МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В.Н. Татищева»
(Астраханский государственный университет им. В.Н. Татищева)

Филиал АГУ им. В.Н. Татищева в г. Знаменске Астраханской области

СОГЛАСОВАНО
Руководитель ОПОП
Бориско С.Н.
«13» ноября 2025 г.

УТВЕРЖДАЮ
Председатель ЦК (МО)
Фисенко Т.Ю.
протокол заседания ЦК (МО) №3
от «13» ноября 2025 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по учебной дисциплине

Базы данных

Составитель	Бориско С.Н., к.т.н., доцент, завкафедрой ЗнМИ; Мустафаев Н.Г., к.т.н., доцент кафедры ЗнМИ; Тимошкин А.А., к.т.н., доцент кафедры ЗнМИ; Устинов А.С., к.т.н., доцент кафедры ЗнМИ; Каштанов Д.Ю., ассистент кафедры ЗнМИ
Согласовано с работодателями	Литвинов С.П., к.т.н., заместитель командира войсковой части 15644 по научно-исследовательской и испытательной работе; Кирьянов М.Н., ведущий инженер ПАО «Ростелеком»
Наименование специальности	09.02.12 Техническая эксплуатация и сопровождение информационных систем
Квалификация выпускника	Специалист по технической эксплуатации и сопровождению информационных систем
Форма обучения	очная
Год приема (курс)	2026 (2 курс)

Знаменск, 2025 г.

СОДЕРЖАНИЕ

1. Общие положения

Фонд оценочных средств (далее – ФОС) предназначен для контроля и оценки результатов освоения обучающимися учебной дисциплины «Базы данных».

ФОС включают контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с требованиями ФГОС СПО и содержанием рабочей программы учебной дисциплины.

2. Результаты освоения учебной дисциплины, подлежащие проверке

Код компетенции	Планируемые результаты освоения учебной дисциплины		
	Практический опыт	Умения	Знания
ОК 2	-способен применять теоретические знания на практике при работе с различными операционными системами; -умеет анализировать и решать задачи системного администрирования - готов к освоению новых технологий в области операционных систем и сред.	-определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации -выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска	-номенклатура информационных источников, применяемых в профессиональной деятельности -приемы структурирования информации

3. Распределение оценивания результатов обучения по видам контроля

Наименование элемента практического опыта, умений или знаний	Наименование оценочного средства текущего контроля и промежуточной аттестации	
	Текущий контроль	Промежуточная аттестация
ПО.1. способен применять теоретические знания на практике при работе с различными операционными системами ПО.2. умеет анализировать и решать задачи системного администрирования; ПО.3 готов к освоению новых технологий в области операционных систем и сред	Компьютерное тестирование на знание терминологии по теме. Контрольные задания, решение задач по теме.	Вопросы к экзамену
У1. определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации У2. выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска		

31. номенклатура информационных источников, применяемых в профессиональной деятельности 32. приемы структурирования информации		

4. Контрольные задания для оценки результатов освоения учебной дисциплины

4.1. Контрольные задания для текущего контроля

Раздел 1. Разработка, администрирование и защита баз данных

Тестовые задания

1. (ОВ) Основная цель защиты данных в хранилищах — это обеспечение трёх ключевых свойств информации:
a) Доступности, конфиденциальности и целостности (CIA-триада)
b) Скорости, объёма и стоимости
c) Масштабируемости, отказоустойчивости и производительности
d) Кэширования, индексирования и архивирования

2. (МВ) Какие из перечисленных угроз относятся к угрозам безопасности данных в хранилищах?
a) Атаки типа SQL-инъекция (SQL Injection)
b) Внутренние угрозы (действия недобросовестных сотрудников)
c) Аппаратные сбои (отказ дисков, контроллеров)
d) Перегрузка хранилища из-за большого количества запросов

3. (СО) Угроза, при которой злоумышленник получает доступ к данным, для просмотра которых у него нет полномочий, называется нарушением _____.
Ответ: _____

4. (ОВ) Случайное или умышленное изменение данных пользователем или процессом, не имеющим на это прав, — это нарушение:
a) Доступности
b) Целостности
c) Конфиденциальности
d) Аудитопригодности

5. (ОВ) Модель контроля доступа, при которой каждому объекту (файлу, таблице) присваивается метка безопасности (уровень секретности), а субъекту (пользователю) — уровень допуска, называется:
a) Дискреционное управление доступом (DAC)
b) Ролевое управление доступом (RBAC)
c) Мандатное управление доступом (MAC)
d) Управление доступом на основе атрибутов (ABAC)

6. (МВ) Какие из перечисленных механизмов относятся к аутентификации пользователя?
a) Пароль
b) Аппаратный токен (USB-ключ)

c) Биометрия (отпечаток пальца, сканирование лица)
d) Список контроля доступа (ACL)

7. (CO) Принцип безопасности, согласно которому пользователь должен иметь минимальный набор привилегий, необходимых для выполнения своей работы, называется принципом _____.
Ответ: _____

8. (OB) Механизм, который позволяет отслеживать и регистрировать все значимые события, происходящие в системе (кто, что, когда и с каким объектом сделал), называется:
a) Шифрование
b) Резервное копирование
c) Аудит (журналирование)
d) Сегментация сети

9. (MB) Какие утверждения о симметричном шифровании верны?
a) Для шифрования и расшифрования используется один и тот же ключ.
b) Алгоритмы симметричного шифрования, как правило, работают быстрее асимметричных.
c) Яркий пример — алгоритм RSA.
d) Основная проблема — безопасная передача секретного ключа сторонам.

10. (CO) Алгоритм шифрования, который стал промышленным стандартом для симметричного шифрования и использует блоки по 128 бит и ключи 128, 192 или 256 бит, называется _____.
Ответ (аббревиатура): _____

11. (OB) Шифрование, при котором данные шифруются непосредственно на устройстве хранения (накопителе или контроллере), называется:
a) Шифрование на уровне приложения
b) Шифрование на уровне файловой системы
c) Шифрование «на лету» (Transparent Data Encryption — TDE)
d) Шифрование на транспортном уровне (TLS)

12. (CO) Технология, обеспечивающая криптографическую защиту целостности и аутентичности данных с помощью секретного ключа, результат которой часто передаётся вместе с данными, называется _____ код (MAC).
Ответ (полное название): _____

13. (OB) Стратегия резервного копирования, предполагающая создание полной копии всех данных каждый раз, называется:
a) Полное копирование (Full Backup)
b) Инкрементальное копирование (Incremental Backup)
c) Дифференциальное копирование (Differential Backup)
d) Зеркалирование (Mirroring)

14. (MB) Какие из перечисленных характеристик являются важными для политики резервного копирования?
a) RPO (Recovery Point Objective) — целевая точка восстановления
b) RTO (Recovery Time Objective) — целевое время восстановления
c) SLA (Service Level Agreement) — соглашение об уровне обслуживания
d) Все перечисленные

15. (СО) Технология создания точной, побитовой копии физического диска или раздела для быстрого развёртывания или восстановления называется _____.
Ответ: _____

16. (ОВ) Механизм, который позволяет восстановить базу данных на определённый момент времени в прошлом, используя полную копию и журнал транзакций, называется:
a) Point-in-Time Recovery (PITR)
b) Flashback Recovery
c) Snapshot Recovery
d) Export/Import

17. (МВ) Какие меры относятся к физической защите хранилищ данных?
a) Контроль доступа в дата-центр (пропускная система, видеонаблюдение)
b) Огнестойкие сейфы для резервных копий
c) Системы контроля климата и бесперебойного питания (ИБП)
d) Настройка межсетевого экрана (брандмауэра)

18. (СО) Технология, которая предотвращает восстановление данных с физически выведенных из строя или списанных накопителей, называется _____ уничтожение данных.
Ответ: _____

19. (ОВ) Практика разделения сетевого трафика (например, на трафик баз данных, трафик приложений и трафик управления) с целью ограничения потенциального распространения атаки, называется:
a) Виртуализация
b) Сегментация сети
c) Туннелирование (VPN)
d) Балансировка нагрузки

20. (СО) Стандарт безопасности данных индустрии платёжных карт, который устанавливает требования к защите данных держателей карт, называется _____ (аббревиатура).
Ответ: _____

Ключ для проверки

Раздел 1:

1. **a)** Доступности, конфиденциальности и целостности (CIA-триада)
2. **a, b, c** (d — угроза производительности, но не напрямую безопасности в классическом смысле)
3. **конфиденциальности**
4. **b)** Целостности

Раздел 2:
5. **c)** Мандатное управление доступом (MAC)
6. **a, b, c** (d — механизм авторизации, а не аутентификации)
7. **наименьших привилегий** (least privilege)
8. **c)** Аудит (журналирование)

Раздел 3:
9. **a, b, d** (c — неверно, RSA — асимметричный алгоритм)
10. **AES** (Advanced Encryption Standard)
11. **c)** Шифрование «на лету» (Transparent Data Encryption — TDE)
12. **код аутентификации сообщения** (Message Authentication Code)

Раздел 4:
13. **a)** Полное копирование (Full Backup)
14. **d)** Все перечисленные
15. **образ диска** (disk image) или **снапшот** (snapshot) на аппаратном уровне
16. **a)** Point-in-Time Recovery (PITR)

Раздел 5:
17. **a, b, c** (d — мера сетевой безопасности)
18. **физическое** или **деструктивное** (physical destruction)
19. **b)** Сегментация сети
20. **PCI DSS** (Payment Card Industry Data Security Standard)

Контрольные задания:

Блок 1: Анализ угроз и политика безопасности

Задание 1. «Аудит информационных рисков для компании E-Store»
Компания «E-Store» — интернет-магазин электроники. У вас есть следующая информация о системе:

- **Данные:** База данных клиентов (ФИО, email, телефоны, история заказов, хэши паролей). Файловое хранилище с документами (накладные, договоры).
- **Инфраструктура:** Веб-сервер, сервер СУБД (PostgreSQL), файловый сервер. Есть сотрудники: администраторы, менеджеры, бухгалтерия.
- **Известные инциденты за год:** 1) Уволенный сотрудник скачал клиентскую базу перед уходом. 2) DDoS-атака привела к недоступности сайта на 3 часа. 3) Вирус-шифровальщик поразил файловый сервер.

Требуется:

1. Проведите **качественный анализ рисков**. Для каждого актива (БД клиентов, файловое хранилище, доступность сервиса) определите по 2 наиболее вероятные и значимые угрозы.
2. Постройте **матрицу рисков** (Вероятность х Ущерб) для выявленных угроз.
3. Разработайте **план обработки рисков** для двух угроз с наивысшим рейтингом: укажите меры снижения (контроль), передачи (страхование) или принятия риска.
4. Сформулируйте **положение о политике информационной безопасности** для компании (3-5 ключевых тезисов).

Задание 2. «Создание модели контроля доступа для банковского подразделения»
В отделе кредитования банка работают:

- **Кредитные аналитики** — создают заявки, вносят данные клиентов.
- **Начальник отдела** — видит все заявки своего отдела, утверждает/отклоняет.

- **Сотрудник службы безопасности (СБ)** — имеет право читать все заявки во всех отделах на предмет проверки, но не может их изменять.
- **Администратор БД** — имеет технический доступ для обслуживания, но не должен видеть финансовые данные.

Объекты доступа: Таблицы `credit_applications` (заявки), `clients` (клиенты), `internal_log` (журнал аудита).

Требуется:

1. Выберите наиболее подходящую **модель управления доступом** (DAC, MAC, RBAC, ABAC) для этого сценария и обоснуйте выбор.
2. Создайте **матрицу доступа** (строка — роль, столбец — объект/действие). Укажите для каждой роли: SELECT (чтение), INSERT (добавление), UPDATE (изменение), DELETE (удаление).
3. Напишите **SQL-скрипты** для создания ролей и назначения привилегий в соответствии с матрицей (на примере PostgreSQL или другой СУБД).
4. Предложите механизм для реализации требования: «Аналитик может редактировать заявку только в течение 24 часов с момента создания». Как это можно технически реализовать?

Блок 2: Реализация криптографической защиты

Задание 3. «Проектирование системы сквозного шифрования для мессенджера»
Необходимо спроектировать архитектуру безопасного хранения истории переписок в облаке. Требования: сообщения должны быть нечитаемы для облачного провайдера; у пользователей Алисы и Боба должен быть к ним доступ.

Требуется:

1. Опишите **последовательность действий** при установке сеанса связи между Алисой и Бобом с использованием асимметричной криптографии (например, алгоритм Диффи-Хеллмана или RSA).
2. Объясните, какой ключ (сеансовый, открытый, закрытый) и где должен храниться: на устройстве пользователя, в облаке.
3. Нарисуйте **схему** обмена и шифрования сообщения «Привет!» от Алисы к Бобу, начиная с генерации ключей.
4. Предложите способ **резервного копирования** ключей пользователя, чтобы он мог восстановить историю на новом устройстве, но чтобы резервная копия также была защищена. Опишите компромисс между безопасностью и удобством.

Задание 4. «Внедрение Transparent Data Encryption (TDE)»
Вас просят оценить внедрение TDE для базы данных, содержащей персональные данные 1 млн клиентов.

Исходные данные:

- **Без TDE:** Скорость записи = 5000 операций в секунду.
- **Алгоритм:** AES-256.
- **Накладные расходы на шифрование/дешифрование:** ~5% от времени операции ввода-вывода.

- **Требования регулятора:** Шифрование «неактивных» данных (data at rest) обязательно.

Требуется:

1. Рассчитайте **ожидаемую производительность** (операций в секунду) после включения TDE.
2. Составьте **чек-лист из 5 ключевых шагов** для развертывания TDE в промышленной среде (включая этапы: создание мастер-ключа, сертификата, резервное копирование ключей).
3. Опишите **процедуру восстановления** зашифрованной базы данных на другом сервере в случае аварии. Какие компоненты (файлы БД, ключи, сертификаты) необходимо перенести?
4. Проанализируйте **ограничения TDE**: данные в какой момент становятся незашифрованными? Как защитить данные «в движении» (data in motion) и «в использовании» (data in use)?

Блок 3: Планирование аварийного восстановления и аудита

Задание 5. «Разработка плана аварийного восстановления (Disaster Recovery Plan)»
Для интернет-банка критически важна БД транзакций. Технические характеристики:

- Объем БД: 2 ТБ.
- Допустимая потеря данных (RPO): не более 5 минут.
- Допустимое время простоя (RTO): не более 1 часа.
- Пиковая нагрузка: 1000 транзакций в секунду.

Требуется:

1. Выберите и обоснуйте **стратегию резервного копирования** (Full+Incremental/Differential, постоянное реплицирование). Рассчитайте требуемую пропускную способность канала для репликации.
2. Предложите **архитектуру** размещения основного и резервного ЦОД. Нарисуйте схему репликации данных.
3. Рассчитайте **стоимость хранения** резервных копий за год, если используется: а) Локальные диски (стоимость $50/ТБ); б) Облачное холодное хранилище ($10/ТБ/год). Учтите, что нужно хранить полные копии за последние 30 дней и инкрементальные за 7 дней.
4. Напишите **пошаговый runbook** (инструкцию) для операции переключения (failover) на резервный ЦОД. Включите шаги: проверка целостности резервной копии, переключение DNS, оповещение персонала, тестирование функциональности.

Задание 6. «Настройка и анализ журналов аудита (Audit Logs)»
В СУБД есть подозрение на утечку данных через привилегированного пользователя.

Требуется:

1. Напишите **конфигурацию аудита** (на примере PostgreSQL pgAudit или аналога), которая будет логировать:

- Все неудачные попытки входа (FAILED_LOGIN).
- Все операции SELECT и UPDATE с таблицей clients.
- Все действия пользователя с ролью admin.

2. Смоделируйте **набор подозрительных событий** за день и запишите их в виде строк лога (формат: timestamp, user, action, object, result).
3. Напишите **SQL-запрос** для анализа логов, который выявит:

- Попытки подбора пароля с одного IP-адреса (>10 попыток за 5 минут).
- Пользователя, который выполнил аномально большое количество `SELECT` в нерабочее время.

4. Предложите **механизм защиты журналов аудита** от модификации или удаления злоумышленником. Где их следует хранить?

Блок 4: Комплексный кейс

Задание 7. «Комплаенс и защита данных в медицинской информационной системе (МИС)»
Клиника внедряет МИС. Данные: история болезней, диагнозы, назначения (относятся к персональным данным и врачебной тайне). Регуляторные требования: ФЗ-152 (О персональных данных), HIPAA (если международный стандарт).

Требуется:

1. Создайте **матрицу соответствия (compliance matrix)**: в столбцах — требования стандартов (например, «аудит доступа», «шифрование при передаче»), в строках — технические и организационные меры, которые вы предложите для их выполнения.
2. Разработайте **схему псевдонимизации** данных пациентов для использования в тестовых средах разработчиками. Как обеспечить обратимость псевдонимизации для лечащего врача?
3. Рассчитайте **потенциальные штрафы** за утечку данных 1000 записей по ФЗ-152. Сравните со стоимостью внедрения предлагаемых вами мер защиты за 3 года (оценка «от» и «до»).
4. Проведите **тренинг для сотрудников** клиники. Составьте раздаточный материал (памятку) на 1 страницу с 5 основными правилами информационной безопасности для врачей и регистраторов.

Критерии оценки:

- **Блок 1 (Анализ и политики):** Оценивается глубина анализа рисков, корректность построения матрицы доступа, практическая применимость разработанных политик.
- **Блок 2 (Криптография):** Оценивается понимание принципов работы криптографических протоколов, умение проектировать безопасные архитектуры, точность расчетов производительности.
- **Блок 3 (Восстановление и аудит):** Оценивается реалистичность плана DRP, техническая грамотность настройки аудита, способность писать аналитические запросы к логам.
- **Блок 4 (Комплексный кейс):** Оценивается системный подход к compliance, умение балансировать между безопасностью, удобством и стоимостью, навык донесения сложных тем до неспециалистов.
- **Общее:** Структурированность ответов, использование профессиональной терминологии, наличие схем и расчетов, творческий подход к решению нестандартных задач.

4.2 Контрольные задания для промежуточной аттестации

Вопросы для экзамена

1. Дайте определение базы данных и СУБД. Каковы их основные функции и преимущества перед файловым хранением?
2. Опишите трёхуровневую архитектуру ANSI/SPARC. Каково назначение каждого уровня (внешнего, концептуального, внутреннего)?
3. Что такое модель данных? Сравните иерархическую, сетевую и реляционную модели.
4. Объясните основные понятия реляционной модели: отношение (таблица), атрибут (столбец), кортеж (строка), домен, ключ (первичный, внешний).
5. Опишите процесс нормализации баз данных. Каковы цели нормализации и проблемы ненормализованных отношений (аномалии)?
6. Что такое ER-диаграмма (Entity-Relationship)? Объясните сущности, атрибуты, связи (1:1, 1:M, M:N) и их графическое обозначение.
7. Сформулируйте основные правила целостности данных в реляционной модели: целостность сущностей и ссылочную целостность.
8. Что такое денормализация? В каких ситуациях она оправдана и каковы её риски?

9. Что такое SQL? На какие группы делятся операторы SQL (DDL, DML, DCL, TCL)? Приведите примеры команд для каждой группы.
10. Объясните разницу между операторами DELETE, TRUNCATE и DROP TABLE.
11. Что такое представление (VIEW)? Каковы его преимущества и ограничения (в контексте обновления данных через представление)?
12. Опишите назначение и принцип работы индексов в БД. Какие типы индексов вы знаете (B-дерево, хэш, полнотекстовый)?
13. Что такое транзакция в контексте БД? Сформулируйте и объясните свойства транзакций ACID.
14. Опишите проблему параллельного доступа к данным. Что такое «грязное» чтение, неповторяющееся чтение и фантомное чтение?
15. Что такое уровни изоляции транзакций? Опишите стандартные уровни (Read Uncommitted, Read Committed, Repeatable Read, Serializable) и решаемые ими проблемы.
16. Объясните назначение и использование оператора JOIN. В чём разница между INNER JOIN, LEFT/RIGHT OUTER JOIN и CROSS JOIN?
17. Что такое агрегатные функции в SQL? Приведите примеры использования COUNT, SUM, AVG, MIN, MAX вместе с оператором GROUP BY.
18. Объясните разницу между подзапросами (подселектами) и операциями соединения (JOIN). В каких случаях предпочтительнее каждый из подходов?

19. Каковы основные задачи администратора базы данных (DBA)? Разделите их на технические и эксплуатационные.
20. Что такое план выполнения запроса (execution plan)? Как администратор может использовать его для оптимизации производительности?
21. Опишите основные принципы и стратегии резервного копирования БД: полное, инкрементальное, дифференциальное копирование.
22. Что такое журнал транзакций (transaction log)? Какова его роль в обеспечении отказоустойчивости и восстановлении базы данных?
23. Объясните процесс восстановления базы данных после сбоя. В чём разница между восстановлением на момент времени (Point-in-Time Recovery) и восстановлением из резервной копии?

24. Что такое мониторинг производительности БД? Какие ключевые метрики (процессор, память, дисковый ввод-вывод, блокировки) необходимо отслеживать?
25. Опишите методы управления пользователями и правами доступа в СУБД. Что такое ролевая модель (RBAC) и как она упрощает администрирование?
26. Что такое миграция и обновление БД? Какие основные риски связаны с этим процессом и как их минимизировать?

27. Сформулируйте триаду информационной безопасности (CIA) применительно к базам данных. Дайте краткое пояснение каждому компоненту.
28. Объясните разницу между аутентификацией и авторизацией в контексте доступа к СУБД.
29. Что такое контроль доступа? Сравните дискреционный (DAC) и мандатный (MAC) механизмы управления доступом.
30. Опишите основные угрозы безопасности баз данных (SQL-инъекции, несанкционированный доступ, внутренние угрозы, DDoS).
31. Что такое SQL-инъекция (SQL Injection)? Объясните принцип атаки и основные методы защиты (параметризованные запросы, stored procedures, input validation).
32. Для чего предназначено аудирование (auditing) в БД? Какие события следует обязательно регистрировать в журналах аудита?
33. Опишите методы шифрования данных в БД. В чём разница между шифрованием на уровне столбцов, прозрачным шифрованием данных (TDE) и шифрованием на уровне приложения?
34. Что такое маскирование (обфускация) данных? В каких сценариях оно применяется (например, в тестовых средах)?
35. Объясните концепцию «безопасность по умолчанию» (security by default) и «принцип наименьших привилегий» (least privilege) применительно к настройке СУБД.
36. Каковы основные требования стандартов безопасности (например, PCI DSS, GDPR) к хранению и обработке персональных данных в базах данных?

37. Что такое обработка запросов в СУБД? Опишите основные этапы: парсинг, оптимизация, выполнение.
38. Какие факторы влияют на производительность запросов? Опишите роль индексов, статистики, фрагментации и аппаратных ресурсов.
39. Что такое блокировки (locks) в СУБД? Опишите разницу между пессимистичными и оптимистичными блокировками.
40. Что такое тупик (deadlock) в многопользовательской среде? Опишите классический пример «обедающих философов» и способы предотвращения или обнаружения взаимных блокировок.

Критерии оценки

Оценка «5» - (отлично)

При ответе материал изложен грамотным языком в определенной логической последовательности, точно использована терминология, полно раскрыто содержание материала в объеме, предусмотренном программой, продемонстрировано усвоение ранее изученных сопутствующих вопросов. Возможны одна - две неточности при освещении второстепенных вопросов.

Оценка «4» - (хорошо)

Ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы; допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, легко исправленные по замечанию преподавателя.

Оценка «3» - (удовлетворительно)

При ответе неполно или непоследовательно раскрыто содержание материала, но показано общее понимание, имелись затруднения или допущены ошибки в определении понятий.

Оценка «2» - (неудовлетворительно)

При ответе не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, допущены существенные ошибки, показавшие, что обучающийся не владеет обязательными умениями по данной теме в полной мере.