МИНИСТЕРСТВО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
ГАПОУ СО
«НИЖНЕТАГИЛЬСКИЙ ТОРГОВО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ»

Утверждаю:
Зам. директора по УР
_____ М.Г. Дмитриева
«30» июня 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности
09.02.11 Разработка и управление программным обеспечением

Нижний Тагил 2026

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования и примерной основной образовательной программы по специальности 09.02.11 Разработка и управление программным обеспечением.

Организация-разработчик:
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Разработчики:
Репьев Егор Денисович, преподаватель первой квалификационной категории ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Ильина Виктория Денисовна, преподаватель без квалификационной категории ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 4

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ 8

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 15

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» 18

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Место дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «ОП.05 Основы информационной безопасности» принадлежит к общепрофессиональному циклу (общепрофессиональные дисциплины) образовательной программы по специальности 09.02.11 Разработка и управление программным обеспечением. Дисциплина изучается на втором курсе в третьем семестре и формирует основу для освоения дисциплины «ОП.10 Сертификация информационных систем» и профессиональных модулей, связанных с разработкой веб-приложений, баз данных и интеграцией программных модулей.

Цель дисциплины: формирование представлений в области информационной безопасности, понимания угроз, методов и средств защиты информации, практических навыков безопасной разработки веб-приложений на PHP/Laravel, безопасной работы с базами данных и репозиториями Git, а также навыков безопасного и добросовестного применения российских ИИ-ассистентов.

1.2. Цель и планируемые результаты освоения дисциплины

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника. В результате освоения дисциплины обучающийся должен:

Код ОК, ПК	Умения	Знания
ОК 01 ОК 02 ОК 09	– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации; – оценивать риски информационной безопасности и выбирать меры защиты для автоматизированного рабочего места и информационной системы; – выявлять и устранять типовые уязвимости веб-приложений на PHP/Laravel (внедрение SQL-кода, межсайтовое выполнение сценариев, подделка межсайтовых запросов, нарушение контроля доступа);	– сущность и понятие информационной безопасности, характеристику её составляющих; место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; жизненные циклы информации ограниченного доступа в процессе её создания, обработки, передачи; – источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при её обработке в автоматизированных

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Код ОК, ПК	Умения	Знания
	– реализовывать безопасную аутентификацию и разграничение доступа пользователей, обеспечивать безопасное хранение паролей, ключей и секретов в проекте и репозитории Git; – находить и применять нормативные правовые документы по защите информации и персональных данных, в том числе в справочно-правовых системах; – читать описания уязвимостей и рекомендации по безопасности (OWASP, CVE, документация фреймворков) на русском и английском языках; – безопасно использовать российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): обезличивать данные, проверять результат, распознавать попытки внедрения вредоносных инструкций (prompt injection).	(информационных) системах; – современные средства и способы обеспечения информационной безопасности, основы криптографической защиты информации; – основные методики анализа угроз и рисков информационной безопасности; – основные положения законодательства о защите информации и персональных данных (Федеральные законы №149-ФЗ и №152-ФЗ), систему сертификации и лицензирования в области защиты информации; – классификацию уязвимостей веб-приложений (OWASP Top 10) и способы защиты от них в PHP/Laravel; принципы безопасной работы с базами данных; – требования к хранению секретов и учётных данных, правила безопасной работы с репозиториями Git; – возможности, ограничения и риски применения ИИ-ассистентов (утечка данных, «галлюцинации», внедрение вредоносных инструкций); требования 152-ФЗ при их использовании.

Перечень формируемых общих компетенций:

Код	Наименование общей компетенции
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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

1.3. Междисциплинарные связи и используемые информационные технологии

Содержание дисциплины построено так, чтобы результаты её освоения использовались в других дисциплинах и профессиональных модулях специальности. Ключевые связи приведены в таблице.

Дисциплина, модуль	Содержание связи
ОП.01 Операционные системы и среды	Модель прав доступа, принцип наименьших привилегий, журналирование, защита сетевых служб и контейнеров (темы 2.1, 2.2, 3.1, 4.3 ОП.01) – используются в темах 2.3, 3.1 и 4.2 данной дисциплины.
ОП.04 Основы алгоритмизации и программирования	Безопасное кодирование, обработка и проверка входных данных, система контроля версий Git и GitVerse – основа тем 3.2 и 3.3.
ОП.07 Математический аппарат в области информационных технологий	Модульная арифметика, простые числа, элементы теории вероятностей – основа тем 2.1 (оценка рисков) и 2.4 (криптография).
ОП.10 Сертификация информационных систем	Темы 2.2 и 2.3 (нормативное регулирование, меры защиты, классификация угроз) – исходные для тем об аттестации объектов информатизации и тестировании безопасности.
ОП.11 Компьютерные сети	Протоколы TCP/IP, HTTP/HTTPS, межсетевые экраны, VPN – основа тем 2.3, 2.4 и 3.2.
ПМ.01 Разработка, администрирование и защита баз данных	Разграничение доступа к данным, резервное копирование, защита от SQL-инъекций (тема 3.3) – применяются при проектировании и администрировании баз данных MySQL/MariaDB.
ПМ.02 Разработка и интеграция модулей программного обеспечения	Безопасное кодирование, проверка зависимостей, обзор кода (code review) и работа с репозиторием без секретов (темы 3.2, 3.3).
ПМ.03 Проектирование и разработка веб-приложений	Аутентификация, авторизация, защита от XSS, CSRF и SQL-инъекций на Laravel и Orchid Platform (темы 3.1, 3.2) – непосредственно применяются при разработке веб-приложений.
ОГСЭ.04 Иностранный язык в профессиональной деятельности	Чтение описаний уязвимостей, OWASP Cheat Sheet Series и документации на английском языке; терминология безопасности.

Работа с искусственным интеллектом. Тема 4.1 и практическое занятие №4 посвящены безопасному применению российских ИИ-ассистентов (GigaChat, GigaCode, Алиса AI, YandexGPT): рискам утечки данных, внедрению вредоносных инструкций (prompt injection), «галлюцинациям» и требованиям 152-ФЗ. В практических занятиях №2 и №3 ИИ-ассистенты используются как вспомогательное средство (подготовка перечня угроз, поиск недостатков в коде), результат обязательно проверяется по документации и нормативным документам, использование ИИ указывается в отчёте. Передача ИИ-сервисам паролей, ключей, персональных данных и конфиденциальных сведений

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

запрещена. На контрольных работах и дифференцированном зачёте использование ИИ-ассистентов не допускается.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы	**36**
в том числе:	
теоретическое обучение	28
лабораторные и практические занятия	8
самостоятельная работа	–
промежуточная аттестация (дифференцированный зачёт)	в пределах общего объема

Дисциплина изучается на 2 курсе в 3 семестре. Форма промежуточной аттестации – дифференцированный зачёт.

2.2. Тематический план и содержание учебной дисциплины ОП.05 Основы информационной безопасности

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
Раздел 1. Теоретические основы информационной безопасности (10 ч)			
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала** 1. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. 2. Составляющие информационной безопасности: конфиденциальность, целостность, доступность; дополнительные свойства (подлинность, неотказуемость, подотчётность). 3. Понятия «угроза информации» и «риск информационной безопасности». Примеры преступлений в сфере информации и информационных технологий (статьи 272–274.1 Уголовного кодекса РФ). Сущность функционирования системы защиты информации. 4. Место информационной безопасности в системе национальной безопасности страны: Доктрина информационной безопасности Российской Федерации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.	2	ОК 01, ОК 02
Тема 1.2. Основы защиты информации	**Содержание учебного материала** 1. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации (персональные	3	ОК 01, ОК 02, ОК 09

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
	данные, коммерческая, служебная, профессиональная тайна). 2. Виды, источники и носители защищаемой информации. Жизненные циклы конфиденциальной информации в процессе её создания, обработки, передачи, хранения и уничтожения. 3. Цели и задачи защиты информации. Основные понятия в области защиты информации (ГОСТ Р 50922-2006). 4. Элементы процесса менеджмента информационной безопасности. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.		
	В том числе практических занятий и лабораторных работ 1. Практическое занятие №1 «Определение объектов защиты на типовом объекте информатизации и классификация защищаемой информации по видам тайны и степеням конфиденциальности»	2	
Тема 1.3. Угрозы безопасности защищаемой информации	**Содержание учебного материала** 1. Понятие угрозы безопасности информации. Системная классификация угроз: по источнику (внешние и внутренние, антропогенные, техногенные и природные), по целям (нарушение конфиденциальности, целостности, доступности), по характеру (преднамеренные и случайные). 2. Каналы и методы несанкционированного доступа к информации. Уязвимости и их источники. Факторы, воздействующие на информацию при её обработке в автоматизированных системах. Вредоносное программное обеспечение, социальная инженерия, фишинг. 3. Методы оценки уязвимости информации. Банк данных угроз безопасности информации ФСТЭК России (БДУ), идентификаторы CVE и CWE, общая система оценки уязвимостей CVSS. 4. Модель нарушителя и модель угроз как документы объекта информатизации.	3	ОК 01, ОК 02, ОК 09
Раздел 2. Методология защиты информации (12 ч)			
Тема 2.1. Методологические подходы к защите информации. Анализ рисков	**Содержание учебного материала** 1. Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты. 2. Виды мер и основные принципы защиты информации: законность, комплексность, непрерывность, разумная достаточность, минимизация привилегий, многоуровневая	2	ОК 01, ОК 02

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
	защита («эшелонирование»). 3. Основные методики анализа рисков: качественная и количественная оценка, матрица «вероятность – ущерб», реестр рисков, способы обработки риска (снижение, принятие, избегание, передача).		
Тема 2.2. Нормативно-правовое регулирование защиты информации	**Содержание учебного материала** 1. Организационная структура системы защиты информации в Российской Федерации; полномочия ФСТЭК России, ФСБ России, Роскомнадзора. Законодательные акты в области защиты информации: Федеральные законы №149-ФЗ «Об информации, информационных технологиях и о защите информации», №152-ФЗ «О персональных данных», №98-ФЗ «О коммерческой тайне», №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», №63-ФЗ «Об электронной подписи», Закон РФ «О государственной тайне». 2. Требования 152-ФЗ: оператор персональных данных, согласие субъекта, обработка и хранение, уровни защищённости, ответственность за нарушения. 3. Российские и международные стандарты, определяющие требования к защите информации (серия ГОСТ Р ИСО/МЭК 27000, ГОСТ Р ИСО/МЭК 15408). Система сертификации РФ в области защиты информации: основные правила и документы (общие сведения; подробно – в дисциплине ОП.10 «Сертификация информационных систем»). 4. Работа в справочно-правовой системе с нормативными правовыми документами по информационной безопасности: поиск, актуальная редакция, ссылки на статьи (демонстрация на занятии).	3	ОК 02, ОК 09
Тема 2.3. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала** 1. Основные механизмы защиты информации: идентификация и аутентификация, управление доступом, регистрация и учёт событий, контроль целостности, антивирусная защита, межсетевое экранирование, резервное копирование. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных системах. 2. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. 3. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы	3	ОК 01, ОК 02, ОК 09

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
	построения организационно-распорядительной системы: политики, регламенты, инструктажи, ответственность.		
	В том числе практических занятий и лабораторных работ 1. Практическое занятие №2 «Определение и классификация угроз безопасности объекта информатизации. Выбор мер защиты для автоматизированного рабочего места»	2	
Тема 2.4. Основы криптографической защиты информации	**Содержание учебного материала** 1. Задачи криптографии: шифрование, контроль целостности, электронная подпись. Симметричные и асимметричные алгоритмы; стойкость и длина ключа. Роль математического аппарата (простые числа, модульная арифметика). 2. Хеш-функции и их применение: контроль целостности, хранение паролей. Соль и «растяжение» ключа (bcrypt, Argon2). Недопустимость самостоятельной разработки криптоалгоритмов. 3. Протокол TLS и HTTPS, сертификаты X.509, удостоверяющие центры. Электронная подпись по 63-ФЗ. Отечественные криптографические стандарты (ГОСТ Р 34.10-2012 – электронная подпись, ГОСТ Р 34.11-2012 – хеш-функция «Стрибог», ГОСТ Р 34.12-2015 – блочные шифры «Кузнечик» и «Магма»).	2	ОК 01, ОК 02
Раздел 3. Безопасность веб-приложений и баз данных (8 ч)			
Тема 3.1. Аутентификация, авторизация и управление сеансами	**Содержание учебного материала** 1. Идентификация, аутентификация и авторизация. Факторы аутентификации, многофакторная аутентификация, одноразовые пароли. Политика паролей, хранение паролей в виде хеша (Hash::make в Laravel – bcrypt или Argon2), защита от перебора (ограничение частоты попыток, throttle). 2. Управление сеансами: идентификатор сеанса, атрибуты cookie (HttpOnly, Secure, SameSite), пересоздание идентификатора после входа, завершение сеанса. 3. Разграничение доступа в Laravel: middleware, Gate и Policy; роли и права в Orchid Platform. Принцип наименьших привилегий. Нарушение контроля доступа (IDOR) как наиболее распространённая уязвимость.	2	ОК 01, ОК 02, ОК 09
Тема 3.2. Уязвимости веб-приложений. OWASP Top 10	**Содержание учебного материала** 1. Перечень OWASP Top 10 (редакция 2021 г.): нарушение контроля доступа, сбои криптографии, внедрение (инъекции), небезопасное проектирование, небезопасная конфигурация, уязвимые и устаревшие	2	ОК 01, ОК 02, ОК 09

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
	компоненты, сбои идентификации и аутентификации, нарушение целостности данных и ПО, недостатки журналирования и мониторинга, подделка запросов со стороны сервера (SSRF). 2. Внедрение SQL-кода: механизм атаки и защита (подготовленные запросы, Query Builder и Eloquent, недопустимость конкатенации). Межсайтовое выполнение сценариев (XSS): отражённый, хранимый, DOM-вариант; экранирование в Blade ({{ }} и {!! !!}), заголовок Content-Security-Policy. 3. Подделка межсайтовых запросов (CSRF): механизм, токены (директива @csrf), cookie SameSite. Небезопасная загрузка файлов, массовое присвоение (mass assignment, $fillable). Валидация входных данных (FormRequest). 4. Работа с описаниями уязвимостей на английском языке: OWASP Cheat Sheet Series, документация Laravel.		
	В том числе практических занятий и лабораторных работ 1. Практическое занятие №3 «Выявление и устранение уязвимостей веб-приложения на Laravel: XSS, CSRF, SQL-инъекции, контроль доступа»	2	
Тема 3.3. Безопасность баз данных, конфигураций и репозиториев	**Содержание учебного материала** 1. Безопасность СУБД (MySQL, MariaDB, SQLite): отдельные учётные записи приложения с минимальными правами, запрет удалённого доступа администратора, шифрование соединения, хранение чувствительных данных (шифрование полей, Crypt в Laravel), резервное копирование и проверка восстановления. 2. Секреты и конфигурация: файл .env, APP_KEY, токены API; APP_DEBUG=false в промышленной среде; разделение сред разработки и эксплуатации. 3. Git и безопасность: недопустимость фиксации секретов в репозиториях (GitVerse), .gitignore, действия при утечке (немедленная замена ключа, очистка истории, git filter-repo), сканеры секретов, защищённые ветки и проверка изменений (code review). 4. Безопасность зависимостей: composer audit, фиксация версий (composer.lock), обновление компонентов.	2	ОК 01, ОК 02, ОК 09
Раздел 4. Безопасное применение ИИ-ассистентов и организация реагирования (6 ч)			
Тема 4.1. Российские ИИ-ассистенты и информационна	**Содержание учебного материала** 1. Российские ИИ-ассистенты: GigaChat и GigaCode (интеграция с GitVerse), Алиса AI, YandexGPT. Прикладные задачи по информационной	2	ОК 01, ОК 02, ОК 09

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
я безопасность	безопасности: объяснение уязвимости, поиск недостатков в фрагменте кода, подготовка чек-листов, черновиков политик и инструкций, разбор журналов событий. Обязательная проверка результата по документации и в изолированной среде. 2. Риски: утечка данных через запросы к внешнему сервису (пароли, ключи, исходный код с секретами, персональные данные, служебные сведения); «галлюцинации» и небезопасный сгенерированный код (SQL-запросы с конкатенацией, отключённая проверка сертификатов, chmod 777). 3. Внедрение вредоносных инструкций (prompt injection): прямое и косвенное (во вводимом документе, на веб-странице, в комментарии кода). Принципы защиты: разделение инструкций и данных, минимальные полномочия ассистента, человек в контуре принятия решений. 4. Требования 152-ФЗ: передача персональных данных ИИ-сервису как их обработка и передача третьему лицу; основание обработки, обезличивание данных, недопустимость передачи без правовых оснований. Национальный кодекс этики в сфере ИИ, академическая добросовестность, обозначение использования ИИ в работе. Использование ИИ запрещено на контрольных работах и дифференцированном зачёте.		
	В том числе практических занятий и лабораторных работ 1. Практическое занятие №4 «Безопасное применение российских ИИ-ассистентов (GigaChat, Алиса AI): обезличивание данных, проверка ответа, prompt injection»	2	
Тема 4.2. Инциденты информационной безопасности и обеспечение непрерывности	**Содержание учебного материала** 1. Понятие инцидента информационной безопасности. Этапы реагирования: обнаружение, локализация, устранение, восстановление, извлечение уроков. Журналирование и мониторинг как источники данных об инциденте. 2. Резервное копирование по правилу «3-2-1», проверка восстановления, план обеспечения непрерывности. Обязанность уведомления об утечке персональных данных (152-ФЗ) и об инцидентах на объектах критической информационной инфраструктуры (187-ФЗ) – общие сведения. 3. Обучение и осведомлённость пользователей. Ответственность: дисциплинарная,	2	ОК 01, ОК 02

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций
	административная (КоАП РФ, статья 13.11), уголовная (статьи 272–274.1 УК РФ).		
Промежуточная аттестация: дифференцированный зачёт (проводится в пределах общего объема)			
Всего:		**36**	

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения

Кабинет «Основы информационной безопасности» (зона по видам работ «Основы информационной безопасности»), оснащённый в соответствии с примерной основной образовательной программой по специальности:

– автоматизированные рабочие места обучающихся (процессор не ниже Core i5, оперативная память не менее 16 ГБ, SSD, поддержка виртуализации) – по количеству обучающихся в подгруппе;

– автоматизированное рабочее место преподавателя;

– проектор и экран, маркерная доска;

– доступ к сети Интернет, к справочно-правовой системе (КонсультантПлюс или Гарант) и к серверу СДО Moodle;

– программное обеспечение: PHP 8.5 и Composer, Laravel 13, Orchid Platform, MySQL/MariaDB и SQLite, Node.js и Vite, Git, VS Code, веб-браузер с инструментами разработчика; учебный проект с намеренно внесёнными уязвимостями, развёртываемый в изолированной среде (Docker);

– доступ к российским ИИ-ассистентам (GigaChat, Алиса AI) через учебные аккаунты или сервисы, одобренные колледжем; доступ к GitVerse и GigaCode.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Внуков А.А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования. – 3-е изд., перераб. и доп. – М.: Юрайт, 2024. – 161 с.
2. Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надёжность и безопасность программного обеспечения: учебник для среднего профессионального образования. – 2-е изд. – М.: Юрайт, 2025. – 352 с.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

3. Щербак А.В. Информационная безопасность: учебник для среднего профессионального образования. – 2-е изд., перераб. и доп. – М.: Юрайт, 2025. – 252 с.

3.2.2. Электронные образовательные ресурсы

1. Внуков А.А. Основы информационной безопасности: защита информации. – Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/542340
2. Казарин О.В., Шубинский И.Б. Основы информационной безопасности: надёжность и безопасность программного обеспечения. – Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/580668
3. OWASP Top 10 и OWASP Cheat Sheet Series. – URL: https://owasp.org/www-project-top-ten/ ; https://cheatsheetseries.owasp.org/
4. Документация Laravel (разделы «Аутентификация», «Авторизация», «Защита от CSRF», «Хеширование», «Шифрование»). – URL: https://laravel.com/docs
5. Руководство по PHP: раздел «Безопасность». – URL: https://www.php.net/manual/ru/security.php
6. Банк данных угроз безопасности информации ФСТЭК России. – URL: https://bdu.fstec.ru/
7. Pro Git (Скотт Чакон, Бен Штрауб). – URL: https://git-scm.com/book/ru/v2
8. Документация GigaChat API. – URL: https://developers.sber.ru/docs/ru/gigachat/overview
9. GitVerse. Платформа для работы с исходным кодом и GigaCode. – URL: https://gitverse.ru/
10. Материалы, тесты и задания по дисциплине в системе дистанционного обучения колледжа (Moodle).

3.2.3. Дополнительные источники

1. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2014. – 702 с.
2. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».
4. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

5. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
6. Национальный кодекс этики в сфере искусственного интеллекта (Альянс в сфере ИИ, 2021).

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических и лабораторных занятий, тестирования, контрольных работ, а также выполнения обучающимися индивидуальных заданий. Оценка освоения дисциплины предусматривает использование пятибалльной системы оценки.

Результаты обучения	Критерии оценки	Формы и методы оценки
Перечень умений, осваиваемых в рамках дисциплины: – классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации; – оценивать риски информационной безопасности и выбирать меры защиты для автоматизированного рабочего места и информационной системы; – выявлять и устранять типовые уязвимости веб-приложений на PHP/Laravel (внедрение SQL-кода, межсайтовое выполнение сценариев, подделка межсайтовых запросов, нарушение контроля доступа); – реализовывать безопасную аутентификацию и разграничение доступа пользователей, обеспечивать безопасное хранение паролей, ключей и секретов в проекте и репозитории Git; – находить и применять нормативные правовые документы по защите информации и персональных данных, в том числе в справочно-правовых системах; – читать описания уязвимостей и рекомендации по безопасности (OWASP, CVE, документация фреймворков) на русском и английском	«Отлично» – теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» – теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» – теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Тестирование (Moodle) Оценка и защита практических работ Контрольные работы по разделам Наблюдение за выполнением практических заданий Дифференцированный зачёт (практико-ориентированное задание и устный ответ)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Результаты обучения	Критерии оценки	Формы и методы оценки
языках; – безопасно использовать российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): обезличивать данные, проверять результат, распознавать попытки внедрения вредоносных инструкций (prompt injection). **Перечень знаний, осваиваемых в рамках дисциплины:** – сущность и понятие информационной безопасности, характеристику её составляющих; место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; жизненные циклы информации ограниченного доступа в процессе её создания, обработки, передачи; – источники угроз безопасности информации и меры по их предотвращению; факторы, воздействующие на информацию при её обработке в автоматизированных (информационных) системах; – современные средства и способы обеспечения информационной безопасности, основы криптографической защиты информации; – основные методики анализа угроз и рисков информационной безопасности; – основные положения законодательства о защите информации и персональных данных (Федеральные законы №149-ФЗ и №152-ФЗ), систему сертификации и лицензирования в области защиты информации; – классификацию уязвимостей веб-приложений (OWASP Top		

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Результаты обучения	Критерии оценки	Формы и методы оценки
10) и способы защиты от них в PHP/Laravel; принципы безопасной работы с базами данных; – требования к хранению секретов и учётных данных, правила безопасной работы с репозиториями Git; – возможности, ограничения и риски применения ИИ-ассистентов (утечка данных, «галлюцинации», внедрение вредоносных инструкций); требования 152-ФЗ при их использовании.		

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Лист подписей

ГАПОУ СО «Нижнетагильский торгово-экономический колледж»
SHA-256 исходного документа: e555fdcb1daf9d873e54b58691ec20fd5910583fc03ed94227bdcf397e71a3eb
Документ: 20 страниц
Проверка подписей:
https://sig.nttek.ru/v/hCS9xmVrxQiQ1RbcWk7uAmRbUZFHtXivNkEMoA2CmQHIdWqS
Печатная форма сформирована: 13.10.2026 10:27

№	Роль в подписи	Подписант	Сертификат	Дата и время подписания	Результат проверки
1	Утверждаю	Дмитриева Марина Георгиевна Заместитель директора по учебной работе	№ 7E9C18960643A37EF2C929CD1E513CCD, действителен с 08.10.2026 по 08.10.2027	13.10.2026 10:26:37	**подпись действительна** роль и должность подтверждены подписью

Печатная форма не подписывается и служит для удобства чтения. Юридическую силу имеют исходный PDF-документ и файлы электронных подписей (.sig). Подпись — усиленная неквалифицированная электронная подпись (ч. 3 ст. 5 Федерального закона № 63-ФЗ), выданная удостоверяющим центром колледжа.
Время указано по часовому поясу колледжа (Asia/Yekaterinburg, UTC+5).