Вступление

Уважаемый председатель, уважаемые члены Государственной Аттестационной Комиссии, уважаемые коллеги! Я - Горяйнов Дмитрий Андреевич. Разрешите представить на Ваше рассмотрение дипломную работу по теме «разработка подсистема аудита информационной системы, использующей СУБД PostgreSQL»

1 слайд

Необходимость разработки дипломного проекта и соответственно создание программного решения в рамках него обусловлено повышением требований к информационной безопасности и существенный рост рисков потерь от ее нарушения

---

2 слайд

Цель данной работы — на основе существующих моделей и средств для проведения аудита, разработать программное решение аудита, повышающее безопасность информационной системы

Задачи проекта следующие:

- Анализ информационной безопасности, аудита информационной безопасности информационных систем и систем управления БД
- Разработка и анализ архитектуры, компонентов подсистемы и средств, используемых для этого
- Разработка и проектирование подсистемы аудита информационной системы, использующей СУБД PostgreSQL
- Составление экономического обоснования
- Разработка раздела, посвященного защите интеллектуальной собственности

---

3 слайд

Так как в проекте производится разработка подсистемы аудита информационной безопасности, дадим несколько важных определений, представленных на этом слайде. Информационная безопасность — это защищенность информации и инфраструктуры, которая ее поддерживает. Аудит — проверка соответствия некоторого объекта оценки определенным требованиям.

---

4 слайд

Для обеспечения информационной безопасности существуют следующие механизмы: Идентификация. Аутентификация. Криптографические методы и шифрования. Методы разграничения доступа.

Регистрация и аудит является ещё одним механизмом обеспечения защищенности информационной системы. Данный механизм фиксирует все события, которые касаются безопасности, также он позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, оценивать работу пользователей. Аудит — это анализ накопленной информации, проводимый оперативно в реальном времени или периодически.

---

5 слайд

Рассмотрим для чего применяется аудит:

Получение понимания рисков, оценка целесообразности средств управления, оценка соответствия средств управления путем тестирования работы, обоснование риска.

---

6 слайд

После рассмотрения структуры аудита можно перейти к рассмотрению видов аудита.

Суть *активного аудита* состоит в том, что с помощью специального программного обеспечения и специальных методов осуществляется сбор информации о состоянии системы сетевой защиты. При «внешнем» активном аудите специалисты моделируют действия «внешнего» злоумышленника, при «внутреннем» моделируются действия «внутреннего» злоумышленника.

Экспертный аудит является сравнением идеального описания с состоянием информационной безопасности

Аудит на соответствие стандартом является сравнением некоторого описания, приводимым в стандартах с состоянием информационной безопасности.

Пассивный. Также стоит рассмотреть технологии пассивного аудита, которые собирают информацию об уязвимостях системы другими способами, которые в отличие от активного аудита не предполагают большой нагрузки и выполнения сложных запросов. Основная функция - выявление нарушений безопасности, путем анализа данных журналов аудита администратором безопасности в фоновом режиме. Данный вид аудита и представлен в дипломном проекте.

---

7 слайд

Далее рассмотрим этапы, по которым проводятся работы по аудиту безопасности ИС. Такие этапы как инициирование процедуры аудита и сбор информации аудита являются фундаментом для выполнения целей дипломного проекта и не зависят от спецификации системы, в которой проводится аудит, в отличие от трех остальных этапов.

---

8 слайд

На этом слайде представлены два основных подхода к обеспечению безопасности в СУБД.

- В случае избирательного подхода 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, 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.

---

9 слайд

Обозначим несколько задач, которые должен решать аудит.

Аудит доступа к базе данных, для того, чтобы определить, кто, когда и откуда имеет доступ к информации. Неудачные попытки, так же как и попытки входа в аномальное время в течение дня должны быть отслежены.

Аудит изменений в структуре базы данных. Какие-либо изменения, кроме изменений, вносимых администраторами БД в специально отведенное время, следует рассматривать как подозрительные.

Третья задача аудита определяет, подлежит ли аудиту каждая попытка пользователя воспользоваться предоставленным ему правом.

---

10 слайд

На следующем слайде представлены несколько решений аудита в других СУБД, отличной от рассматриваемой в рамках дипломного проекта. Существует возможность использовать стандартные средства аудита таких СУБД такие как: Oracle, MS SQL Server и т.д. Для бесплатных же СУБД, таких как PostgreSQL, таких средств пока нет. Стандартные средства других СУБД являются менее удобными и гибкими в применении, либо осуществляют аудит, сильно нагружая систему, в которой проводится аудит. Дипломный проект лишен всех этих недостатков. Перейдем далее.

---

11 слайд

Рассмотрим систему, по которой проводится аудит в дипломном проекте.

Физическое представление программной системы не может быть полным, если отсутствует информация о том, на каких вычислительных средствах она реализована. Для

представления общей структуры программной системы предназначены диаграммы развертывания. Рассмотрим их.

Общий смысл диаграммы в том, что на рабочей станции имеется приложение Podsystem.exe , которое подключается к серверу базы данных, на котором развернута СУБД PostgreSQL и добавляет в базу данных необходимые таблицы, а так же триггер со своими параметрами для аудита.

---

12 слайд

Общий смысл диаграммы в том, что имеется рабочая станция, подключение к БД, сервер БД, сервер приложений, веб-сервер.

Добавляется возможность использования сервера баз данных неким другим сервером приложений.

Добавляется также возможность подключения приложения podsystem ко второй базе данных, также под управлением системы PostgreSQL и располагающейся на другом сервере базе данных. Приложение podsystem также добавляет в эту базу данных необходимые таблицы и триггер со своими параметрами для аудита.

---

13 слайд

Рассмотрим структуру подсисистемы. Для работы созданного программного продукта необходимо в БД, к которой осуществляется подключении добавить таблицы, представленные на слайде. Также на слайде представлены некоторые SQL запросы и объекты СУБД, которые необходимы для создания такого инструмента, как триггер, который в приложении осуществляет задачи аудита.

2 – получение имени таблицы, исключая служебные таблицы, 1 – получение полей также исключая служебные поля, 3 – получение комментариев из БД для поля. 4 – добавление комментариев поля, 5 – каскадное удаление триггерной функции, 6 – создание триггера на определенную триггерную функцию

---

14 слайд

Рассмотрим разработанную подсистему аудита

На слайде представлена форма ввода пароля и имения, которая появляется сразу после запуска приложения. После ввода этих данных переходим к главному окну, где через меню можно перейти либо к таблице настройкам, либо к созданию триггера, что и рассмотрим на следующем слайде.

---

15 слайд

На этом слайде представлена форма создания и генерации триггера. На этой форме можно выбрать операции, по которым будет проводиться аудит. Также можно выбрать для записи или запроса будет работать триггер аудита. После чего выбираем имя таблицы, затем загружается из БД список полей, которые также выбираем, и для которых можно добавить комментарии. После всего этого и нажатия на кнопку Создать триггер создается триггер по выбранным параметрам, который и является основным инструментом для аудита и записываются данные в таблицу настроек.

---

16 слайд

Предусмотрена защита от добавления триггера на таблицу, где триггер уже существует, при попытке это сделать появляется окно.

При выборе в меню главного окна второго пункта появится окно настроек, в котором можно увидеть какие триггеры на какие таблицы и поля были созданы. Также есть возможность удалить его нажатием кнопки 'delete', при этом триггер и связанная с ним триггерная функция, а также записи в таблице настроек удаляться.

---

17 слайд

Главное окно имеет фильтры таблицы и саму таблицу, которая сама является представлением таблицы logs, которая имеется в БД.

При выборе фильтров пользователя, времени или таблицы происходит обновление таблицы согласно выбранным фильтрам, как это видно на слайде.

---

18 – 19 слайд

Произведена оценка экономической эффективности, разработка целесообразна.

Подготовлены документы для подачи на патент и лицензионный договор.

---

20 слайд

Основные поставленные цели были выполнены в ходе работы по дипломному проекту. Разработанная модель аудита и программный комплекс являются основой для дальнейшей разработки для более сложных систем и задач, но даже на том этапе, на котором проект есть сейчас, проведение аудита осуществляется должным образом, что в свою очередь поможет повысить информационную безопасность любой рассматриваемой системы и базы данных в этой системе.

Доклад окончен. Спасибо за внимание!