Севастопольский государственный университет
Кафедра «Информационные системы»

Управление данными

курс лекций

лектор:
ст. преподаватель кафедры ИС Абрамович А.Ю.

Лекция 7

Администрирование БД. Защита информации в базах данных

АДМИНИСТРИРОВАНИЕ БД

В номенклатуре специалистов, обеспечивающих проектирование, создание, эксплуатацию и использование АИС, соответственно, выделилась отдельная категория, называемая «администраторами систем (баз данных)», играющих ключевую роль в процессах информационного обеспечения деятельности предприятий и организаций.

Термин **«администрирование»** определяет комплекс процессов **при создании, эксплуатации и использовании АИС, связанных с обеспечением надежности и эффективности функционирования АИС, безопасности данных и организацией коллективной работы пользователей различных категорий.**

Комплекс процессов можно разделить по решаемым задачам на следующие группы:

ОБЕСПЕЧЕНИЕ И ПОДДЕРЖАНИЕ НАСТРОЙКИ СТРУКТУРНОГО, ИНТЕРФЕЙСНОГО И ТЕХНОЛОГИЧЕСКОГО КОМПОНЕНТОВ АИС НА СТРУКТУРУ И ПРОЦЕССЫ ПРЕДМЕТНОЙ ОБЛАСТИ СИСТЕМЫ

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ И СОХРАННОСТИ ДАННЫХ

ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ КОЛЛЕКТИВНОЙ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ С ОБЩИМИ ДАННЫМИ

ОБЕСПЕЧЕНИЕ И ПОДДЕРЖАНИЕ НАСТРОЙКИ СТРУКТУРНОГО, ИНТЕРФЕЙСНОГО И ТЕХНОЛОГИЧЕСКОГО КОМПОНЕНТОВ АИС НА СТРУКТУРУ И ПРОЦЕССЫ ПРЕДМЕТНОЙ ОБЛАСТИ СИСТЕМЫ

Участие администратора системы в этапах проектирования и ввода АИС в эксплуатацию: **администратор выступает экспертом в команде разработчиков по выбору СУБД и ее особенностям в плане реализации тех или иных компонент концептуальной схемы создаваемого банка данных, участвует в процессах создания типовых запросов, экранных форм для ввода и вывода данных, шаблонов отчетов**. На этапе проектирования и в процессе дальнейшей эксплуатации при наполнении системы данными **администратор системы производит анализ адекватности и эффективности спроектированной внутренней схемы базы данных и при необходимости может осуществлять ее корректировку**.

В эту же группу функций входит **создание и поддержание словарно-классификационной базы** (словари, справочники, ключевые слова, тезаурусы), **которая должна адекватно отражать особенности предметной области информационной системы**.

ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ И СОХРАННОСТИ ДАННЫХ

Обеспечение надежности и сохранности данных **является одной из главных обязанностей администратора АИС** и включает, в свою очередь, решение ряда **следующих технологических и профилактических задач**:

- планирование, конфигурирование и поддержание системы использования устройств внешней памяти, на которых размещаются файлы данных;
- архивирование и резервирование данных;
- восстановление данных после сбоев и повреждений;
- проверка и поддержание целостности данных.

Проверка и поддержание целостности данных является также неотъемлемой функцией администраторов и **заключается в обеспечении настройки и функционирования защитных механизмов СУБД поддерживающих ограничения целостности данных и связей в конкретной базе данных**.

ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ КОЛЛЕКТИВНОЙ РАБОТЫ ПОЛЬЗОВАТЕЛЕЙ С ОБЩИМИ ДАННЫМИ

Исходя из особенностей технологических процессов в предметной области и круга решаемых задач, **определяются функциональные группы работников, отвечающих за ввод, обработку и использование общих данных системы**. На этой основе строится перечень и схема пользователей системы, определяются их конкретные функции, полномочия, разрабатываются необходимые технологические и интерфейсные элементы, прорабатываются и устанавливаются внутренние параметры и характеристики коллективной обработки данных. **Администратор АИС, по сути, является как раз организатором и руководителем этих технологических процессов организации работы эксплуатационного персонала и абонентов-пользователей системы.**

Обязанностью администратора системы является создание и поддержание системы разграничения доступа к данным и защиты данных от несанкционированного доступа.

ЗАЩИТА БАЗЫ ДАННЫХ

Под **защитой базы данных** понимают обеспечение защищенности базы данных против любых предумышленных или непредумышленных угроз с **помощью различных компьютерных и некомпьютерных средств.**

Проблемы защиты баз данных:

ПОХИЩЕНИЕ И ФАЛЬСИФИКАЦИЯ ДАННЫХ	УТРАТА КОНФИДЕНЦИАЛЬНОСТИ (НАРУШЕНИЕ ТАЙНЫ)	ПОТЕРЯ ДОСТУПНОСТИ	НАРУШЕНИЕ НЕПРИКОСНОВЕННОСТИ ЛИЧНЫХ ДАННЫХ	УТРАТА ЦЕЛОСТНОСТИ
основное внимание должно быть сосредоточено **на сокращении общего количества удобных ситуаций для выполнения подобных действий**.	конфиденциальными считаются те данные, **которые являются критичными для всей организации.**	либо данные, либо система, одновременно окажутся **недоступными пользователям.**	следствием нарушения неприкосновенности личных данных будут **юридические меры, принятые в отношении организации.**	приводит **к искажению или разрушению данных**, что может иметь самые серьезные последствия для дальнейшей работы организации.

ТИПЫ УГРОЗ ДЛЯ БД

Под **угрозой** будем понимать любую ситуацию или событие, намеренное или непреднамеренное, которое **способно неблагоприятно повлиять на систему, а следовательно, и на всю организацию.**

Вред может быть **очевидным** (например, потеря оборудования, программного обеспечения или данных) или **неочевидным** (например, потеря доверия партнеров или клиентов).

Преднамеренные угрозы всегда осуществляются людьми и могут быть совершены как авторизированными, так и неавторизированными пользователями, причем последние могут не принадлежать организации.

*Любая опасность должна рассматриваться как **потенциальная возможность нарушения системы защиты**, которая в случае своей реализации может оказать то или иное негативное влияние. Хотя некоторые типы опасностей могут быть как намеренными, так и непреднамеренными, результаты в любом случае будут одинаковы.*

Любая организация должна установить типы возможных угроз, которым может подвергнуться ее система, после чего разработать соответствующие планы и требуемые контрмеры, с оценкой уровня затрат, необходимых для их реализации.

Неограниченные привилегии базы данных

Обычно это происходит, когда **пользователям базы данных предоставляются многочисленные привилегии в системе**, что приводит к злоупотреблению привилегиями, которое может быть чрезмерным, законным или неиспользуемым.

Существуют некоторые меры контроля, которые должны быть реализованы следующим образом:

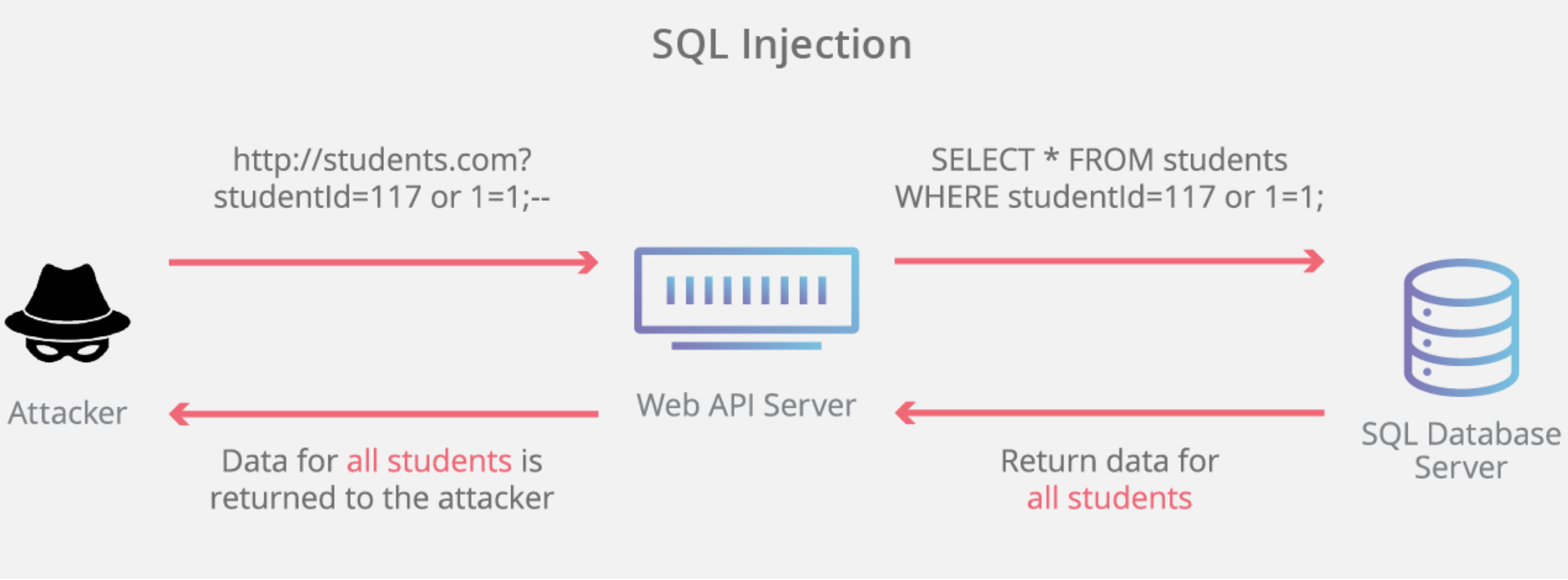
- необходимо приложить все усилия для внедрения **очень строгой политики контроля доступа и контроля привилегий**;
- **не предоставлять и не утверждать чрезмерные привилегии всем сотрудникам**, и выделить время для немедленной деактивации любых устаревших привилегий.

Внедрение SQL-кода (SQL-инъекции)

Этот тип атаки внедрения SQL-кода происходит, когда **вредоносный код внедряется через frontend и затем передается в backend.** **SQL-инъекция – это метод использования пользовательских данных через поле ввода веб-страниц.** Этот процесс позволяет злоумышленнику получить абсолютный доступ к информации, хранящейся в базе данных.

В ходе проведения такой атаки делается попытка модификация SQL-выражения, которое приложение отправляет базе данных. Выполняется атака путём подстановки особым образом подготовленных данных в поля ввода, которые может заполнять пользователь.

Целью обычно является кража данных или их повреждение. Внедрение SQL-кода нацелено на традиционные базы данных, а внедрение NoSQL кода - на базы BIG Data.



- злоумышленники могут использовать эту уязвимость **для извлечения учетных данных пользователей из базы данных.** После чего они могут выдавать себя за реальных пользователей и красть их деньги или данные.
- злоумышленники могут **получить права администратора в базе данных**, чтобы стереть, скопировать или повредить все данные на сервере;
- в некоторых случаях SQL-инъекция также позволяет злоумышленникам получить **доступ к операционной системе**. Это приводит к атаке на внутреннюю сеть бизнеса.

Плохой аудиторский след

Согласно некоторым стандартам безопасности, **каждое событие в базе данных должно быть записано для целей аудита.** Если нет возможности представить доказательства наличия журнала аудита базы данных, то это может представлять собой очень серьезный риск для безопасности, поскольку в случае вторжения невозможно будет провести «расследование».

Открытые резервные копии баз данных

Каждой организации необходим очень хороший план резервного копирования, но когда резервные копии доступны, они становятся открытыми для компрометации и кражи.

Шифрование и аудит производственных баз данных и резервных копий - лучшая форма защиты корпоративных конфиденциальных данных.

Неправильная конфигурация базы данных

Некоторые из угроз, встречающихся в базе данных, являются результатом их **неправильной конфигурации**. Злоумышленники обычно пользуются базой данных, которая имеет **стандартную учетную запись и настройки конфигурации**.

Это **тревожный сигнал, что при настройке базы данных не должно быть ничего похожего на учетную запись по умолчанию, а параметры должны быть настроены таким образом, чтобы злоумышленнику было сложно что-либо сделать.**

Плохое управление данными

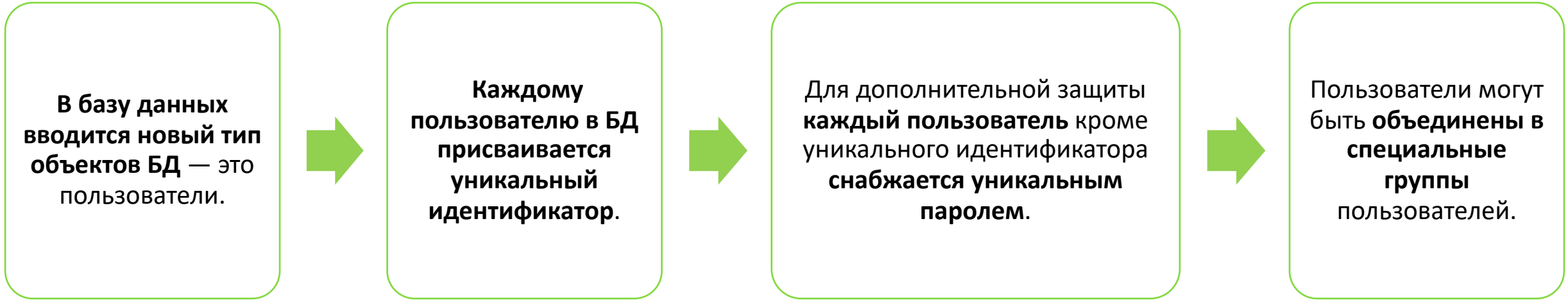
Если не провести надлежащую инвентаризацию новых данных, добавленных в базу, то они могут стать уязвимыми. **Поэтому очень важно шифровать данные в состоянии покоя и применять необходимые разрешения и средства контроля.**

ПОДХОДЫ К БЕЗОПАСНОСТИ ДАННЫХ

В современных СУБД поддерживается один из двух наиболее общих подходов к вопросу обеспечения безопасности данных: **избирательный подход и обязательный подход.** В обоих подходах **единицей данных или «объектом данных»,** для которых должна быть создана система безопасности, **может быть как вся база данных целиком, так и любой объект внутри базы данных.**

В случае **избирательного управления** некоторый пользователь обладает различными правами (привилегиями или полномочиями) при работе с данными объектами. Разные пользователи могут обладать разными правами доступа к одному и тому же объекту. **Избирательные права характеризуются значительной гибкостью.**

В случае **неизбирательного управления**, наоборот, каждому объекту данных присваивается некоторый классификационный уровень, а каждый пользователь обладает некоторым уровнем допуска. При таком подходе **доступом к определенному объекту данных обладают только пользователи с соответствующим уровнем допуска.**



Привилегии или полномочия пользователей или групп — это набор действий (операций), которые они могут выполнять над объектами БД.

В ряде коммерческих СУБД используется понятие «роли». **Роль — это поименованный набор полномочий.** Существует ряд стандартных ролей, которые определены в момент установки сервера баз данных. **И имеется возможность создавать новые роли, группируя в них произвольные полномочия.** Введение ролей позволяет **упростить управление привилегиями пользователей**, структурировать этот процесс. Кроме того, введение ролей не связано с конкретными пользователями, поэтому **роли могут быть определены и сконфигурированы до того, как определены пользователи системы**. Пользователю может быть назначена **одна или несколько ролей.**

КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БД

На самом элементарном уровне концепции обеспечения безопасности баз данных исключительно просты. Необходимо поддерживать два фундаментальных принципа: **проверку полномочий и проверку подлинности (аутентификацию).**

Проверка полномочий основана на том, что каждому пользователю или процессу информационной системы соответствует набор действий, которые он может выполнять по отношению к определенным объектам.

Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированное действие, действительно тот, за кого он себя выдает.

Система назначения полномочий имеет иерархический характер. Самыми высокими правами и полномочиями обладает системный администратор или администратор сервера БД.

СУБД В СВОИХ СИСТЕМНЫХ КАТАЛОГАХ ХРАНИТ КАК ОПИСАНИЕ САМИХ ПОЛЬЗОВАТЕЛЕЙ, ТАК И ОПИСАНИЕ ИХ ПРИВИЛЕГИЙ ПО ОТНОШЕНИЮ КО ВСЕМ ОБЪЕКТАМ.

Схема предоставления полномочий строится по следующему принципу. Каждый объект в БД имеет владельца — пользователя, который создал данный объект. Владелец объекта обладает всеми правами-полномочиями на данный объект, в том числе он имеет право предоставлять другим пользователям полномочия по работе с данным объектом или забирать у пользователей ранее предоставленные полномочия.

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ БАЗЫ ДАННЫХ

Зачем проводить тестирование безопасности базы данных?

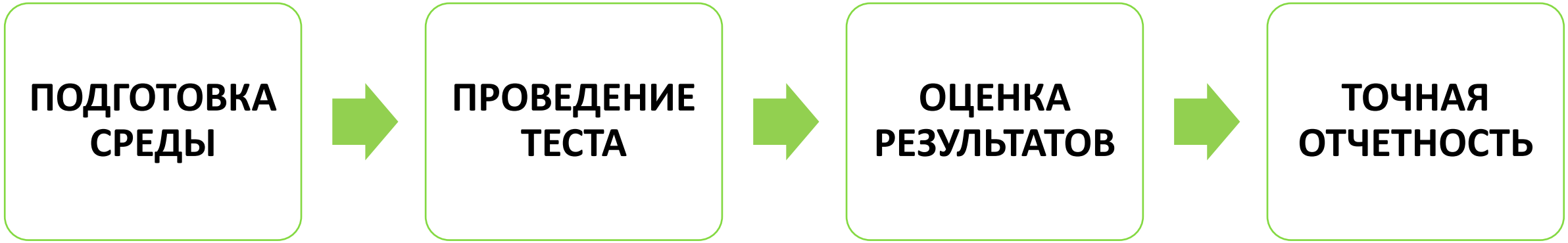
Этот тест проводится для обнаружения любых слабых мест или уязвимостей в конфигурации безопасности базы данных и для смягчения последствий любого нежелательного доступа к базе данных. **Все конфиденциальные данные должны быть защищены от злоумышленников, поэтому регулярные проверки безопасности очень важны и обязательны.**

Основные функции, по которым тестирование безопасности базы данных является обязательным:

- аутентификация;
- авторизация;
- учет;
- конфиденциальность;
- целостность;
- доступность;
- устойчивость.

Этот процесс включает в себя тестирование различных уровней на основе бизнес-требований. К тестируемым уровням относятся бизнес-уровень, уровень доступа и уровень пользовательского интерфейса.

ПРОЦЕСС ТЕСТИРОВАНИЯ БАЗЫ ДАННЫХ



Техники тестирования безопасности баз данных

- **тест на проникновение:** Это процесс имитации атаки на сеть, компьютерную систему или веб-приложение для обнаружения в них любых уязвимостей.
- **сканер уязвимостей:** Это использование сканера для сканирования системы на наличие известных уязвимостей с целью их устранения и исправления.
- **аудит безопасности:** Это процесс оценки реализации и соответствия политик и стандартов безопасности организации.
- **оценка рисков:** Это общий процесс выявления всех опасностей и рисков, способных нанести серьезный вред системе.