

**ПРИЛОЖЕНИЕ А**  
**ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**  
**ПО ДИСЦИПЛИНЕ «Информационная безопасность баз данных»**

**1. Перечень оценочных средств для компетенций, формируемых в результате освоения дисциплины**

<b>Код контролируемой компетенции</b>	<b>Способ оценивания</b>	<b>Оценочное средство</b>
ПК-8: Способен обеспечивать информационную безопасность уровня баз данных	Зачет	Комплект контролирующих материалов для зачета

**2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания**

Оцениваемые компетенции представлены в разделе «Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций» рабочей программы дисциплины «Информационная безопасность баз данных».

При оценивании сформированности компетенций по дисциплине «Информационная безопасность баз данных» используется 100-балльная шкала.

<b>Критерий</b>	<b>Оценка по 100-балльной шкале</b>	<b>Оценка по традиционной шкале</b>
Студент освоил изучаемый материал, выполняет задания в соответствии с индикаторами достижения компетенций, может допускать отдельные ошибки.	25-100	<i>Зачтено</i>
Студент не освоил основное содержание изученного материала, задания в соответствии с индикаторами достижения компетенций не выполнены или выполнены неверно.	0-24	<i>Не зачтено</i>

**3. Типовые контрольные задания или иные материалы, необходимые для оценки уровня достижения компетенций в соответствии с индикаторами**

*1. Задания на выбор автоматизированного средства контроля состояния баз данных*

<b>Компетенция</b>	<b>Индикатор достижения компетенции</b>
ПК-8 Способен обеспечивать информационную безопасность уровня баз данных	ПК-8.1 Выбирает автоматизированные средства контроля состояния баз данных

Предлагается следующая задача профессиональной деятельности: на сервере под управлением ОС Debian установлен сервер СУБД MySQL 5.7. На нем развернута база данных example\_db, с хранением данных в таблицах типа InnoDB. Настроены 3 пользователя – root, web\_prod, web\_dev.

Задание 1.

Выбрать автоматизированное средство контроля состояния указанной базы данных для обнаружения SQL-инъекций при запросах со стороны сервера веб-приложения, использующего указанную базу данных

Задание 2.

Выбрать автоматизированное средство контроля состояния указанной базы данных для обнаружения взаимных блокировок при выполнении транзакций в InnoDB-таблицах

Задание 3.

Выбрать автоматизированное средство контроля состояния указанной базы данных для обнаружения и обработки ошибок множественных соединений к базе данных

#### *2.Задания на выявление угроз безопасности уровня баз данных*

<b>Компетенция</b>	<b>Индикатор достижения компетенции</b>
ПК-8 Способен обеспечивать информационную безопасность уровня баз данных	ПК-8.2 Выявляет угрозы безопасности на уровне баз данных

Предлагается следующая задача профессиональной деятельности: на сервере под управлением ОС Debian установлен сервер СУБД MySQL 5. На нем настроены 3 пользователя – root, web\_prod, web\_dev

Задание 1.

Сформировать команду сканера безопасности nmap для выявления следующих угроз безопасности указанной базы данных: получение списка пользователей сервера MySQL с помощью атаки User enumeration

Задание 2.

Сформировать команду сканера безопасности nmap для выявления следующих угроз безопасности указанной базы данных: возможность обхода авторизации с неправильным паролем (CVE-2012-2122)

Задание 3.

Сформировать команду сетевого sniffера tcpdump для выявления следующих угроз безопасности СУБД: наличие вредоносного кода в потоках сетевых данных MySQL

Задание 4.

Сформировать команду MySQL для выявления следующих угроз безопасности СУБД: обнаружение обычных пользователей, имеющих повышенные привилегии, которые позволяют считывать произвольные файлы сервера

**4. Файл и/или БТЗ с полным комплектом оценочных материалов прилагается.**

