нормы действующего законодательства, регулирующие особенности рассмотрения дел в порядке приказного производства.

***Ключевые слова**: арбитражный процесс, приказное производство, судебный приказ, взыскатель, должник.*

Сведения об авторе:
Музолев Иван Владимирович – магистрант частного образовательного учреждения высшего образования «Таганрогский институт управления и экономики», Ростовская область, г.Таганрог

UDC 004.056

OVERVIEW OF DATABASE INFORMATION PROTECTION APPROACHES IN MODERN DATABASE MANAGEMENT SYSTEMS

Nazarko A. V., Chernyshova A. V., Girovskaya I. V.
nazar2539@gmail.com

***Abstract.** This article discusses the classification of database security levels. Based on the classification, it is analyzing the database information protection approaches in modern DBMS. Tools for the protection of database information at the database management system level are considered. The advantages and disadvantages of existing database information protection solutions at the database management system level are defined.*

***Keywords:** information protection, databases, DBMS, safety approaches, protection tools, access control.*

To establish access to database information and work with it, the database management system (DBMS) is applied. The DBMS is a set of language and software, designed to create, maintain and share the database by many users. The DBMS is divided into data models. Let us consider the DBMS with the relational data model. DBMS provides features such as: sorting, database communication, event registration, reporting of changes made, etc.

The significance and value of the information fed into the database requires ensuring the protection of this information using the DBMS funds [6].

Analysis of database information protection approaches in modern DBMS

When designing information security tools in the DBMS, potential threats should be considered. The main threat is the risk of hacking and loss of confidential information stored in the database. When analyzing security, it is necessary to take into account that even the most minor defects in the protection system may entail the occurance of more serious threats. Unrecorded or malfunctioning standard information security methods with high probability are the cause of hacking a database or leakage of information from it. Let us consider some database protection approaches.

The database information security system in the DBMS must be multi-level, the number of protection levels reduces the risk of a database hacking. Lower levels include such approaches as: password protection, data encryption, delineation of access rights, registering operations, backup. These are the main approaches, without which the full protection is unattainable.

Based on the "Criteria for determining the security of computer systems" four grades of security (Security Classes) are distinguished:

- Class D – provides minimal protection (Minimal Protection), these are systems that are not suitable for other classes;
- Class C – provides selective protection (Discretionary Protection);
- Class B – provides mandatory protection (Mandatory Protection);
- Class A – provides proven protection (Verified Protection) [2].

Electoral access control (C class C) is divided into 2 subclasses – C2 and C1 – less secure than C2. The C1 subclass implies the division of data and the user, both mutual and separate access to data. The C2 subclass additionally provides logging into the system, audit and resource isolation. The class C is supported by many DBMS and is based on identifying users, database objects (tables, views, domains defined by the user set of symbols, stored procedures, etc.) and privileges - a set of actions on a particular object.

The authenticity of the user is confirmed by his identification or user recognition on his identifier – login and password. The accuracy of the identifier is confirmed – authentication. After that, the user is logged in and only data is available, based on the delimitation of access rights.

For the reliability of password protection, you must follow the instructions:

- the password must consist of a combination of letters, numbers or special signs;
- password length is at least six characters;

Passwords should be often changed and stored in secret.

A group of users who have the same group identifier can be maintained in the system, which are provided with the same access rights – this allows you to simplify the administration process. Operations of adding individual users to a group or removal from it can be performed regardless of the privilege task operation for this group.

The delimitation of access rights is a fairly flexible and developed system of any multiuser DBMS. The database administrator provides access rights to users in accordance with the principle of minimal powers necessary to fulfill direct official duties. Most of the DBMS provides a set of basic access rights management tools. Users and groups are endowed with access rights to specific database objects. Moreover, many DBMS indicate the allowed access type, for example, only reading, etc.

You can manage actions right with a specific object, depending on its type, for example, read, add, delete, and change records in the tables. Some DBMSs include access control at the table or view column level [3].

Mandatory access control (class B) – data objects are assigned certain classification levels that form a strict hierarchical order (for example, "secret", "top secret", "for official use", etc.), and users have security levels. It is divided into three subclasses – B1 – the least secure, B2 and B3 is the most secure.

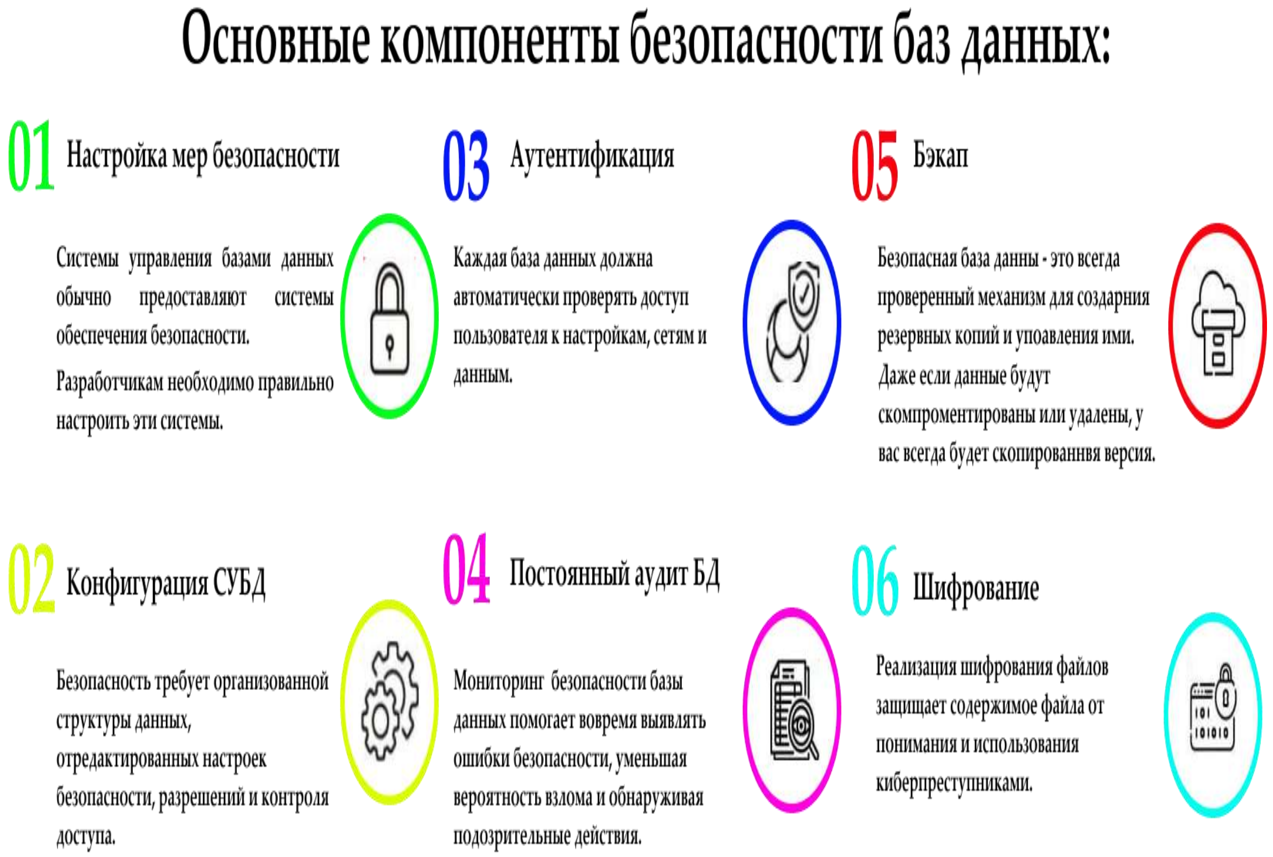
Subclass B1: Each data object contains a mark about its classification level, as well as an informal report on the current security strategy. Subclass B2: Additionally requires a formal approval of the current security strategy. Subclass B3: Supports audit, data recovery and purpose administrator assignment.

Such a rigid database structure is used in military, or government organizations. Access to the database object is carried out when the admission level is identical. To modify the object, the user's security level should be equal to the classification level of the object due to this, any information made by the user, is automatically assigned to the level identical to the classification of this user – this eliminates the secret data to the user with a high level of secrecy to a file with a smaller classification level.

Verified access control (Class A) is the safest approach and requires mathematical evidence of compliance of the security method of a given strategy.

Data encryption. To obtain unauthorized access to the database, not only the usual access to the system, and by moving part of the database through the connection to the channel. To prevent such a threat, it is necessary to use cryptographic means of information hiding (storing and transmitting confidential data in encrypted form).

Modes of operation with encrypted databases: decryption of the required file or part of the file on an external media (when working with information, it is again encrypted on an external storage device) or decryption in RAM - immediately before performing the necessary data actions (encryption procedures are built into the DBMS) (see Fig. 1).



Основные компоненты безопасности баз данных:

01 Настройка мер безопасности

Системы управления базами данных обычно предоставляют системы обеспечения безопасности.

Разработчикам необходимо правильно настроить эти системы.

02 Конфигурация СУБД

Безопасность требует организованной структуры данных, отредактированных настроек безопасности, разрешений и контроля доступа.

03 Аутентификация

Каждая база данных должна автоматически проверять доступ пользователя к настройкам, сетям и данным.

04 Постоянный аудит БД

Мониторинг безопасности базы данных помогает вовремя выявлять ошибки безопасности, уменьшая вероятность взлома и обнаруживая подозрительные действия.

05 Бэкап

Безопасная база данны - это всегда проверенный механизм для создарния резервных копий и упоавления ими. Даже если данные будут скомпроментированы или удалены, у вас всегда будет скопированнвя версия.

06 Шифрование

Реализация шифрования файлов защищает содержимое файла от понимания и использования киберпреступниками.

Figure 1 – Basic database security components

Registration of operations and backup. Logging allows you to register detailed information about all the operations of users with the database, it plays a significant role when detecting unauthorized actions with the database, identifying vulnerabilities in the protection system, as well as eliminate any data distortions. In addition to the above, you can also mention a backup that allows you to restore data in case of hardware or software failures. It is also recommended to configure a regular data backup and replication to a remote computer. The safety of databases should be styled, starting with the adoption of basic measures. Considered protection approaches are capable of a certain extent to ensure the confidentiality and integrity of data, but their use does not guarantee full data security [4].

Overview of DBMS protection tools

The presentation is the named sample dynamically supported by the server from one or more tables. This is a virtual table that the records are formed when the user appeals to it according to the request previously assigned to it. Using views, access is formed not to a whole table, but to certain records necessary for the user.

Suppose you are interested in a composite list of weather records and cities coordinates. To solve this problem, you must create a view on this request, actually assign a name request, and then access it as a regular table:

CREATE VIEW myview AS SELECT city, temp_lo, temp_hi, prcp, date, location FROM weather, cities WHERE city = name; SELECT * FROM myview;

Active use of views is a key aspect of good SQL database design. Presentations allow you to hide the internal device of your tables that may vary as the application develops, for reliable interfaces. Presentations can be used almost everywhere where ordinary tables can be used. And quite often, ideas are created on the basis of other ideas. It can be concluded that the view is the simplest method of protection of both confidentiality and data integrity, allowing you to clearly limit the data available to the user and control the data set that the user has the right to modify [3]. The trigger is a subroutine that automatically operates in the case of data modification in the table. Triggers are also classified according to whether they are triggered before, after or instead of operation. They are called BEFORE, AFTER and INSTAND OF, respectively. The working triggers of the operator levels are triggered before the operator begins to do anything, while the AFTER level triggers operator is triggered at the very end of the operator's operation. With the help of triggers, you can check the user's privileges, that is, answered the question whether the user has the right to modify specific data (you can perform to modifying data, with deficiency of the user's rights to this operation will be canceled), logging (for example, in a separate audit table) All Events related to data modifications in a protected table - makes it possible to quickly find the user who has fulfilled the unauthorized data modification. Triggers make it possible to effectively monitor the integrity of the data and to protocate their modification [5].

Encryption functions. Built-in encryption functions are not available in all DBMS, therefore, this method cannot be called universal. In the PostgreSQL DBMS, encryption is encrypted at different levels and is provided with flexibility in choosing data protection tools when the server is lost, incompetent administrators or in unprotected networks. Encryption may be necessary to ensure confidential data protection: financial transfers, etc. Encrypt user passwords - stored in the form of haze (password_encryption determines the hashing algorithm), the administrator does not have access to not hashized passwords. Pgcrypto provides the ability to store the selected base fields in encrypted form. Used when valuable only part of the database data. For decryption, the client transmits the key, the server decrypts the data and transmits them back to the client. Decoded data and decryption key are on the server during the decryption and data transmission process. This creates a vulnerability to intercept data and the keys face with full access.

SSL server authentication. The client and the server have the ability to check each other's authenticity using SSL certificates. To do this, you must configure them accordingly, which is more reliable than the password. With such a protection, the fake computer will not be able to issue itself for the server in order to obtain passwords for database users. Attacks with an intermediary ("man in the middle" the inconspicuous transmission of all requests and data between the client and a genuine server) is also more likely to be prevented [1].

Advantages and disadvantages of existing data protection solutions at the DBMS level

Data protection solutions at the DBMS level are simple in operation, but in spite of the simplicity they effectively ensure the confidentiality and integrity of the data.

The disadvantage of data protection solutions by embedded DBMS means is that protection with their help is difficult to provide for an existing system. At the design stage of protected database, an additional level of protection is envisaged in the form of a comprehensive use of representations, triggers and built-in cryptographic functions of the DBMS.

Decipheration of encrypted database information on an external device. Dignity is an independent sequential functioning of encryption and DBMS. Disadvantage – as a result of a failure , a part of the database may remain recorded an in unencrypted way.

Decipheration of encrypted database information in RAM. Dignity is a high level of protection against unauthorized access. The disadvantage is a low level of performance of the DBMS due to its complications.

Hence, within the framework of the article the means of protecting modern DBMS are briefly reviewed. A description is presented of the possibility of using them to protect data in the database at the DBMS level. When considering existing approaches, solutions and means to ensure the safety of databases, their advantages and disadvantages were revealed. In the future, it is planned to consider in more detail the vulnerability in client-server applications of two-bonded and three-bed architecture on a specific example of a database, as well as submit recommendations for designing and creating secure client-server applications using modern DBMS.

References

1. Возможности шифрования [Электронный ресурс] /. – Режим доступа: https://postgrespro.ru/media/docs/postgresql/12/ru/postgres-A4.pdf – Загл. с экрана.
2. Классы информационной безопасности в международных стандартах [Электронный ресурс] /. – Режим доступа: https://arinteg.ru/articles/klassy-informatsionnoy-bezopasnosti-v-mezhdunarodnykh-standartakh-30970.html – Загл. с экрана.

3. Методы защиты данных встроенными средствами СУБД [Электронный ресурс] /. – Режим доступа: http://www.panasenko.ru/Articles/192/192.html – Загл. с экрана.

4. Обзор механизма работы триггеров [Электронный ресурс] /. – Режим доступа: https://postgrespro.ru/media/docs/postgresql/12/ru/postgres-A4.pdf/ – Загл. с экрана.

5. Основные аспекты безопасности СУБД: что следует знать [Электронный ресурс] /. – Режим доступа: https://tproger.ru/articles/dbsecurity-basics – Загл. с экрана.

6. Системы управления базами данных [Электронный ресурс] /. – Режим доступа: http://www.bseu.by/it/tohod/sdo4.htm – Загл. с экрана.

7. С ЧЕГО НАЧИНАЕТСЯ ЗАЩИТА БАЗЫ ДАННЫХ? [Электронный ресурс] /. – Режим доступа: https://www.dataarmor.ru/с-чего-начинается-защита-базы-данных – Загл. с экрана.

ОБЗОР ПОДХОДОВ К ЗАЩИТЕ ИНФОРМАЦИИ БАЗ ДАННЫХ В СОВРЕМЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

Аннотация. *В данной статье рассматривается классификация уровней безопасности баз данных. Опираясь на классификацию, производится анализ подходов защиты информации баз данных в современных СУБД. Рассмотрены средства защиты информации баз данных на уровне системы управления базами данных. Определены достоинства и недостатки существующих решений по защите информации баз данных на уровне системы управления базами данных.*

Ключевые слова: *защита информации, базы данных, СУБД, подходы к безопасности, средства защиты, управление доступом.*

Сведения об авторах:

Назарко Анна Вадимовна – студент группы ПИм-20 факультета компьютерных наук и технологий, ГОУ ВПО «Донецкий национальный технический университет»

Чернышова Алла Викторовна – старший преподаватель кафедры «Программная инженерия», ГОУ ВПО «Донецкий национальный технический университет»

Гировская Ирина Валерьевна – старший преподаватель кафедры английского языка, ГОУ ВПО «Донецкий национальный технический университет»