**Kopach V. V. student of group 125-20-1**
**Scientific supervisor: Olishevskiy I. H., assistant of the department of information security and telecommunications**
*(Dnipro University of Technology, Dnipro, Ukraine)*

## SECURITY OF RELATIONAL DATABASE SYSTEMS

In the modern world, many routine procedures have been transferred to digital form, and whether it is an online purchase on the Internet, filling out a questionnaire or creating an account, all data must be stored in a place inaccessible to outsiders. That's what databases are for.

A database is an ordered collection of information or data that is stored on a computer system. Today there are more than 50 different types of databases, but they can be divided into three main categories: hierarchical, object-oriented and relational. Their main difference lies in the different structure and, accordingly, different work, but relational databases are the most popular – first of all, this is due to the simplified process of extracting the necessary information from a large number of records. Also, the main advantages of a relational database are ease of use and display of information, complete separation of access to data from their physical organization, the ability to concisely describe the basic operations on data, thanks to a developed mathematical apparatus, and the creation of languages for manipulating non-procedural type of data. Information modeling in the form of a set of linked tables is a universal method for organizing data and is relevant for a user of any level: both beginner and advanced. However, the relational database, at the same time, has a number of certain disadvantages. For example, one of the significant drawbacks in the work can be called the slowest access to data compared to hierarchical and object-oriented databases. Basically, this problem concerns data access at the level of their physical organization, that is, indexed files, so some difficulties may arise at this stage. As another drawback, the features of this model at the conceptual level are often singled out – keys, entity identifiers, if they are incorrectly distributed, can undermine the functioning of the database, and then the management of stored data will become limited. This problem does not seem so large-scale when we are operating with a small amount of data; however, such an error can disable a multi-level system until the error is eliminated.

But the greatest threat to any computer system, including database systems, is vulnerabilities. Most of them are related to incorrect installation and configuration of the database by its administrator. Among such errors, one can single out incorrect rights management – this is fraught with unauthorized use or disclosure of confidential information. Access to backups entails the threat of copying backups by unauthorized users, after which data stored on servers can be extracted. Roughly the same consequences follow the non-compliance with the software installation policy in the organization – thus, hidden database servers appear, which administrators do not know about, and therefore cannot prevent potential information leakage. However, SQL injection attacks are identified as the main form of database vulnerabilities. Such a threat is especially acute for relational, the most used, databases. Malicious code is injected from the front-end of the web application and then passed to the back-end, and this is the following principle: malicious code is inserted into user input variables, which is then combined with SQL commands and executed. In the process of executing the code, the text string ends earlier and a new command is attached. This attack can take a more subtle form by injecting unsafe code into strings intended to be stored in tables or as metadata. And if the inserted SQL code is syntactically correct, the corrupted data cannot be detected programmatically. The upward trend in attacks and consequent data theft can be seen in Figure 1. In 2020, the total amount of data breaches reached over 250 million, which is one of the highest rates of all time. And, despite the fact that in 2022 there were many times less data leaks, the figures in the third quartile are 4.5 times higher than in the first quartile of the same year, which suggests that an outbreak with large-scale attacks is not excluded.

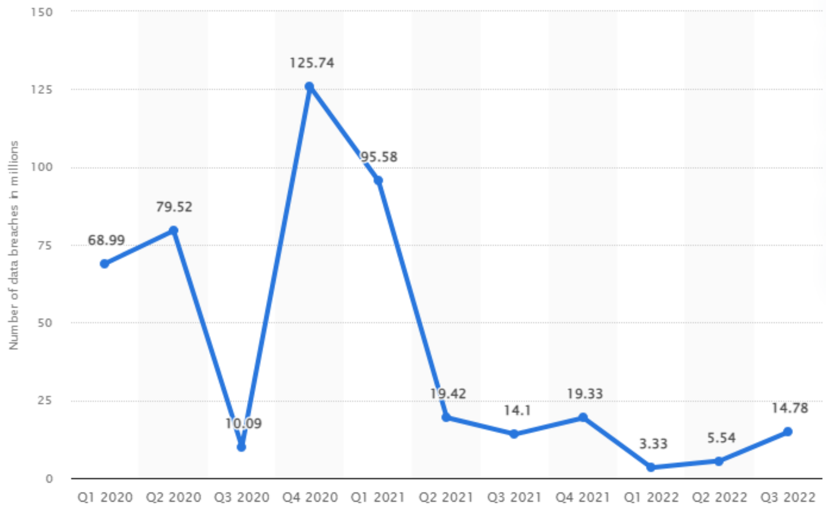

Figure 1 – Data leakage statistics from 2020 to 2022

To avoid any unauthorized intrusion into the database, it is essential to regularly test its security. Typically, this process involves testing different layers, such as the business layer, the access layer, or the user interface layer. System testing takes place in several stages and can be of different types: a penetration test simulates a cyber-attack on a system, a vulnerability scanner automatically looks for common vulnerabilities, a security audit assesses compliance with an organization’s security policies and standards, and a risk assessment allows you to identify and analyze all possible threats and risks. Each of these types is aimed at one goal – to strengthen the security of the database system and to warn against violation of the integrity and confidentiality of information. After testing and identifying actual vulnerabilities, it is equally important to fix existing problems as soon as possible. The most common troubleshooting tips for these issues include blocking malicious web requests, managing user rights and eliminating excessive privileges, archiving external data, and encrypting databases and masking their fields. In addition, special attention should be paid to protection against SQL injections – this can be done using restrictions on the input of special characters and keywords, the use of secure SQL parameters and, of course, constant monitoring of database access activity and attacks on protocols.

As a conclusion, we can summarize that in today's conditions of active development and transition to technology, it is important to pay more attention to the security of databases, since they contain a large amount of confidential information of thousands and millions of users, and must not to forget about monitoring and regularly checking the reliability of database system security.

## Reference

1. Database Security [Electronic resource] // https://www.imperva.com/learn/data-security/database-security/
2. The Top 10 Most Common Database Security Vulnerabilities [Electronic resource] // https://www.datasunrise.com/potential-db-threats/10-common-vulnerabilities/
3. Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022 [Electronic resource] // https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/#:~:text=During%20the%20third%20quarter%20of,2020%2C%20nearly%20125 %20million%20cases