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
09.02.12 Техническая эксплуатация и сопровождение информационных систем

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 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

**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» ..... 16

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» ..... 19



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 образовательной программы по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем. Дисциплина изучается на третьем курсе в пятом (50 часов) и шестом (22 часа) семестрах; экзамен проводится в шестом семестре. Дисциплина опирается на ОП.01 «Операционные системы и среды», ОП.02 «Архитектура аппаратных средств и основы сетевых технологий», ОП.04 «Математический аппарат в отрасли информационных технологий» и ОП.09 «Основы компьютерных сетей» и формирует основу для выполнения профессиональных задач по обнаружению инцидентов информационной безопасности в ПМ.01 (ПК 1.7) и ПМ.02 (ПК 2.5).

**Цель дисциплины:** формирование у обучающихся знаний о целях, угрозах и методах защиты информации, умений настраивать базовые механизмы защиты серверов Linux, сетей и контейнеров (управление доступом, криптографическая защита, TLS и SSH, межсетевые экраны, укрепление операционной системы, резервное копирование), навыков выявления инцидентов информационной безопасности и передачи информации о них в службу ИБ, знаний требований законодательства о персональных данных (152-ФЗ), а также навыков безопасного применения российских ИИ-ассистентов (GigaChat, Алиса AI).

## 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<br>ОК 02<br>ОК 09<br>ПК 1.7<br>ПК 2.5 | – классифицировать защищаемую информацию по видам тайны и категориям доступа, определять объекты защиты и источники угроз;<br>– классифицировать угрозы и уязвимости информационной системы, строить модель угроз и оценивать риски информационной безопасности;<br>– применять нормативные правовые | – сущность и понятие информационной безопасности, свойства информации (конфиденциальность, целостность, доступность), место ИБ в системе национальной безопасности;<br>– виды, источники и носители защищаемой информации, жизненный цикл информации ограниченного доступа; |



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 |
|---|---|---|
| | акты и стандарты в области защиты информации и персональных данных (149-ФЗ, 152-ФЗ), определять уровень защищённости персональных данных;<br>– настраивать идентификацию, аутентификацию и разграничение доступа в Linux (пользователи, группы, sudo, ACL, политика паролей);<br>– применять средства криптографической защиты: хэширование, шифрование, электронную подпись, сертификаты X.509, протокол TLS, защищённый доступ по SSH;<br>– настраивать межсетевой экран (nftables, ufw), выполнять базовое укрепление (hardening) операционной системы Debian/Ubuntu, безопасно настраивать контейнеры Docker и Docker Compose;<br>– организовывать резервное копирование и восстановление данных, анализировать журналы и идентифицировать инциденты информационной безопасности (ПК 1.7, ПК 2.5), оформлять сообщение об инциденте;<br>– читать описания уязвимостей и рекомендации по безопасности на русском и английском языках (БДУ ФСТЭК, CVE, документация);<br>– безопасно использовать российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): обезличивать данные, проверять результат, распознавать внедрение вредоносных инструкций (prompt injection). | – источники угроз безопасности информации, типовые атаки и меры противодействия; методики анализа угроз и рисков;<br>– основные положения законодательства о защите информации и персональных данных (149-ФЗ, 152-ФЗ, 187-ФЗ), систему лицензирования и сертификации средств защиты;<br>– модели управления доступом (DAC, MAC, RBAC), принцип наименьших привилегий, методы аутентификации, основы парольной защиты;<br>– основы криптографической защиты информации, российские криптографические стандарты, назначение PKI, TLS и SSH;<br>– принципы сетевой безопасности, назначение межсетевых экранов, VPN и систем обнаружения вторжений; основы укрепления Linux и безопасности контейнеров;<br>– принципы резервного копирования (правило 3-2-1, RPO и RTO), основы аудита и мониторинга, понятие и классификацию инцидентов ИБ, процедуры и регламенты передачи информации об инцидентах;<br>– 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 |



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

| Код | Наименование общей компетенции |
|---|---|
| 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. |

## 1.3. Междисциплинарные связи и используемые информационные технологии

Результаты освоения дисциплины используются в других дисциплинах и профессиональных модулях специальности; в свою очередь, дисциплина опирается на материал, изученный ранее. Ключевые связи приведены в таблице.

| Дисциплина, модуль | Содержание связи |
|---|---|
| ОП.01 Операционные системы и среды | Права доступа Linux, пользователи и группы, systemd, журналы и сигналы – основа тем 3.1, 4.2, 5.2; на них строятся практические работы №4, 10, 13. |
| ОП.02 Архитектура аппаратных средств и основы сетевых технологий | Устройство серверов и сетевого оборудования, модель взаимодействия открытых систем – база для темы 4.1 (сегментация, межсетевой экран, VPN). |
| ОП.03 Информационные технологии в профессиональной деятельности | Работа со справочно-правовыми системами и поиск нормативных актов – тема 2.1; оформление документов оператора – практическая работа №3. |
| ОП.04 Математический аппарат в отрасли информационных технологий | Комбинаторика и энтропия пароля, вероятность и риск, формула Байеса для оценки срабатываний системы обнаружения, расчёт доступности и ёмкости хранилища резервных копий – темы 1.2, 3.1, 5.1. |
| ОП.06 Базы данных | Права и роли СУБД, резервные копии и дампы, защита от SQL-инъекций и учёт действий пользователей – темы 3.1, 5.1, 5.2 (ПК 2.5). |
| ОП.07 Основы алгоритмизации и программирования | Сценарии Bash и Python, используемые для проверки хэшей, резервного копирования и анализа журналов – практические работы №5, 12, 13. |
| ОП.09 Основы компьютерных сетей | Протоколы TCP/IP, DNS, маршрутизация и фильтрация – основа тем 3.3, 3.4, 4.1; практические работы №6–9. |
| ПМ.01 Техническая поддержка процессов создания (модификации) и сопровождения информационных систем | Темы 3.4, 4.1, 4.2, 5.2 формируют ПК 1.7: обнаружение инцидентов ИБ, связанных с работой информационных систем, и передача информации о них; безопасное развёртывание на Docker и CI/CD – тема 4.3. |
| ПМ.02 Администрирование | Темы 5.1 и 5.2 формируют ПК 2.5: выявление инцидентов |



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

| Дисциплина, модуль | Содержание связи |
|---|---|
| баз данных | ИБ при обеспечении функционирования баз данных, временное блокирование доступа к элементам БД, резервное копирование и восстановление. |
| СГ.04 Иностранный язык в профессиональной деятельности | Чтение описаний уязвимостей, документации OpenSSL, nftables, Docker и сообщений об ошибках на английском языке. |

**Работа с искусственным интеллектом.** Тема 6.1 и практическая работа №14 посвящены безопасному применению российских ИИ-ассистентов (GigaChat, GigaCode, Алиса AI, YandexGPT): рискам утечки данных, «галлюцинациям», небезопасным командам и коду, внедрению вредоносных инструкций (prompt injection) и требованиям 152-ФЗ. В практических работах №2, 9, 10 и 13 ассистент используется как вспомогательное средство (черновик перечня угроз, пояснение вывода nmap и конфигурации, разбор журнала после обезличивания); результат обязательно проверяется по документации, БДУ ФСТЭК и в изолированной среде, использование ИИ указывается в отчёте. Запрещается передавать ИИ-сервисам пароли, ключи, адреса и топологию реальных сетей, журналы, персональные данные и иные конфиденциальные сведения. Решения о блокировке доступа и изменении настроек принимает человек. На контрольных работах, тестировании и экзамене 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** | **72** |
| **в том числе:** | |
| теоретическое обучение | 44 |
| лабораторные и практические занятия | 28 |
| самостоятельная работа | – |
| промежуточная аттестация (экзамен) | в пределах общего объема |

Дисциплина изучается на 3 курсе в 5–6 семестре. Форма промежуточной аттестации – экзамен.

### 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. Основы информационной безопасности: объекты, угрозы и риски (11 ч)** | | | |
| **Тема 1.1. Основные понятия информационной безопасности. Объекты защиты, угрозы и уязвимости** | **Содержание учебного материала**<br>1. Информационная безопасность и защита информации: понятия, цели, задачи. Свойства информации: конфиденциальность, целостность, доступность (триада CIA), подотчётность и неотказуемость. Место ИБ в системе национальной безопасности, Доктрина информационной безопасности РФ.<br>2. Виды защищаемой информации: государственная тайна, коммерческая тайна, персональные данные, служебная тайна, информация общего пользования. Носители и жизненный цикл информации: создание, обработка, хранение, передача, уничтожение.<br>3. Объекты защиты информационной системы специальности: серверы Linux, сетевое оборудование, базы данных, контейнеры, репозитории, резервные копии, учётные данные и ключи.<br>4. Угрозы, уязвимости, атаки, риск: соотношение понятий. Источники угроз (внешние и внутренние нарушители, стихийные и технические факторы). Классификация угроз по свойствам информации и по способу реализации.<br>5. Типовые атаки: подбор пароля, фишинг и социальная инженерия, вредоносное ПО и шифровальщики, атаки отказа в обслуживании (DDoS), перехват трафика (MITM), эксплуатация уязвимостей, компрометация цепочки поставок. | 5 | 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 |
|---|---|---|---|
| | 6. Источники сведений об уязвимостях: Банк данных угроз безопасности информации ФСТЭК России, базы CVE; чтение описаний на русском и английском языках. Модель угроз и модель нарушителя. | | |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №1 «Классификация защищаемой информации и построение модели угроз типовой информационной системы (веб-сервер, база данных, контейнеры)» | 2 | |
| **Тема 1.2. Анализ и оценка рисков информационной безопасности. Политика безопасности** | **Содержание учебного материала**<br>1. Понятие риска: вероятность реализации угрозы и ущерб. Качественная и количественная оценка; матрица рисков; ожидаемые годовые потери.<br>2. Методы обработки риска: снижение, принятие, передача (страхование), уклонение. Остаточный риск. Экономическое обоснование мер защиты.<br>3. Политика информационной безопасности организации: структура, роли и ответственность, принцип наименьших привилегий, разделение обязанностей, многоуровневая защита (defence in depth).<br>4. Применение ИИ-ассистента при подготовке перечня угроз: что можно поручить, как проверить результат по БДУ ФСТЭК и документации. | 2 | ОК 01, ОК 02 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №2 «Оценка рисков информационной безопасности: матрица «вероятность – ущерб» и выбор мер защиты» | 2 | |
| **Раздел 2. Правовые и организационные основы защиты информации (8 ч)** | | | |
| **Тема 2.1. Законодательство о защите информации и персональных данных. Сертификация и лицензирование** | **Содержание учебного материала**<br>1. Система нормативных актов: Федеральные законы № 149-ФЗ «Об информации, информационных технологиях и о защите информации», № 152-ФЗ «О персональных данных», № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», № 63-ФЗ «Об электронной подписи».<br>2. Персональные данные: категории (общие, специальные, биометрические), оператор, субъект, согласие, права субъекта, обязанности оператора, локализация данных, уведомление Роскомнадзора, утечки персональных данных.<br>3. Уровни защищённости персональных данных в информационных системах (Постановление Правительства РФ № 1119), состав мер по приказу ФСТЭК России № 21; классы | 4 | 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 |
|---|---|---|---|
| | защищённости государственных информационных систем (приказ ФСТЭК России № 17).<br>4. Ответственность за нарушения: административная (КоАП РФ), уголовная (глава 28 УК РФ – преступления в сфере компьютерной информации), дисциплинарная и материальная.<br>5. Лицензирование и сертификация в области защиты информации: роль ФСТЭК России и ФСБ России, сертифицированные средства защиты, сертификаты соответствия.<br>6. Требования 152-ФЗ при использовании ИИ-ассистентов: недопустимость передачи персональных данных и конфиденциальных сведений внешним сервисам, обезличивание. | | |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №3 «Классификация информационной системы персональных данных, определение уровня защищённости и подготовка документов оператора» | 2 | |
| **Тема 2.2. Организационные меры защиты. Стандарты управления ИБ. Человеческий фактор** | **Содержание учебного материала**<br>1. Стандарты семейства ГОСТ Р ИСО/МЭК 27000 и система менеджмента информационной безопасности (СМИБ): цикл «планирование – выполнение – проверка – совершенствование».<br>2. Организационные меры: должностные инструкции, допуск к информации, соглашения о неразглашении, инструктаж, контроль доступа в помещения, управление носителями.<br>3. Социальная инженерия и человеческий фактор: фишинг, претекстинг, физическое проникновение; обучение пользователей и правила безопасного поведения. Правила деловой переписки при сообщении об инцидентах.<br>4. Взаимодействие технической поддержки со службой информационной безопасности заказчика: каналы связи, регламент передачи информации, ответственность. | 2 | ОК 01, ОК 02, ПК 1.7 |
| **Раздел 3. Управление доступом, криптография, PKI и защищённый удалённый доступ (18 ч)** | | | |
| **Тема 3.1. Идентификация, аутентификация и авторизация. Модели управления доступом** | **Содержание учебного материала**<br>1. Идентификация, аутентификация, авторизация и учёт действий (AAA). Факторы аутентификации; многофакторная аутентификация; одноразовые пароли (TOTP).<br>2. Хранение паролей: хэш, соль, медленные функции (bcrypt, Argon2, yescrypt в /etc/shadow); парольные политики и менеджеры паролей.<br>3. Модели доступа: дискреционная (DAC), мандатная (MAC), ролевая (RBAC); права Linux, | 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 |
|---|---|---|---|
| | ACL (setfacl), sudo и файлы sudoers, подключаемые модули аутентификации PAM, принцип наименьших привилегий.<br>4. Типовые ошибки: общие учётные записи, права 777, оставленные пароли по умолчанию, избыточные права служб. | | |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №4 «Управление доступом в Linux: учётные записи, sudo, списки ACL и политика паролей» | 2 | |
| **Тема 3.2. Основы криптографической защиты информации** | **Содержание учебного материала**<br>1. Задачи криптографии. Симметричные алгоритмы (AES; российские ГОСТ Р 34.12-2015 «Кузнечик» и «Магма»), режимы шифрования, длина ключа.<br>2. Асимметричные алгоритмы (RSA, эллиптические кривые), обмен ключами. Гибридное шифрование.<br>3. Хэш-функции (SHA-256, ГОСТ Р 34.11-2012 «Стрибог»): свойства, контроль целостности, коды аутентичности сообщений (HMAC).<br>4. Электронная подпись: принцип, ГОСТ Р 34.10-2012, Федеральный закон № 63-ФЗ, виды подписей. Стеганография как смежное направление.<br>5. Практическое применение: утилиты sha256sum, openssl, gpg; шифрование данных «в покое» и «в передаче». | 3 | ОК 01, ОК 02 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №5 «Хэширование, симметричное шифрование и электронная подпись средствами OpenSSL и GnuPG» | 2 | |
| **Тема 3.3. Инфраструктура открытых ключей, сертификаты X.509 и протокол TLS** | **Содержание учебного материала**<br>1. Инфраструктура открытых ключей (PKI): удостоверяющий центр, цепочка доверия, корневой и промежуточный сертификаты, срок действия и отзыв (CRL, OCSP).<br>2. Структура сертификата X.509: субъект, издатель, открытый ключ, расширения (subjectAltName). Запрос на сертификат (CSR).<br>3. Протокол TLS 1.2 и 1.3: рукопожатие, наборы шифров, прямая секретность, HSTS. Типовые ошибки: просроченный сертификат, несоответствие имени, устаревшие протоколы.<br>4. Автоматизация выпуска сертификатов (протокол ACME), хранение закрытых ключей и права доступа к ним. | 3 | ОК 01, ОК 02, ОК 09 |
| | **В том числе практических занятий и лабораторных работ** | 2 | |



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 |
|---|---|---|---|
| | 1. Практическая работа №6 «Собственный удостоверяющий центр на OpenSSL, сертификат X.509 и настройка TLS на веб-сервере nginx» | | |
| **Тема 3.4. Безопасный удалённый доступ: SSH** | **Содержание учебного материала**<br>1. Протокол SSH: аутентификация сервера (known_hosts), аутентификация клиента по паролю и по ключам, ssh-agent, переадресация портов и её риски.<br>2. Укрепление sshd_config: PermitRootLogin no, PasswordAuthentication no, AllowUsers, смена порта как вспомогательная мера, ограничение числа попыток.<br>3. Защита от подбора: fail2ban, ограничение по адресам межсетевым экраном; признаки подбора в журнале auth.log.<br>4. Управление ключами: генерация (ssh-keygen, ed25519), хранение, ротация и отзыв; запрет размещения закрытых ключей в репозиториях Git. | 2 | ОК 01, ОК 02, ОК 09, ПК 1.7 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №7 «Безопасная настройка SSH: ключевая аутентификация, запрет входа по паролю и под root, защита от подбора» | 2 | |
| **Раздел 4. Защита сетей, операционных систем и контейнеров (18 ч)** | | | |
| **Тема 4.1. Сетевая безопасность: сегментация, межсетевые экраны, VPN, обнаружение вторжений** | **Содержание учебного материала**<br>1. Угрозы сетевого уровня: сканирование, перехват, подмена ARP и DNS, DDoS. Сегментация сети, DMZ, VLAN как мера изоляции.<br>2. Межсетевые экраны: фильтрация с отслеживанием состояния соединений, политика по умолчанию «запретить», nftables и ufw в Debian/Ubuntu, журналирование отброшенных пакетов.<br>3. VPN (WireGuard, OpenVPN, IPsec): назначение и принципы; защита каналов между площадками.<br>4. Системы обнаружения и предотвращения вторжений (IDS/IPS), fail2ban; сканирование собственной инфраструктуры (nmap) как метод контроля и границы допустимого: только разрешённые узлы.<br>5. Защита служб: привязка к интерфейсам, закрытие лишних портов, обратный прокси и ограничение частоты запросов. | 4 | ОК 01, ОК 02, ОК 09, ПК 1.7 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №8 «Межсетевой экран nftables и ufw: политика «запрещено всё, кроме разрешённого» на учебном стенде»<br>2. Практическая работа №9 «Сканирование собственного стенда (nmap) и анализ открытых | 4 | |



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 |
|---|---|---|---|
| | портов и журналов аутентификации» | | |
| **Тема 4.2. Укрепление (hardening) операционной системы Linux** | **Содержание учебного материала**<br>1. Принципы укрепления: минимизация поверхности атаки, своевременное обновление (unattended-upgrades), удаление лишних пакетов и служб.<br>2. Права и файловая система: SUID/SGID, параметры монтирования (noexec, nosuid, nodev), разделение разделов, защита /etc и ключей.<br>3. Параметры ядра sysctl, обязательное разграничение доступа (AppArmor), песочница служб systemd (ProtectSystem, NoNewPrivileges и др.).<br>4. Аудит и проверка соответствия: Lynis, рекомендации CIS, подсистема auditd. Фиксация исходного состояния и отчёт об устранённых замечаниях.<br>5. Борьба с вредоносным ПО: антивирусное ПО на серверах Linux, актуализация баз сигнатур. | 3 | ОК 01, ОК 02, ПК 1.7 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №10 «Укрепление (hardening) Debian/Ubuntu: чек-лист, аудит утилитой Lynis, ограничение служб systemd» | 2 | |
| **Тема 4.3. Безопасность контейнеров и конвейера CI/CD** | **Содержание учебного материала**<br>1. Модель угроз контейнеров: общее ядро, побег из контейнера, уязвимые базовые образы, секреты в образах.<br>2. Безопасный Dockerfile: минимальный базовый образ, фиксированные версии, непривилегированный пользователь (USER), отсутствие секретов в слоях, многоэтапная сборка.<br>3. Параметры запуска и Compose: read_only, cap_drop, no-new-privileges, ограничения ресурсов, закрытые сети, недопустимость привилегированных контейнеров и монтирования docker.sock.<br>4. Сканирование образов и зависимостей на известные уязвимости; безопасное хранение секретов в Docker secrets и переменных CI.<br>5. Безопасность CI/CD (GitVerse Actions): секреты репозитория, права токенов, проверка зависимостей, защита основной ветки. | 3 | ОК 01, ОК 02, ОК 09 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №11 «Безопасный Dockerfile и Docker Compose: непривилегированный пользователь, секреты, ограничение ресурсов и сканирование образа» | 2 | |
| **Раздел 5. Защита данных, аудит, мониторинг и реагирование на инциденты (11 ч)** | | | |
| **Тема 5.1. Защита** | **Содержание учебного материала** | 3 | 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 |
|---|---|---|---|
| **данных: резервное копирование и восстановление, шифрование носителей** | 1. Резервное копирование как мера обеспечения доступности и целостности. Показатели RPO и RTO. Полные, дифференциальные и инкрементные копии.<br>2. Правило 3-2-1; неизменяемые и внешние копии как защита от шифровальщиков; шифрование копий и хранение ключей отдельно от данных.<br>3. Инструменты: rsync, tar, restic, дампы СУБД (mysqldump). Сценарии Bash, расписание (cron и таймеры systemd), контроль успешного выполнения.<br>4. Проверка восстановления: регулярные учебные восстановления, контрольные суммы. Шифрование диска и разделов (LUKS), безопасное удаление данных. | | ПК 2.5 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №12 «Резервное копирование с шифрованием и проверка восстановления: rsync, restic, сценарий Bash и расписание» | 2 | |
| **Тема 5.2. Журналирование, аудит, мониторинг и управление инцидентами информационной безопасности** | **Содержание учебного материала**<br>1. Журналы ИС: journald, rsyslog, auth.log, журналы nginx и СУБД. Централизованный сбор, синхронизация времени, защита журналов от изменения.<br>2. Мониторинг и оповещения (Prometheus, Grafana) как средство обнаружения аномалий; понятие SIEM и корреляции событий.<br>3. Понятие и классификация инцидентов ИБ, типовые признаки (подбор пароля, необычные выгрузки данных из БД, изменение конфигураций, вредоносные процессы). Инциденты при работе с БД.<br>4. Жизненный цикл реагирования: подготовка, обнаружение, локализация, устранение, восстановление, анализ уроков. Временное блокирование доступа к системе или элементам БД при обнаружении инцидента.<br>5. Процедуры и регламенты передачи информации об инциденте в службу ИБ: содержание сообщения, сроки, каналы; взаимодействие с ГосСОПКА и Роскомнадзором при утечках ПДн.<br>6. Основы цифровой криминалистики: сохранение доказательств, цепочка хранения, снимок диска и журналов. | 4 | ОК 01, ОК 02, ОК 09, ПК 1.7, ПК 2.5 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №13 «Анализ журналов, выявление инцидента ИБ и оформление сообщения об инциденте в службу | 2 | |



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 |
|---|---|---|---|
| | информационной безопасности» | | |
| **Раздел 6. Безопасное применение ИИ-ассистентов (6 ч)** | | | |
| **Тема 6.1. Российские ИИ-ассистенты и информационная безопасность** | **Содержание учебного материала**<br>1. Российские ИИ-ассистенты: GigaChat, GigaCode (интегрирован с GitVerse), Алиса AI, YandexGPT; возможности и ограничения; режимы применения (чат, API, помощник в редакторе).<br>2. Риски: утечка паролей, ключей, персональных данных и конфиденциальных сведений через запросы; «галлюцинации»; небезопасный код и опасные команды в ответах; внедрение вредоносных инструкций (prompt injection) через обрабатываемые тексты и журналы; отравление данных.<br>3. Правила безопасной работы: обезличивание, запрет передачи секретов и данных заказчика, использование только одобренных колледжем сервисов, проверка ответа по документации и в изолированной среде, указание использования ИИ (академическая добросовестность), запрет ИИ на контрольных и экзамене.<br>4. Допустимые прикладные сценарии в ИБ: пояснение конфигурации и журнала, подготовка чек-листа hardening, черновик политики или инструкции, генерация тестовых данных; недопустимые: принятие решений о блокировке без проверки, передача реальных журналов.<br>5. Нормативные основы: 152-ФЗ, Национальный кодекс этики в сфере искусственного интеллекта; ответственность оператора за утечку. | 4 | ОК 01, ОК 02, ОК 09, ПК 1.7 |
| | **В том числе практических занятий и лабораторных работ**<br>1. Практическая работа №14 «Безопасное применение российских ИИ-ассистентов: обезличивание данных, проверка ответа и оформление использования ИИ» | 2 | |
| **Промежуточная аттестация: экзамен (проводится в пределах общего объема)** | | | |
| **Всего:** | | **72** | |



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

**Лаборатория «Основ информационной безопасности» (кабинет информационной безопасности), оснащённая 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 системы дистанционного обучения Moodle;

– программное обеспечение: Debian/Ubuntu (в виртуальных машинах), OpenSSL, GnuPG, nginx, OpenSSH, nftables и ufw, fail2ban, nmap (только в изолированной учебной сети), Lynis, Docker и Docker Compose, restic и rsync, Git, Python 3;

– изолированная учебная сеть для виртуальных машин (стенд из сервера, клиента и «нарушителя») без доступа к сетям колледжа;

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

– комплект раздаточных материалов: матрицы рисков, образцы политик и регламентов, формы сообщения об инциденте.

### 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. Баланов А.Н. Защита информационных систем. Кибербезопасность: учебное пособие для СПО. – СПб.: Лань, 2024. – 84 с. – ISBN 978-5-507-48808-7.



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

2. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для СПО. – СПб.: Лань, 2024. – 284 с. – ISBN 978-5-507-49251-0.
3. Нестеров С.А. Основы информационной безопасности: учебник для СПО. – 2-е изд., стер. – СПб.: Лань, 2022. – 324 с. – ISBN 978-5-8114-9489-7.
4. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО. – 5-е изд., стер. – СПб.: Лань, 2024. – 124 с. – ISBN 978-5-507-47517-9.

### 3.2.2. Электронные образовательные ресурсы

1. Баланов А.Н. Защита информационных систем. Кибербезопасность. – Электронно-библиотечная система «Лань». – URL: https://e.lanbook.com/book/394547
2. Баланов А.Н. Комплексная информационная безопасность. – Электронно-библиотечная система «Лань». – URL: https://e.lanbook.com/book/414950
3. Нестеров С.А. Основы информационной безопасности. – Электронно-библиотечная система «Лань». – URL: https://e.lanbook.com/book/195510
4. Прохорова О.В. Информационная безопасность и защита информации. – Электронно-библиотечная система «Лань». – URL: https://e.lanbook.com/book/385082
5. Банк данных угроз безопасности информации ФСТЭК России. – URL: https://bdu.fstec.ru/
6. Документация Debian и Ubuntu (Руководство по безопасности, OpenSSH, nftables, ufw). – URL: https://www.debian.org/doc/ ; https://help.ubuntu.com/
7. Документация Docker (разделы Security, Compose). – URL: https://docs.docker.com/
8. OWASP Cheat Sheet Series. – URL: https://cheatsheetseries.owasp.org/
9. Документация GigaChat API. – URL: https://developers.sber.ru/docs/ru/gigachat/overview
10. GitVerse. Платформа для работы с исходным кодом и GigaCode. – URL: https://gitverse.ru/
11. Курс «Основы информационной безопасности» в системе дистанционного обучения колледжа (Moodle).

### 3.2.3. Дополнительные источники

1. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».



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

3. Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».
5. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
6. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
8. ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015 (криптографические стандарты).
9. Национальный кодекс этики в сфере искусственного интеллекта (Альянс в сфере искусственного интеллекта, 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:**<br>– классифицировать защищаемую информацию по видам тайны и категориям доступа, определять объекты защиты и источники угроз;<br>– классифицировать угрозы и уязвимости информационной системы, строить модель угроз и оценивать риски информационной безопасности;<br>– применять нормативные правовые акты и стандарты в области защиты информации и персональных данных (149-ФЗ, 152-ФЗ), определять уровень защищённости персональных данных;<br>– настраивать идентификацию, аутентификацию и разграничение доступа в Linux (пользователи, группы, sudo, ACL, политика паролей);<br>– применять средства криптографической защиты: хэширование, шифрование, электронную подпись, сертификаты X.509, протокол TLS, защищённый доступ по SSH;<br>– настраивать межсетевой экран (nftables, ufw), выполнять базовое укрепление (hardening) операционной системы Debian/Ubuntu, безопасно настраивать контейнеры Docker и Docker Compose;<br>– организовывать резервное копирование и восстановление | «Отлично» – теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко.<br>«Хорошо» – теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.<br>«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.<br>«Неудовлетворительно» – теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки. | Тестирование (Moodle)<br>Оценка и защита практических работ<br>Контрольные работы по разделам<br>Наблюдение за выполнением практических заданий на учебном стенде<br>Экзамен (устный ответ по билету и практическое задание) |



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 |
|---|---|---|
| данных, анализировать журналы и идентифицировать инциденты информационной безопасности (ПК 1.7, ПК 2.5), оформлять сообщение об инциденте;<br>– читать описания уязвимостей и рекомендации по безопасности на русском и английском языках (БДУ ФСТЭК, CVE, документация);<br>– безопасно использовать российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): обезличивать данные, проверять результат, распознавать внедрение вредоносных инструкций (prompt injection).<br>**Перечень знаний, осваиваемых в рамках дисциплины:**<br>– сущность и понятие информационной безопасности, свойства информации (конфиденциальность, целостность, доступность), место ИБ в системе национальной безопасности;<br>– виды, источники и носители защищаемой информации, жизненный цикл информации ограниченного доступа;<br>– источники угроз безопасности информации, типовые атаки и меры противодействия; методики анализа угроз и рисков;<br>– основные положения законодательства о защите информации и персональных данных (149-ФЗ, 152-ФЗ, 187-ФЗ), систему лицензирования и сертификации средств защиты;<br>– модели управления доступом (DAC, MAC, RBAC), принцип наименьших привилегий, методы аутентификации, основы парольной защиты;<br>– основы криптографической защиты информации, российские | | |



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 |
|---|---|---|
| криптографические стандарты, назначение PKI, TLS и SSH;<br>– принципы сетевой безопасности, назначение межсетевых экранов, VPN и систем обнаружения вторжений; основы укрепления Linux и безопасности контейнеров;<br>– принципы резервного копирования (правило 3-2-1, RPO и RTO), основы аудита и мониторинга, понятие и классификацию инцидентов ИБ, процедуры и регламенты передачи информации об инцидентах;<br>– 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: ae3d40086ab98ac6353463ebb504d95c2e5a605178d5d66f72ee3bf3b6269b7c
Документ: 21 страница
Проверка подписей: https://sig.nttek.ru/v/kj8DHMONpe9lQ6cT9tdPO4eTHTUZyk1KKPGOVeQcQcX5kmsV
Печатная форма сформирована: 15.10.2026 09:46

| № | Роль в подписи | Подписант | Сертификат | Дата и время подписания | Результат проверки |
|---|---|---|---|---|---|
| 1 | Утверждаю | Дмитриева Марина Георгиевна<br>Заместитель директора по учебной работе | № 7E9C18960643A37EF2C929CD1E513CCD, действителен с 08.10.2026 по 08.10.2027 | 15.10.2026 09:43:24 | **подпись действительна**<br>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).