	Оценка	ОК01, ОК02,	Учет			

	теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК09, ПК1.4, ПК1.5, У2, З4	результатов текущего контроля			
Тема 2.4	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК1.1, ПК1.4, ПК3.5, У2, З4	Учет результатов текущего контроля			
Тема 2.5	Оценка теоретического и практического материала. Беседа, тестирование, наблюдение, анализ кейсов, выполнение практических работ.	ОК01, ОК02, ОК09, ПК1.4, ПК1.5, ПК3.3, ПК3.5, ПК3.7, У2, У4, З5	Учет результатов текущего контроля			

3.2 Перечень вопросов и заданий для текущего контроля знаний по дисциплине ОП.05 Основы информационной безопасности

Тема 1.1. Информационная культура и цифровая гигиена

Основы информационной среды: что такое информация и зачем ей управлять. Информационная перегрузка: стратегии фильтрации. Цифровая гигиена и личная инфосреда. Критическое мышление и проверка информации: Надёжные и ненадёжные источники: критерии оценки. Введение в фактчекинг: уровни лжи и методы опровержения

Тема 1.2. Организация, хранение и использование данных

Основы организации и хранения информации: Структура файлов и папок логика и автоматизация. Организация хранилищ в облаке и на локальных устройствах. Типы данных и носителей: от архива до дата-центра.

Систематизация и описание данных. Принципы каталогизации и индексирования. Метаданные: зачем нужны и как правильно задавать. Основы документирования информации

Тема 1.3. Правовые и этические аспекты информационной работы

Правовые рамки и нормативное регулирование. Авторское право: что можно использовать, а что — нет. Свободные лицензии: Creative Commons и публичное достояние. Закон о персональных данных и GDPR: базовое знание. Работа с конфиденциальной информацией: что нельзя разглашать. Проверка достоверности и борьба с дезинформацией: Проверка источников: как удостовериться в достоверности. Инструменты фактчекинга: Snopes, Factcheck.org, Provereno. Признаки фейков: от фотофальсификации до deepfake. Академическая и профессиональная этика: Цитирование и плагиат: правила, инструменты, ловушки. Этическое курирование контента: как не навредить. Профессиональная репутация и след в интернете

Тема 2.1. Введение в информационную безопасность

Основные понятия и определения. История и развитие информационной безопасности. Актуальные угрозы и риски в информационной безопасности

Тема 2.2. Управление безопасностью информации

Нормативно-правовое регулирование в области ИБ. Политики и процедуры безопасности. Оценка рисков и управление ими. Соответствие стандартам и нормативам (ISO 27001, GDPR и др.)

Тема 2.3. Криптография

Основы криптографии: симметричные и асимметричные алгоритмы. Хэширование и цифровые подписи. Применение криптографии в приложениях. Стеганография

Тема 2.4. Защита сетевой инфраструктуры

Основы сетевой безопасности. Защита от атак (DDoS, MITM и др.) Использование VPN и межсетевых экранов

Тема 2.5. Безопасность приложений

Уязвимости веб-приложений (OWASP Top Ten). Безопасное программирование: лучшие практики. Тестирование на проникновение и анализ уязвимостей

3.3 Практические работы по дисциплине

Практическая работа №1	Деконструкция манипулятивных текстов: разбор новостного поста и выявление искажений.
Практическая работа №2	Создание структурированной базы данных (например, каталог медиафайлов с метаданными и фильтрами).
Практическая работа №3	Фактчекинг-кейс: разоблачение ложной информации; подготовка материала с соблюдением авторских прав, оформлением сносок, атрибуции и выбором лицензии.
Практическая работа №4	Работа с симметричными и асимметричными алгоритмами. Хэширование и создание цифровой подписи сообщения.