Введение:

Современные требования бизнеса, предъявляемые к определению уровня обеспечения информационной безопасности, и существенный рост рисков потерь (материальных, финансовых, моральных, информационных) от нарушения информационной безопасности во всех сферах жизнедеятельности общества и государства, диктуют настоятельную необходимость использовать в своей работе обоснованные технико-экономические методы и средства, позволяющие количественно и качественно измерять уровень защищенности организаций и систем информационной технологий, а также оценивать экономическую эффективность затрат на информационную безопасность. Одним из направлений, позволяющих оценить уровень обеспечения информационной безопасности, является аудит информационной безопасности, цель которого - установление степени выполнения требований по обеспечению состояния защищенности системы информационных технологий. На сегодняшний день СУБД играют ключевую роль в обеспечении эффективного выполнения процессов предприятий. Вместе с тем повсеместное использование СУБД для хранения, обработки и передачи информации приводит к повышению актуальности проблем, связанных с их защитой. Именно для решения этих проблем и применяется аудит безопасности системы. В качестве объекта аудита может выступать как СУБД в целом, так и её отдельные сегменты, в которых проводится обработка информации, подлежащей защите. Существует возможность использовать стандартные средства аудита таких СУБД как: Oracle, MS SQL Server и т.д. Но, как правило, данные средства есть только у платных СУБД. Для бесплатных же СУБД, таких, к примеру, как PostreSQL, подобных решений пока не нет. Основной задачей является разработка решения аудита информационной системы, использующей СУБД PostgreSQL. Данную задачу можно решить путём создания подсистемы аудита, которая позволит обнаружить действия, нарушающие целостность основной систем, другими словами, с помощью данной подсистемы можно выявить как мошеннически введенные данные, так и несанкционированные запросы.

Глава 1:

В настоящее время организации все больше зависят от информации, которую они используют. Если подвергать риску эту информацию с точки зрения потерь или несанкционированного доступа конкурентов могут последовать разрушительные последствия для организации. Таким образом, управление информационной безопасностью стало серьезной проблемой для всех организаций. Управление информационной безопасностью основывается на множестве политик и внутреннем контроле, с помощью которых организация и управляет своей информационной безопасностью. Информация и системы, которые обрабатывают ее, имеют решающее значение в работе практически всех организаций. Информация становится все более уязвимой для большого количества рисков, которые могут поставить под угрозу само существование предприятия. Это вынуждает принимать сложные решения о том, как сделать информационную безопасность эффективней. Цели информационной безопасности, как правило, считается выполненным, если: 1) Информационные системы имеются в наличии и готовы к использованию при необходимости; 2) Данные и информация раскрывается только тем, кто имеет право их знать (конфиденциальность); 3) Данные и информация защищена от несанкционированного изменения (целостность). Организации должны реализовать эти цели, чтобы удостовериться, что их ценная информация защищается от возможных потерь, недоступности, изменения или неправомерного раскрытия. Стоит рассмотреть принципы аудита средств управления информационной безопасности и как они могут помочь организациям обеспечить, чтобы эти цели были удовлетворены и что никаких недостатков системы существуют. Однако, во-первых, важна

причина, почему аудит так важен. Цель аудита состоит в том, чтобы оценить производительность управления. Из-за распространенного использования систем информационных технологий, важно, чтобы средства управления существовали. Средства управления IT - определенные процессы IT, разработанные, чтобы поддерживать бизнес-процесс. Средства управления IT могут быть категоризированы или как общие средства управления или как средства управления приложением. Общие средства управления - те средства управления, которые широко распространены на все компоненты систем, процессы и данные для данной организации или системной среды. Они включают средства управления такими областями как центр обработки данных и сетевые операции, системный сбор программного обеспечения и обслуживание, система обеспечения безопасности доступа и сбор прикладной системы, разработка и обслуживание. Средства управления приложением - те средства управления, которые являются подходящими для индивидуальных подсистем учета, такими как платежная ведомость или кредиторская задолженность. Они относятся к обработке отдельных приложений и помогают гарантировать, что транзакции произошли, авторизованы, и полностью и точно зарегистрированы, обработаны и сообщены. Это означает, что организации должны заняться расследованиями, достигают ли средства управления своих целей, выполняя аудит. Целью аудита является: 1) Обеспечение управления с достаточной гарантией того, что цели управления будут достигнуты; 2) Обоснование риска, где есть существенные слабые места управления; 3) Консультирование руководства по корректирующим действиям. Общепринятая структура процесса аудита заключается в следующем: 1) Получение понимания связанных рисков бизнес-требований и соответствующих мер контроля; 2) Оценка целесообразности установленных средств управления; 3) Оценка соответствия путем тестирования работают ли средства управления как предписано, последовательно и непрерывно; 4) Обоснование риска целей управления, не встречаемых при помощи аналитических методов и/или консультационных альтернативных источников.