DOI: 10.14529/ctcr160219

DEVELOPMENT AND EXPLOITATION OF DATABASES APPLICATION IN RESPECT OF INFORMATION SECURITY REQUIREMENTS

E.S. Yarosh, *elc-y@yandex.ru*
South Ural State University, Chelyabinsk, Russian Federation

This paper describes creation of database application, which correspond the requirements of data security. The main emphasis is put on protection of personal information. It is shown that increase of security level is reached due to normalization, especially to the level of the fifth normal form, safety of metadata and tables keys, existence audit tool for control user actions, the accounting of the destroyed data and its repeated destruction at restore database from backup copy, determination of volume of the destroyed data, which won't allow inappropriate data using.

Keywords: database, personal data, information security.

Problems databases security is very important now. It became especially important by adoption in 2006 of the Federal law "About personal data". Big concern among users and developers of information systems with the personal data (PD) was generated. Now this problem is actually too. Some applications developed before adoption of the personal data law not allow to effective protection of PD. In some new development this aspect isn't always carefully worked too. It is obvious that questions of data security have to be considered both at a creation stage, and at a stage of exploitation of system. But there is a number of irresolvable collisions in principle which understanding allows to search some compromises accepted for specific conditions.

Questions of data protection should pay attention already at a database design stage.

There are two directions in the area of DBMS now: SQL-and NoSQL-systems. However NoSQL-systems are not so mass to use like traditional relational DBMS. Therefore design of database applications with data security is considered in aspect of relational model in this article.

During mass acquisition of relational approach there was a slogan "Any Correct Database Has to Be Normalized". Later some developers began to treat it less categorically. For example, at creation of data storages developers often carry out denormalization for reduction of number of tables and, as a result, search acceleration. However normalization can render a great service in aspect of protection of PD.

The majority of correctly organized, i.e. normalized at least to the third normal form databases with PD has the structure shown in Fig. 1.

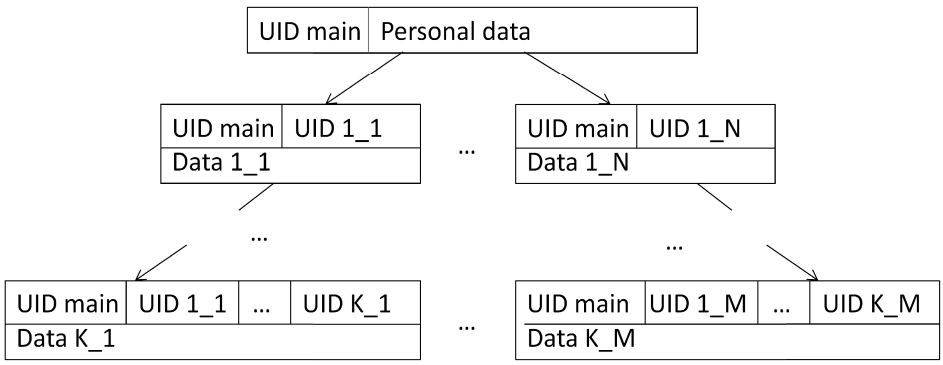

Fig. 1. Typical data base structure with PD

There is single main table, which contain personal data. Every line of this table is characterized by the unique identifier UID main. Other tables are subordinated. They are attached to main table by means of inheritance of the corresponding identifier. Thus, the subordinated tables become automatically depersonalized and it is enough to cipher or protect by otherwise method the main table for according to the law of personal data.

Normalization to the third normal form level is the elementary and very effective way of ensuring data security in many cases. However it isn't enough for a number of applications. Exposure is appeared by the linked keys like UID main – UID 1_L – … – UID P_Q, which are serving for a binding of the subordinated tables to the main table and to each other. Access to linked keys allows opening structure of data and communication between them. Risk of data disclosure increases when database designer use objects naming rules, for example, [1], which are very convenient for regular work. The concordant naming system allows track logic of a data structure and make them more readable. Certainly, it is useful for developers, who complete the project after time or when team work is in use. Risk data disclosure is on other bowl of scales, for example, by insider.

Splitting of linked keys is promoted also by reduction to the fifth normal form. The fifth normal form is focused on the work with dependent joins. I'll show a classical example. Let relation EMPLOYEE-DEPARTMENT-PROJECT consider only the key attributes like Employee_code, Department_code and Project_code. One employee can work in several departments, and in each department he can take part in several projects. Reduction to the fifth normal form generates three tables: EMPLOYEE-DEPARTMENT (Employee_code, Department_code), EMPLOYEE-PROJECT (Employee_code, Project_code), DEPARTMENT-PROJECT (Department_code, Project_code). As the result, the number of tables, which should be analyzed for disclosure of data, increases. Besides, anomalies of data removal and inserting are eliminated. That is characteristic for normalization in general. However it should be noted that dependent joins between three attributes is meeting not often. Dependent joins between more than three attributes almost can't be specified in practice.

Data reliability is of great importance during the work with PD. This question usually lies in a zone of responsibility of the application user who has rights to data input or update. However, as a rule, this work is executing of the lowest position personal (for example, order takes, medical record administrator, etc.). Unfortunately, this personal sometimes isn't fully qualified and responsible. Requirement of definition a source of data distortions is appear in this case. DBMS audit level (if it is available) is excess in this case. This operation is excessively resource-intensive. Besides, it is intended for the high qualified specialist in the area of DBMS administration and analysis of DBMS work. Practically search of the data distortion source usually is carried out by the application administrator who is an expert in subject domain, but who isn't DBMS specialist. Therefore audit of the user actions is necessary in similar systems. The simplest decision of this problem consists in addition to main table and other sensitive tables some fields. Information about user who executed operation with data, operation type (input or adjustment), date, time and other necessary data is fixed in this fields. It is obvious that the report on these data also is necessary. As for removal operation, it should be carried to the especially protected. It is possible to allocate this mode, for example, by means of the separate protected menu item. Perhaps, maintaining the special journal of removals will be required. Use of temporal databases [2] can become a solution of the problem of illegitimate changes roll back. An example is the Oracle Flashback [3] technology. But it is very expensive and troublesome solution to the majority of "ordinary" information systems.

One more collision is generated by need of backup copies. The rule "3-2-1" is considered in [4]. This rule provides creation of at least three backup copies of data, storage of backup copies on two different mediums, storage of one backup copy out of office. This rule is very useful in the context of data safety. But during the work with personal data some condition occurs when the law demands guaranteed destruction this PD. Three-day term is taken away for this purpose. It is obvious that backup copies made before the term of destruction of personal data can be treated as violation of law of PD. All destroyed data automatically will be restored at emergency data restore on backup copies. The developer of the "correct" application needs to provide the special tool for detection such data and their repeated destruction.

If application provides the data analysis in a temporary section or sending data to data storage for the subsequent analysis, data destruction is inadmissible. The law on PD orders data depersonalization in this case. It can be made by partial removal of data. For example, a name, a surname, and a middle name can be removes from the table storing personal information. But saving of other sensitive information like phone number, e-mail addresses etc. may be undesirable in case of loss of control over data. The law is respected in form. But leakage of such depersonalized database and its use by the foreign organizations, for example, for the persuasive offer of goods and services, obviously discredits the firm

which was legally data owner. Therefore the destroyed information volume under depersonalization also has to be planed carefully at the stage of creation of application.

Summarizing the above, it is possible to formulate the following principles of maintenance of data security at the stage of creation and exploitation database applications:

1) Normalization, at opportunity to the level of the fifth normal form;

2) Protection of metadata, keys of tables in particular;

3) Availability of audit tool for control user actions;

4) Accounting of the destroyed data, organization of repeated destruction in case of restore database from a backup copy;

5) The volume of the destroyed data has to be such to exclude using of the remained data for unauthorized purposes.

References

1. Mikhaylichenko A. *Pravila imenovaniya ob"ektov bazy dannykh* [Rules of Database Object Naming]. Available at: http://citforum.ru/database/articles/naming_rule.

2. Kostenko B.B., Kuznetsov S.D. *Istoriya i aktualnye problemy temporalnykh baz Dannykh* [History and Actual Problems of Temporal Databases]. Available at: http://citforum.ru/database/articles/temporal/.

3. *Tekhnologiya Oracle Flashback* [Technology of Oracle Flashback]. Available at: http://www.oracle.com/technetwork/ru/database/oracle-flashback-tech-433693-ru.html.

4. Levkina M. [The Rule of Backup Copy "3-2-1" is Continue Actual]. *Windows IT Pro*, 2015, no. 4, pp. 23–24. (in Russ.)

Received 13 February 2016

УДК 004.6 + 004.56 **DOI: 10.14529/ctcr160219**

РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ПРИЛОЖЕНИЙ БАЗ ДАННЫХ С УЧЕТОМ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.С. Ярош

Южно-Уральский государственный университет, г. Челябинск

Рассматриваются вопросы создания прикладных систем, основанных на базах данных, отвечающих требованиям защиты информации. Основной упор сделан на защиту персональных данных. Показано, что повышение уровня защищенности достигается за счет нормализации, особенно до уровня пятой нормальной формы, обеспечения безопасности метаданных и ключей таблиц, наличия средств аудита уровня приложения, учета удаляемой информации и ее повторного удаления при восстановлении баз данных из резервных копий, определения достаточного объема удаляемых данных с целью недопущения их нецелевого использования.

Ключевые слова: базы данных, персональные данные, информационная безопасность.

Литература

1. Михайличенко, А. Правила именования объектов базы данных / А. Михайличенко. – http://citforum.ru/database/articles/naming_rule/.

2. Костенко, Б.Б. История и актуальные проблемы темпоральных баз данных / Б.Б. Костенко, С.Д. Кузнецов. – http://citforum.ru/database/articles/temporal/.

3. Технология Oracle Flashback. – http://www.oracle.com/technetwork/ru/database/oracle-flashback-tech-433693-ru.html.

4. Левкина, М. Правило резервного копирования «3-2-1» по-прежнему актуально / М. Левкина // Windows IT Pro. – 2015. – № 4 . – С. 23–24.

Ярош Елена Семёновна, канд. техн. наук, доцент кафедры электронных вычислительных машин, Южно-Уральский государственный университет, г. Челябинск; elc-y@yandex.ru.

Поступила в редакцию 13 февраля 2016 г.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Yarosh, E.S. Development and Exploitation of Databases Application in Respect of Information Security Requirements / E.S. Yarosh // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2016. – Т. 16, № 2. – С. 160–163. DOI: 10.14529/ctcr160219

FOR CITATION

Yarosh E.S. Development and Exploitation of Databases Application in Respect of Information Security Requirements. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2016, vol. 16, no. 2, pp. 160–163. DOI: 10.14529/ctcr160219