

Подсистема аудита информационной системы, использующей СУБД PostgreSQL

Дипломант: Горяйнов Дмитрий Андреевич, гр. 7361

ФКТИ, АСОИУ, Компьютерная безопасность

Руководитель: к.т.н. Зорин Кирилл Михайлович

Цели и задачи

- Цель: разработать программное решение аудита, повышающее безопасность информационной системы
- Задачи
 - Анализ информационной безопасности, аудита информационной безопасности информационных систем и систем управления БД
 - Разработка и анализ архитектуры, компонентов подсистемы и средств, используемых для этого
 - Разработка подсистемы аудита информационной системы, использующей СУБД PostgreSQL
 - Составление экономического обоснования
 - Раздел, посвященный защите интеллектуальной собственности.

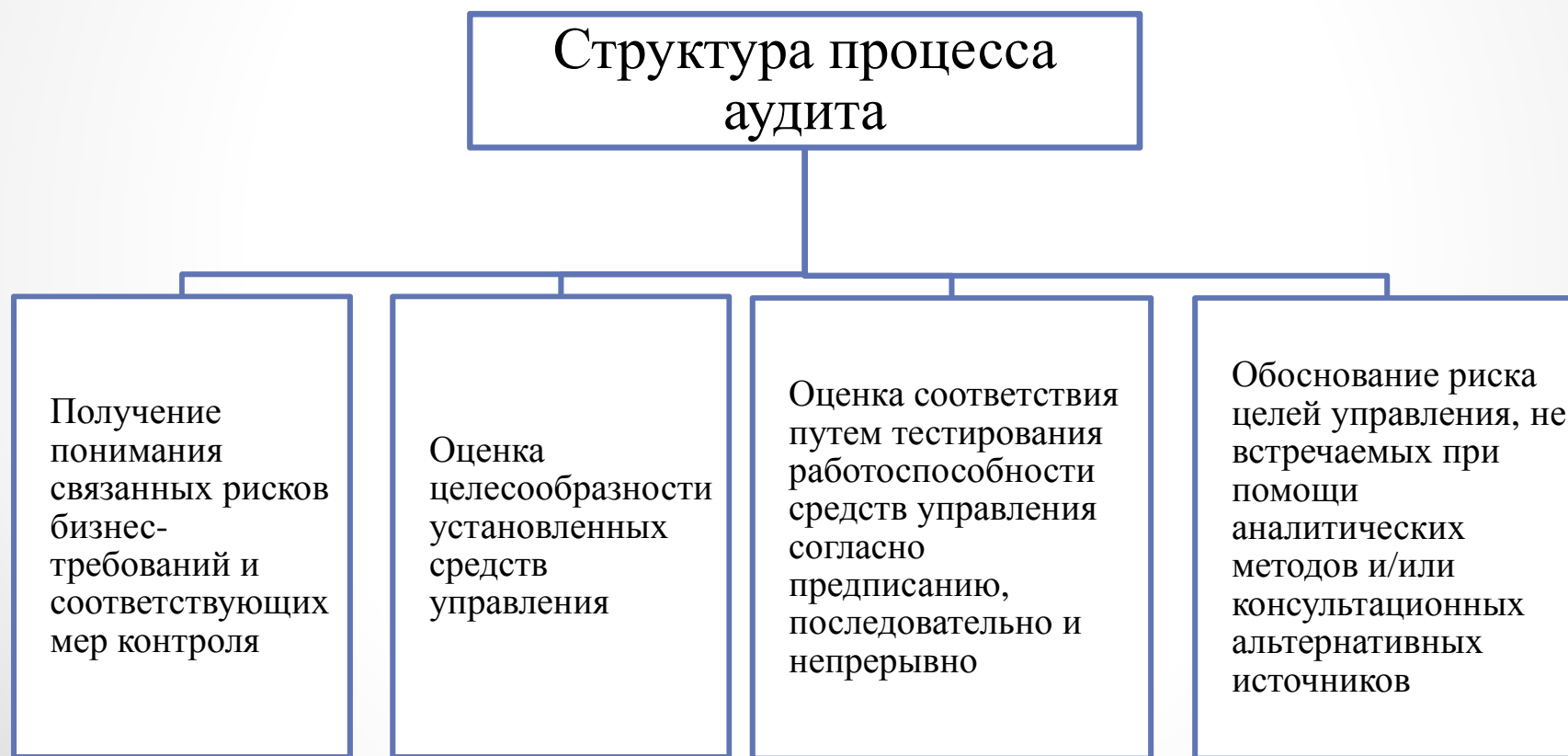
Информационная безопасность и аудит

- Информационная безопасность — это защищенность информации и инфраструктуры, которая ее поддерживает, от преднамеренных или случайных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации
- Аудит — в общем случае, проверка соответствия некоторого объекта оценки определенным требованиям. В области защиты информации употребляется термин «аудит информационной безопасности»

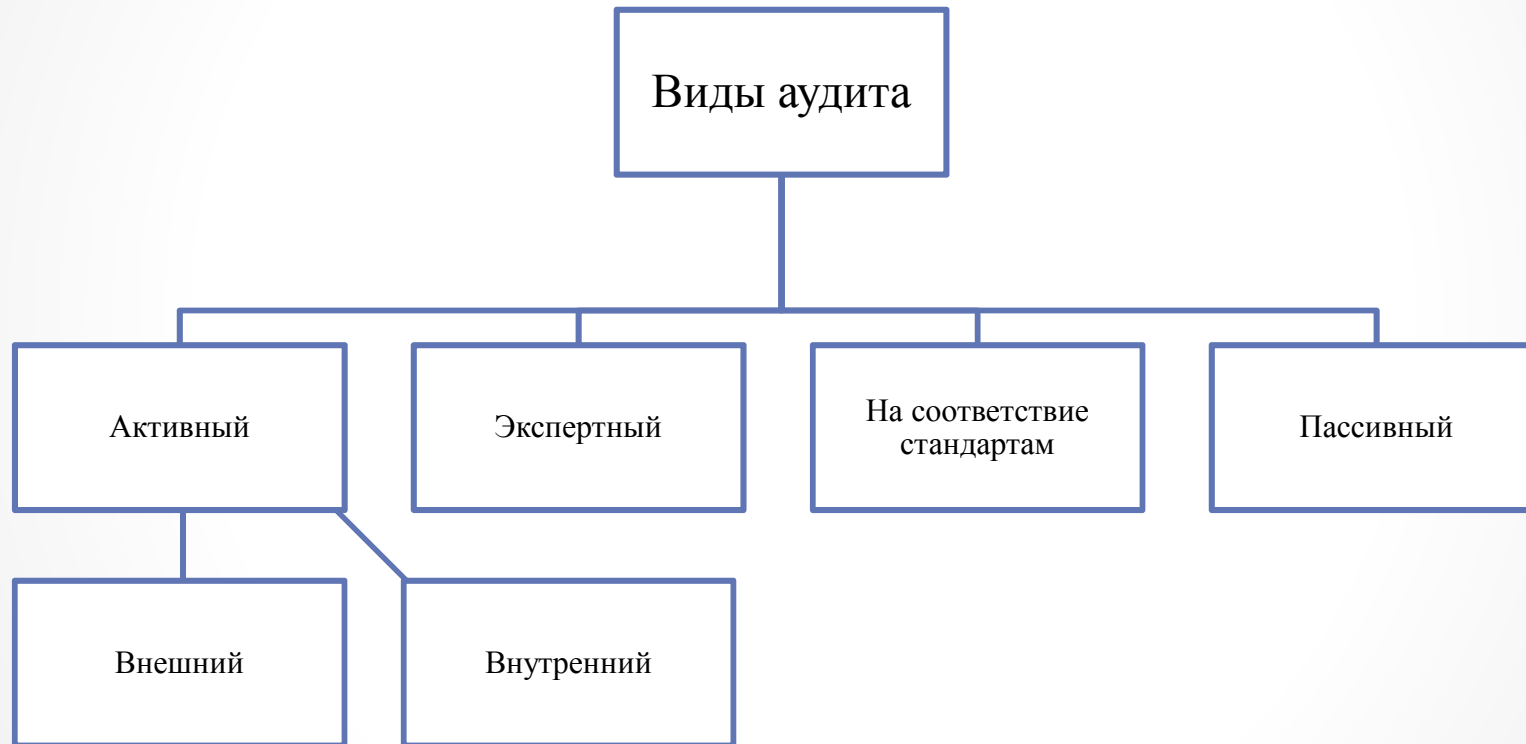
Механизмы обеспечения безопасности информационных систем

- Идентификация и аутентификация
- Криптография и шифрование
- Методы разграничение доступа
- Регистрация и аудит

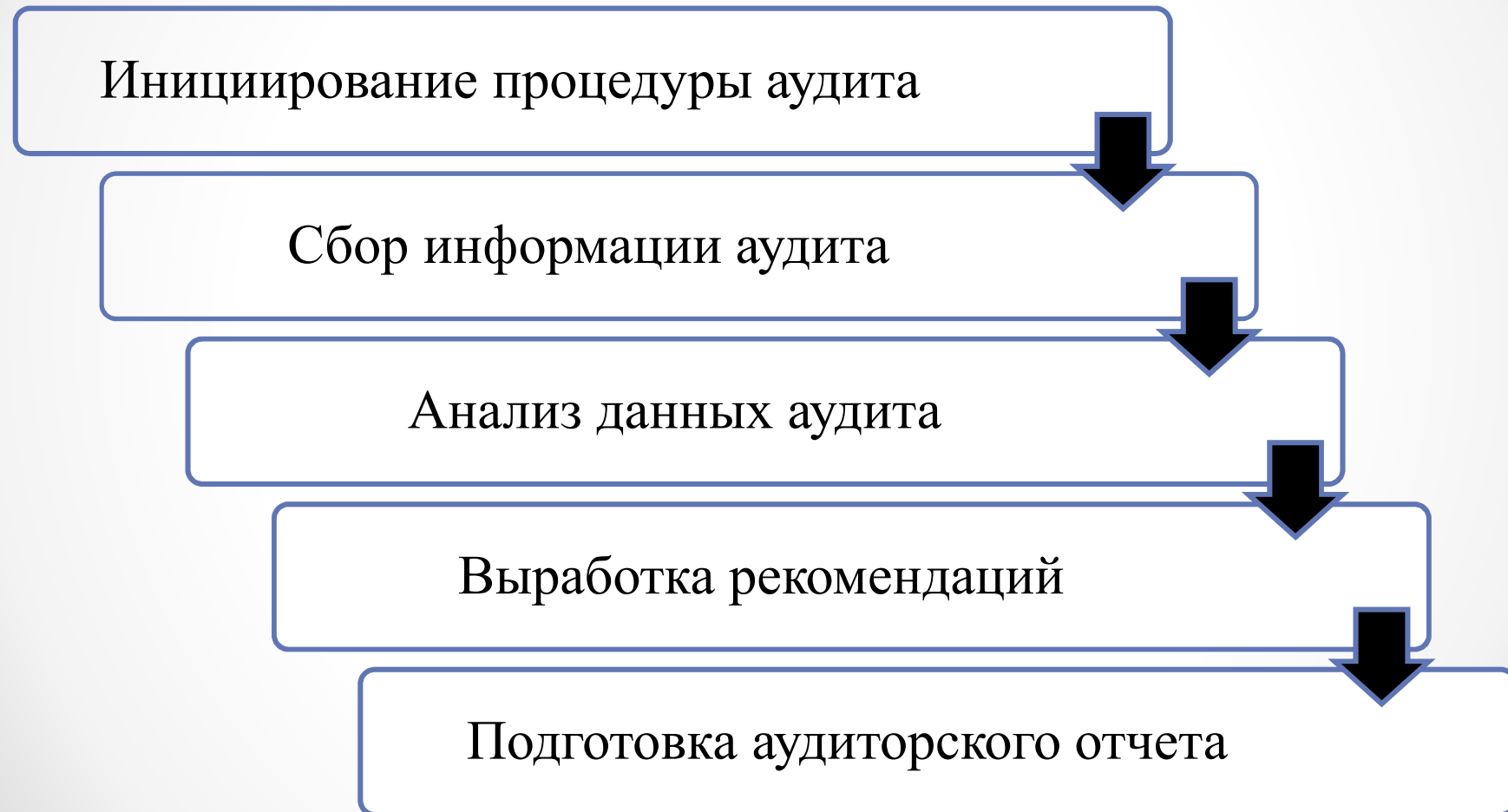
Аудит информационной безопасности



Виды аудита информационной безопасности



Этапность работ по аудиту



Информационная безопасность в СУБД

Общие подходы к
вопросу обеспечения
безопасности данных
в СУБД

Избирательный

Обязательный

Аудит систем управления базами данных

- Задачи аудита

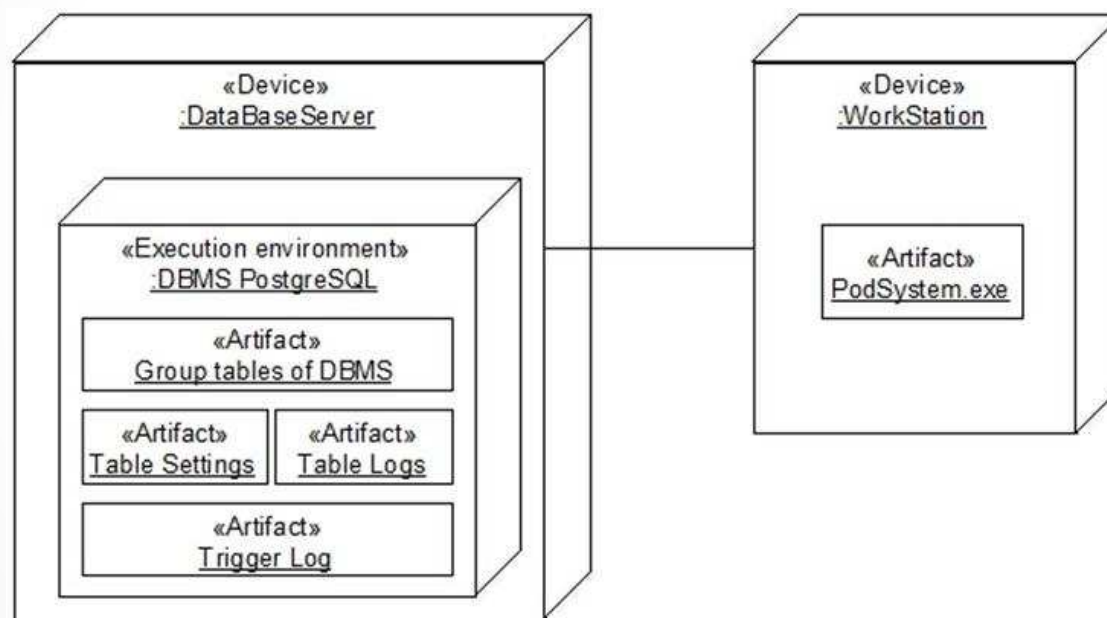


Аудит различных систем управления базами данных

- Существует возможность использовать стандартные средства аудита таких СУБД как: Oracle, MS SQL Server, т.д.
- Также есть несколько вариантов решения задач аудита:
 - CT (Change Tracking)
 - CDC (Change Data Capture)
 - SQL Server Audit

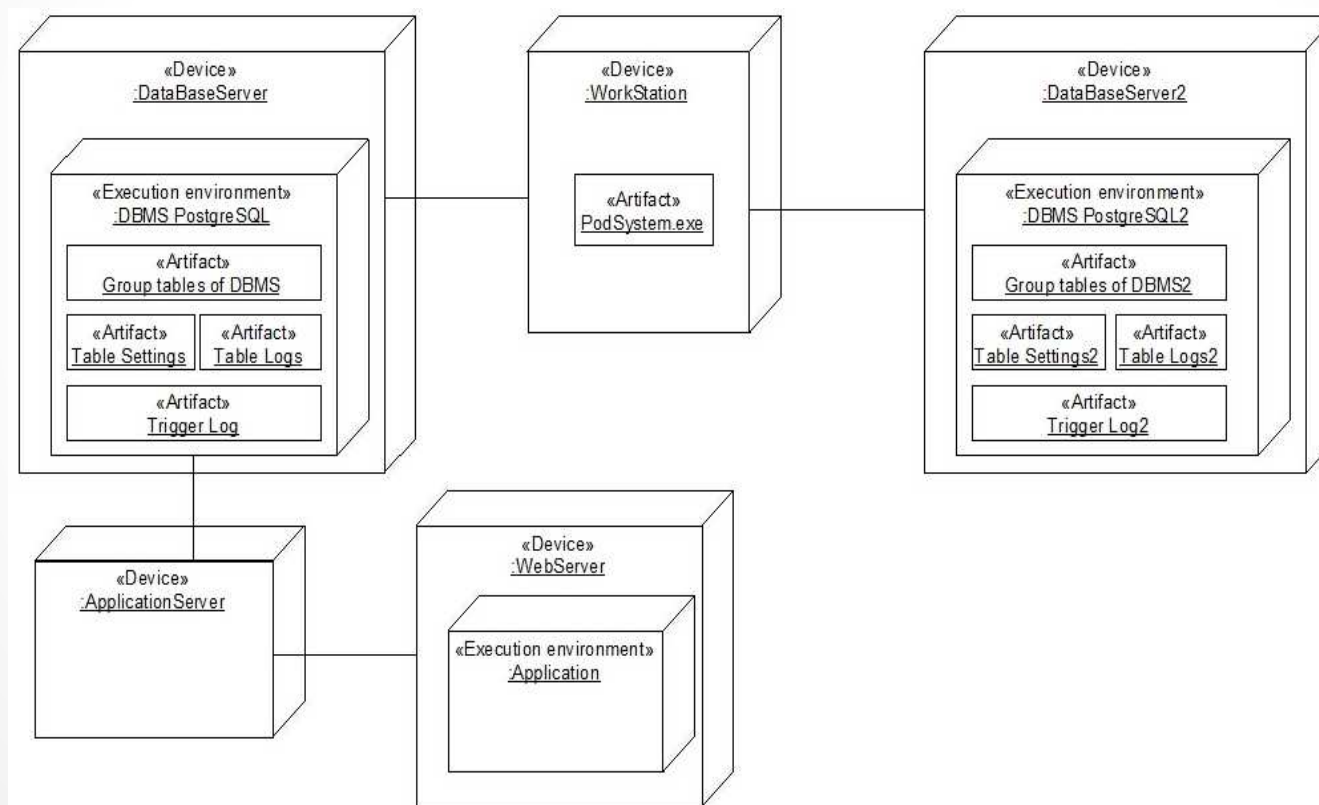
Разработка подсистемы аудита системы управления базой данных

- Диаграмма развертывания



Разработка подсистемы аудита системы управления базой данных

- Возможное расширение функциональности подсистемы



Структура подсистемы

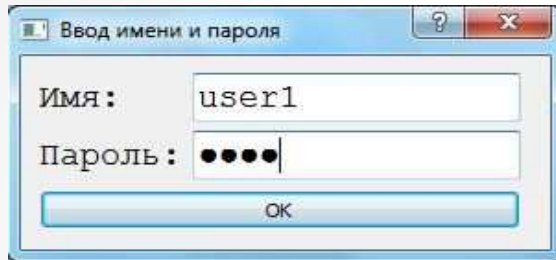
- **Используемые таблицы в базе данных**

Таблица logs	Таблица settings
text	table_name
added	
username	pole_name
tablename	

- **Используемые SQL-запросы (наиболее важные)**
- **1)** SELECT attname FROM pg_attribute, pg_type WHERE typname = 'jilci' AND attrelid = typrelid AND attname NOT IN ('cmin', 'cmax', 'ctid', 'oid', 'tableoid', 'xmin', 'xmax')
- **2)** SELECT tablename FROM pg_tables WHERE tablename NOT LIKE 'pg_%' AND tablename NOT LIKE 'sql_%' AND tablename NOT LIKE 'logs' AND tablename NOT LIKE 'settings'
- **3)** SELECT description from pg_description join pg_class on pg_description.objoid = pg_class.oid where relname = 'jilci' and objsubid = 5
- **4)** COMMENT ON COLUMN jilci.num IS 'Номер квартиры';
- **5)** DROP FUNCTION add_to_log_jilci () CASCADE
- **6)** CREATE TRIGGER log AFTER INSERT OR UPDATE OR DELETE ON jilci FOR EACH ROW EXECUTE PROCEDURE add_to_log_jilci ();

Подсистема аудита

- Запрос имени и пароля



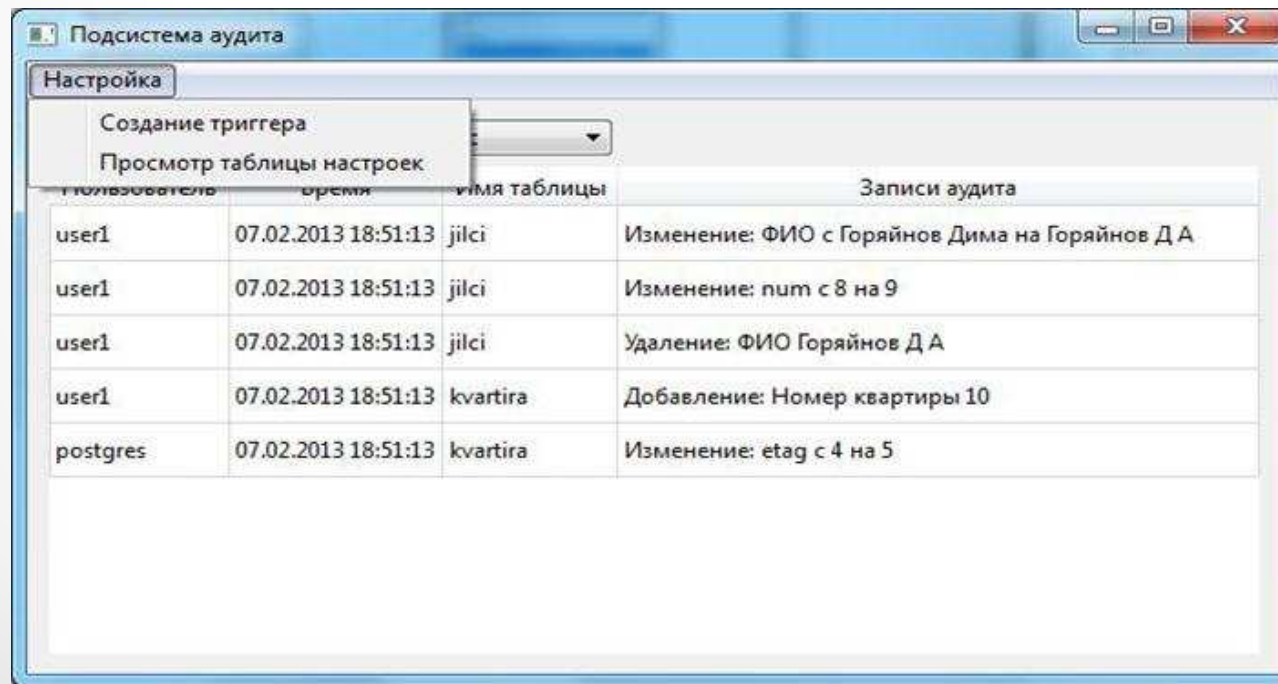
Ввод имени и пароля

Имя: user1

Пароль: ••••

OK

- Меню главного окна



Подсистема аудита

Настройка

- Создание триггера
- Просмотр таблицы настроек

Пользователь	Время	Имя таблицы	Записи аудита
user1	07.02.2013 18:51:13	jilci	Изменение: ФИО с Горяйнов Дима на Горяйнов Д А
user1	07.02.2013 18:51:13	jilci	Изменение: num с 8 на 9
user1	07.02.2013 18:51:13	jilci	Удаление: ФИО Горяйнов Д А
user1	07.02.2013 18:51:13	kvartira	Добавление: Номер квартиры 10
postgres	07.02.2013 18:51:13	kvartira	Изменение: etag с 4 на 5

Подсистема аудита

- Создание и генерация триггера

Создание триггера

Отслеживаемые операции: Выполнение для:

☐ Добавление ☐ Записи (row)
☐ Удаление ☐ Запроса (statement)
☐ Изменение

Выбор Таблицы:

nachis

Выбор полей:	Комментарии:
id_n	
data_n	
data_pog	
sum_n	
id_sp	

Создать триггер

Создание триггера

Отслеживаемые операции: Выполнение для:

☐ Добавление ☒ Записи (row)
☒ Удаление ☐ Запроса (statement)
☒ Изменение

Выбор Таблицы:

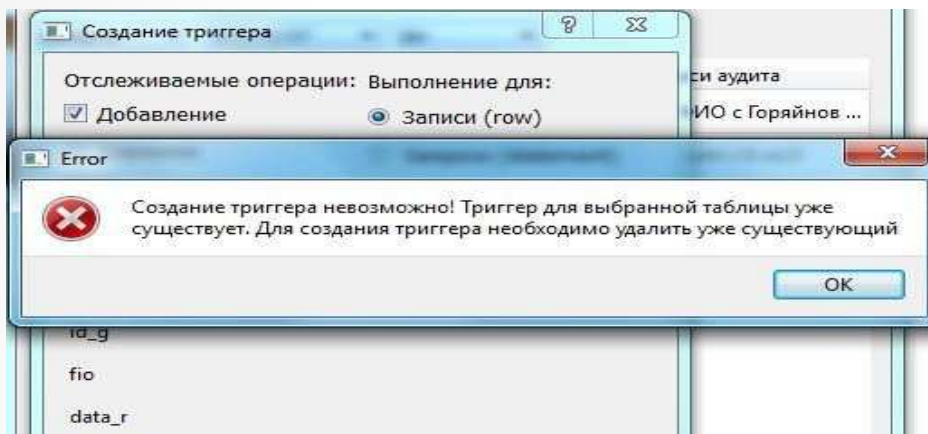
jilci

Выбор полей:	Комментарии:
id_g	
fio	ФИО
data_r	
data_reg	
num	Номер квартиры

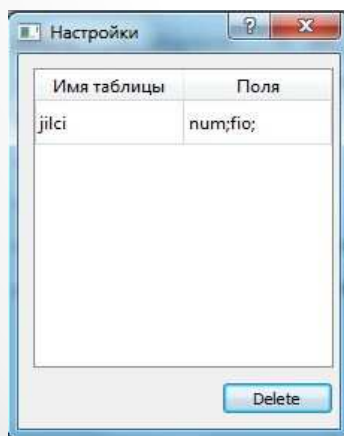
Создать триггер

Подсистема аудита

- Проверка на существование

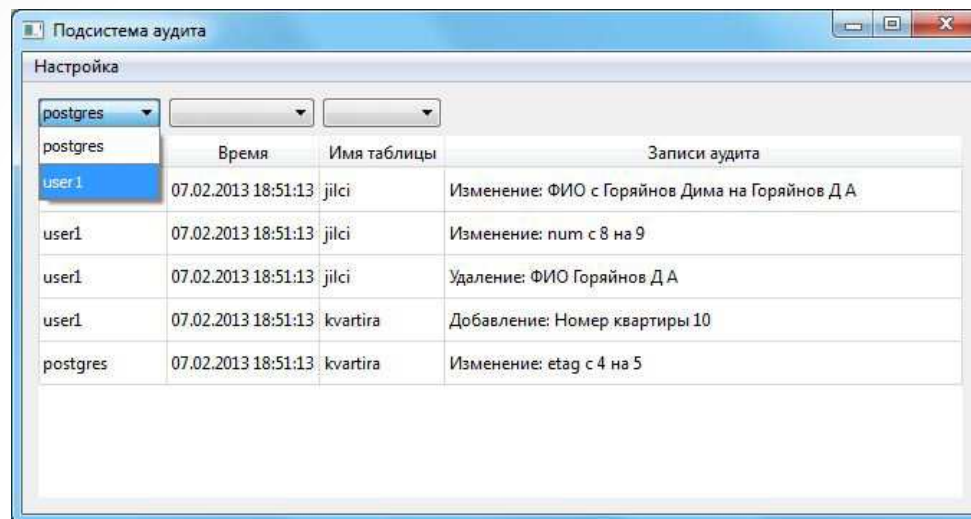


- Окно настроек



Подсистема аудита

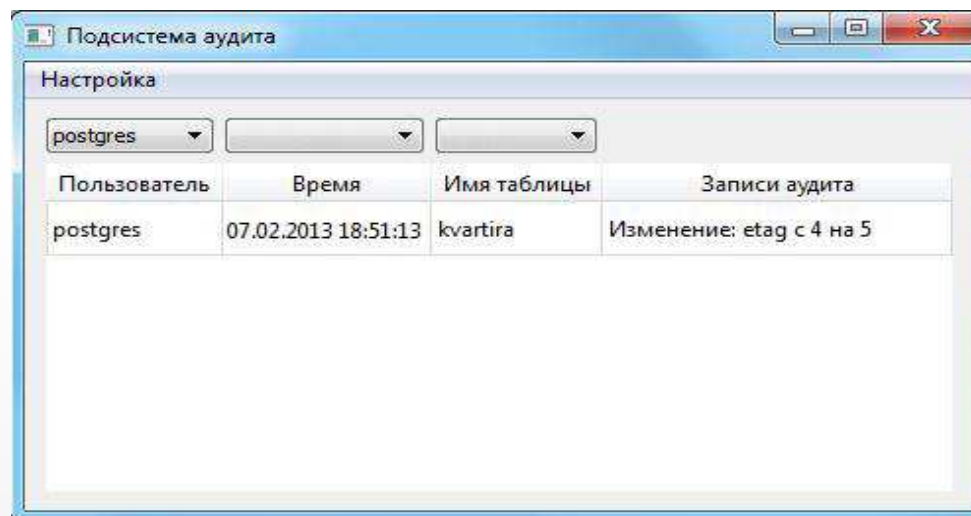
- Фильтры главное окна



Подсистема аудита

Настройка

postgres			
postgres	Время	Имя таблицы	Записи аудита
user1	07.02.2013 18:51:13	jilci	Изменение: ФИО с Горяйнов Дима на Горяйнов Д А
user1	07.02.2013 18:51:13	jilci	Изменение: num с 8 на 9
user1	07.02.2013 18:51:13	jilci	Удаление: ФИО Горяйнов Д А
user1	07.02.2013 18:51:13	kvirtira	Добавление: Номер квартиры 10
postgres	07.02.2013 18:51:13	kvirtira	Изменение: etag с 4 на 5



Подсистема аудита

Настройка

postgres			
Пользователь	Время	Имя таблицы	Записи аудита
postgres	07.02.2013 18:51:13	kvirtira	Изменение: etag с 4 на 5

Экономическая оценка

- Трудоемкость составляет 92 чел/дни
- Себестоимость НТПр составляет 213685 руб
- Уровень качества составляет 1,55
- Основным преимуществом данного НТПр является эффективное выявление причин, способствующих повышению защищенности информации

Защита интеллектуальной собственности

- Комплект документов для получения патента;
- Лицензионный договор

Форма РП	
№ Входящий	№ Регистрационный
от _____ г.	от _____ г.
В ФЕДЕРАЛЬНЫЙ ОРГАН ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ Бережовская наб., 30, корп. 1, Москва, Г-59, ГСП-5, 123995	
ЗАЯВЛЕНИЕ НА ГОСУДАРСТВЕННУЮ РЕГИСТРАЦИЮ	
<input checked="" type="checkbox"/> ПРОГРАММЫ ДЛЯ ЭВМ или <input type="checkbox"/> БАЗЫ ДАННЫХ (отметить [X])	
Представляя указанные ниже документы, подтверждаю (ем) отсутствие сведений, составляющих государственную тайну, и прошу (проси) зарегистрировать программу для ЭВМ (базу данных)	
1. ПРАВООБЛАДАТЕЛЬ (ЗАЯВИТЕЛЬ(И)) ОГРН: _____ (для правообладателя, юридического лица)	
Горяинов Дмитрий Андреевич	
Указанное лицо является: <input type="checkbox"/> государственным заказчиком; <input type="checkbox"/> муниципальным заказчиком; <input type="checkbox"/> исполнителем работ по <input type="checkbox"/> государственному контракту <input type="checkbox"/> муниципальному контракту	
заказчик работ _____ (наименование заказчика)	
контракт от _____ № _____	
(Указывается полностью или наименование заявителя(ов) и его (их) место жительства или место нахождения, включая указание страны. Данные о местожительстве автора(ов)-заявителя(ов) приводятся в графе 9А) (Всего заявителей 1)	
2. ОСНОВАНИЯ ВОЗНИКНОВЕНИЯ ПРАВ НА РЕГИСТРИРУЕМУЮ ПРОГРАММУ ДЛЯ ЭВМ ИЛИ БАЗУ ДАННЫХ (отметить [X]) (заполняется, если заявитель является юридическим лицом, или сетью заявителей не соответствует сетью авторов) <input type="checkbox"/> заявитель является работодателем автора <input type="checkbox"/> передача прав автором или его правопреемником заявителю <input type="checkbox"/> передача прав работодателем заявителю <input type="checkbox"/> право наследования <input type="checkbox"/>	
3. НАЗВАНИЕ РЕГИСТРИРУЕМОЙ ПРОГРАММЫ ДЛЯ ЭВМ ИЛИ БАЗЫ ДАННЫХ Подсистема аудита информационной системы	
3А. ПРЕДЫДУЩЕЕ ИЛИ АЛЬТЕРНАТИВНОЕ НАЗВАНИЕ (подчеркнуть) _____ нет	
4. НАЗВАНИЕ СОСТАВНОГО ПРОИЗВЕДЕНИЯ (если регистрируемая программа для ЭВМ или база данных является частью составного произведения) _____ нет	
5. СВЕДЕНИЯ О ПРЕДЫДУЩЕЙ РЕГИСТРАЦИИ Номер предыдущей регистрации _____ Дата предыдущей регистрации _____ число _____ месяц _____ год _____	
6. ДАТА СОЗДАНИЯ РЕГИСТРИРУЕМОЙ ПРОГРАММЫ ДЛЯ ЭВМ ИЛИ БАЗЫ ДАННЫХ (заполняется указав число, месяц, год создания регистрируемой программы для ЭВМ или базы данных) число 2 месяц 2013 год	
7. МЕСТО И ДАТА ПЕРВОГО ВЫПУСКА В СВЕТ РЕГИСТРИРУЕМОЙ ПРОГРАММЫ ДЛЯ ЭВМ ИЛИ БАЗЫ ДАННЫХ страна <u>Российская Федерация</u> 10 число 02 месяц 2013 год	
8. СВЕДЕНИЯ О ПРОИЗВЕДЕНИЯХ, ЯВЛЯЮЩИХСЯ ОБЪЕКТАМИ АВТОРСКОГО ПРАВА (заполняется, если заявитель регистрирует программы для ЭВМ или базы данных)	

Выводы:

- проведен детальный анализ информационной безопасности и аудита информационных систем
- разработаны и подробно описаны архитектура, компоненты разработанной подсистемы аудита и используемые для этого средства;
- разработка подсистемы осуществлена при помощи СУБД PostgreSQL, с помощью SQL запросов, которые были описаны, и инструментария QT

Проведение аудита при помощи дипломного проекта осуществляется должным образом, что в свою очередь поможет повысить информационную безопасность любой рассматриваемой системы и базы данных в этой системе.