Министерство образования Иркутской области
Государственное бюджетное профессиональное
образовательное учреждение Иркутской области
«Иркутский авиационный техникум»

# Методические указания по выполнению самостоятельной работы по междисциплинарному курсу

МДК.01.02 Управление базами данных

специальности
09.02.11 Разработка и управление программным обеспечением

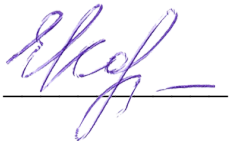
**Иркутск, 2026**

РАССМОТРЕНЫ

Председатель ЦК

_____ / /

УТВЕРЖДАЮ
Зам. директора


_____ Е.А. Коробкова

| № | Разработчик ФИО |
|---|---|
| 1 | Кудрявцева Марина Анатольевна |

## Пояснительная записка

МДК.01.02 Управление базами данных относится к ПМ.01 разработка, администрирование и защита баз данных. Самостоятельная работа является одним из видов учебно работы обучающегося без взаимодействия с преподавателем.

**Основные цели самостоятельной работы:**

- систематизация и закрепление теоретических знаний и практических умений обучающихся;
- углубление и расширение теоретических знаний, формирование умений использовать справочную документацию и дополнительную литературу;
- развитие познавательных способностей и активности обучающихся, творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельного мышления;
- развитие исследовательских умений.

**Рекомендации для обучающихся по выработке навыков самостоятельной работы:**

Внимательно читать план выполнения работы. Учиться кратко и емко излагать свои мысли. Обращать внимание на рекомендуемые источники.

## Тематический план

| Раздел Тема | Тема занятия | Название работы | Количество часов |
|---|---|---|---|
| **Раздел 1. Управление базами данных в системах управления базами данных** Тема 5. Обеспечение безопасной работы сервера системы управления базами данных | Методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование. | Методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование. | 2 |

**Самостоятельная работа №1**

**Название работы:** Методы создания и управления защищенными соединениями с базой данных, включая VPN-туннели и SSL-шифрование..

**Цель работы:** Спроектировать и обосновать архитектуру защищённого соединения между приложением и базой данных MySQL, используя SSL/TLS-шифрование и VPN-туннели, с учётом принципов безопасности, производительности и соответствия стандартам (например, PCI DSS, ISO 27001)..

**Уровень СРС:** воспроизводящая.

**Форма контроля:** Текстовый отчёт (до 3 страниц) или презентация (до 10 слайдов)..

**Количество часов на выполнение:** 2 часа.

**Задание:**

Вы - системный архитектор компании, разрабатывающей веб-приложение, работающее с MySQL 8.0+.

Приложение размещено в облачной среде (AWS/Azure), а MySQL — в изолированной подсети VPC, недоступной напрямую из интернета.

Ваша задача — обеспечить безопасный, надёжный и соответствующий стандартам доступ к БД для приложения.

Требования:

1. Используйте SSL/TLS для шифрования трафика между приложением и MySQL.
2. Используйте VPN-туннель (например, IPsec или WireGuard) для изоляции сети приложения от публичного интернета.
3. Опишите, какие компоненты должны быть защищены (клиент, сервер, сеть).
4. Обоснуйте выбор между SSL и VPN — когда использовать каждый, и почему их можно комбинировать.
5. Приведите примеры конфигураций (на уровне команд или файлов конфигурации):
    1. Для MySQL (my.cnf / mysqld.cnf).
    2. Для клиента (например, mysql CLI или Python mysql-connector-python).
    3. Для VPN (например, WireGuard конфиг).
6. Опишите процедуру управления сертификатами (выпуск, обновление, отозвание).
7. Укажите риск, если SSL не включён, и риск, если VPN не используется.
8. Предложите мониторинг и аудит для проверки защищённости соединения.

| **Критерий** | **Баллы** | **Описание** |
|---|---|---|
| **1. Корректное применение SSL/TLS** | 15 | Чётко описано, как включить SSL в MySQL, как настроить клиент, |

| Критерий | Баллы | Описание |
|---|---|---|
| | | какие сертификаты используются . Указаны обязательные параметры для MySQL 8.0+. |
| **2. Корректное применение VPN-туннеля** | 15 | Описан тип VPN , приведён рабочий конфиг (сервер и клиент), указаны подсети, порты, ключи, маршрутизация. Объяснено, как трафик направляется через туннель. |
| **3. Комбинирование SSL + VPN** | 10 | Обосновано, почему оба метода используются вместе: SSL — шифрование данных на уровне приложения, VPN — изоляция сети и защита от сетевых атак.<br>Это многоуровневая защита (defense in depth). |
| **4. Безопасная конфигурация MySQL** | 10 | Показаны правильные настройки в my.cnf: require_secure_transport = ON, ssl-ca, ssl-cert, ssl-key.<br>Указано использование hoststssl в mysql.user (через CREATE USER ... REQUIRE SSL). |
| **5. Управление сертификатами** | 10 | Описан процесс: генерация через OpenSSL, развертывание на сервере и клиентах, автоматическое обновление , отозвание.<br>Указан срок действия (например, 90 дней). |
| **6. Анализ рисков** | 10 | Чётко описаны риски: <br> — Без SSL: перехват логинов, |

| Критерий | Баллы | Описание |
| --- | --- | --- |
| | | паролей, данных в сети (например, через MITM). <br> — Без VPN: эксплуатация уязвимостей MySQL (например, CVE-2023-21971), брутфорс, DDoS, сканирование портов. |
| **7. Мониторинг и аудит** | 10 | Предложены инструменты : <br> — tcpdump / Wireshark для проверки шифрования (пакеты не в открытом виде)<br> — MySQL-логи: log_warnings = 2, log_error_verbosity = 3, проверка SHOW VARIABLES LIKE 'have_ssl';<br> — мониторинг сертификатов: ssl_exporter + Prometheus + Grafana<br> — аудит доступа: MySQL Audit Plugin или SIEM (ELK, Splunk). |
| **8. Ясность, структура, техническая точность** | 10 | Ответ логичен, без ошибок, использует корректную терминологию (например, не “SSL-подключение”, а “TLS-соединение с проверкой сертификата”). Нет размытых формулировок. |
| **9. Практическая применимость** | 10 | Решение не теоретическое — можно внедрить на реальной инфраструктуре. Указаны конкретные команды, файлы, параметры. Примеры работоспособны в |

| Критерий | Баллы | Описание |
| --- | --- | --- |
| | | Linux/Cloud. |

**Критерии оценки:**

оценка «5» - Набрано 90-100 баллов.

оценка «4» - Набрано 70-89 баллов.

оценка «3» - Набрано 50-69 баллов.