Троян И.В. Защита от атак с использованием временных таблиц в базах данных // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 1(51) с. 168–171

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.736

# ЗАЩИТА ОТ АТАК С ИСПОЛЬЗОВАНИЕМ ВРЕМЕННЫХ ТАБЛИЦ В БАЗАХ ДАННЫХ

**Троян И.В.**
*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: it.bonch@gmail.com*

**Временные таблицы широко используются в базах данных для хранения промежуточных данных, однако они могут стать вектором атак, если не обеспечена надлежащая защита. В статье рассматриваются основные угрозы, связанные с использованием временных таблиц, такие как SQL-инъекции, эксплуатация временных таблиц для эскалации привилегий, а также методы защиты, включая контроль доступа, шифрование и мониторинг активности.**

Ключевые слова: Временные таблицы, базы данных, SQL-инъекции, безопасность, эскалация привилегий, контроль доступа, шифрование.

# PROTECTING AGAINST ATTACKS USING TEMPORARY TABLES IN DATABASES

**Troyan I.V**.
*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: it.bonch@gmail.com*

**Temporary tables are widely used in databases for storing intermediate data, but they can become an attack vector if not properly secured. This article explores the main threats associated with temporary tables, such as SQL injection and privilege escalation, and discusses protection methods, including access control, encryption, and activity monitoring**.

Keywords: Temporary tables, databases, sql injection, security, privilege escalation, access control, encryption..

## Введение

Временные таблицы являются важным инструментом в базах данных, поскольку они позволяют хранить временные данные, используемые для выполнения сложных операций, оптимизации запросов или выполнения аналитических вычислений. Однако, несмотря на их полезность, временные таблицы могут представлять угрозу для безопасности, если они используются неправильно или без должной защиты. Злоумышленники могут использовать уязвимости, связанные с временными таблицами, для кражи данных, изменения конфиденциальной информации или даже получения доступа к системам, которые выходят за рамки базы данных.

Одной из наиболее распространённых атак на базы данных является использование SQL-инъекций, с помощью которых злоумышленники получают возможность создавать или модифицировать временные таблицы для достижения своих целей. Например, при

недостаточной валидации входных данных злоумышленник может создать временные таблицы, содержащие вредоносные данные, или использовать их для обхода механизмов аутентификации. Проблема осложняется тем, что временные таблицы часто не подвергаются такому же уровню защиты, как основные таблицы базы данных, из-за их временной природы.

В статье рассматриваются основные риски, связанные с временными таблицами, и предлагаются методы их предотвращения, включая внедрение строгих политик доступа, использование современных технологий шифрования и мониторинг активности для обнаружения подозрительных действий.

**Защита от атак с использованием временных таблиц в базах данных**

Временные таблицы, как правило, создаются для выполнения промежуточных операций, таких как сортировка, агрегация данных или хранение результатов сложных вычислений. Однако их временный характер и высокая степень использования в процессе обработки данных делают их привлекательным объектом для атак. Одна из главных проблем заключается в том, что временные таблицы создаются и используются во временных пространствах, доступ к которым может быть плохо контролируемым. Злоумышленники могут использовать этот недостаток для реализации атак, направленных на нарушение конфиденциальности, целостности или доступности данных[1].

Наиболее известный тип атак, связанный с временными таблицами, — это SQL-инъекции. В рамках такой атаки злоумышленники вводят вредоносные SQL-запросы через пользовательский ввод или API-интерфейсы, которые затем исполняются сервером базы данных. Если временные таблицы используются для хранения результатов запросов, атакующий может вставить туда вредоносные данные. Например, временная таблица, используемая для проверки идентификаторов сессий, может быть скомпрометирована для предоставления атакующему доступа к данным других пользователей[2].

Ещё одной угрозой является эксплуатация временных таблиц для эскалации привилегий. Если пользователь базы данных имеет право на создание временных таблиц, он потенциально может попытаться модифицировать данные в основной базе, используя свои привилегии через временные таблицы. Например, временные таблицы могут быть использованы для выполнения сложных SQL-запросов, которые маскируют доступ к конфиденциальной информации или попытки её изменения[3].

Важной частью защиты временных таблиц является управление доступом. Рекомендуется ограничивать права на создание и модификацию временных таблиц только для тех пользователей, которым это действительно необходимо. Например, использование принципа наименьших привилегий может значительно снизить вероятность эксплуатации временных таблиц в качестве вектора атаки. Кроме того, использование механизмов аутентификации и авторизации, таких как роли и группы, может помочь в ограничении доступа к временным таблицам[4].

Шифрование данных, хранящихся во временных таблицах, — ещё один важный аспект безопасности. Современные базы данных предоставляют возможности шифрования на уровне столбцов или таблиц, что позволяет защитить данные, даже если атакующий получит к ним доступ. Однако стоит учитывать, что шифрование увеличивает нагрузку на сервер, поэтому его следует использовать выборочно, исходя из чувствительности данных.

Мониторинг активности базы данных помогает обнаруживать подозрительное поведение, связанное с временными таблицами. Например, аномально большое количество создаваемых временных таблиц или использование сложных SQL-запросов, которые отклоняются от стандартных рабочих процессов, могут указывать на попытки злоумышленников проникнуть в систему. Использование инструментов журналирования и анализа логов позволяет выявлять и предотвращать подобные атаки до того, как они нанесут ущерб[5].

Важно учитывать, что временные таблицы также могут стать вектором атак в случае их неправильного удаления. Например, если временная таблица не удаляется после завершения её использования, она может быть использована злоумышленником для внедрения вредоносных данных или выполнения атак. Поэтому рекомендуется использовать автоматическое удаление временных таблиц после завершения транзакции или сессии, а также регулярно проверять временные пространства на предмет остатков данных.

**Заключение**

Временные таблицы являются неотъемлемой частью современных баз данных, однако их использование сопряжено с рядом рисков для безопасности. Уязвимости, связанные с временными таблицами, могут быть использованы злоумышленниками для выполнения SQL-инъекций, эскалации привилегий и других видов атак. Эти угрозы требуют внедрения надёжных механизмов защиты, включая строгий контроль доступа, шифрование данных и мониторинг активности.

Защита временных таблиц должна быть приоритетом для разработчиков и администраторов баз данных, поскольку они часто становятся незамеченными объектами атак. Соблюдение принципов минимизации прав, регулярное обновление систем безопасности и автоматическое удаление временных таблиц после их использования — всё это ключевые меры для обеспечения надёжной защиты.

В условиях, когда базы данных продолжают оставаться одной из основных целей кибератак, эффективная защита временных таблиц становится необходимым элементом стратегии безопасности организаций. Только комплексный подход, сочетающий технические и организационные меры, способен предотвратить потенциальные угрозы и сохранить конфиденциальность, целостность и доступность данных в информационных системах.

**Список литературы**

1. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.
2. Миняев А. А. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 716-719.
3. Душин С. Е. и др. Синтез структурно-сложных нелинейных систем управления. – 2004.
4. Красов А. В., Сахаров Д. В., Тасюк А. А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 1. – С. 70-76.

5. Красов А. В. и др. Актуальные угрозы безопасности информации в сфере здравоохранения и офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 92-101

**References**

1. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch–Bruevich, 1996.
2. Minyaev A. A. Method for evaluating the effectiveness of the information protection system of geographically distributed information systems of personal data //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 716-719.
3. Dushin S. E. et al. Synthesis of structurally complex nonlinear control systems. – 2004.
4. Krasov A.V., Sakharov D. V., Stasyuk A. A. Designing an intrusion detection system for an information network using big data // High-tech technologies in space research of the Earth. – 2020. – Vol. 12. – No. 1. – pp. 70-76.
5. Krasov A.V. et al. Current threats to information security in the field of healthcare and ophthalmology //Ophthalmosurgery. - 2022. – No. 4s. – pp. 92-101.