

УДК 004.9

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ БАЗАМИ ДАННЫХ

*Игнатъева М.А., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н, доцент
ФГБОУ ВО Ульяновский ГАУ*

Ключевые слова: защита информации, базы данных, системах управления базами данных.

В статье анализируются особенности решения проблемы защиты информации в современных системах управления базами данных, обеспечение эффективной и надежной работоспособности системы баз данных.

В современном мире любая работа связана с оперированием большим объемом информации, которая выполняется широким кругом лиц. Защита данных от несанкционированного доступа является одной из главных задач при построении любой информационной системы.

Для СУБД важны три основных аспекта информационной безопасности:

- конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право;
- целостность - избежание несанкционированной модификации информации;
- доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Темой данной статьи является первый из них – средства защиты от несанкционированного доступа к информации.

Существуют два основных вида информационной защиты СУБД – дискреционная и мандатная.

Дискреционное управление доступам — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Дискреционная защита является многоуровневой логической защитой.

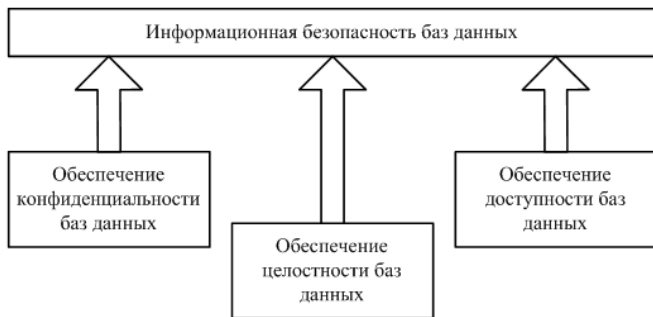


Рисунок 1 - Информационная безопасность баз данных

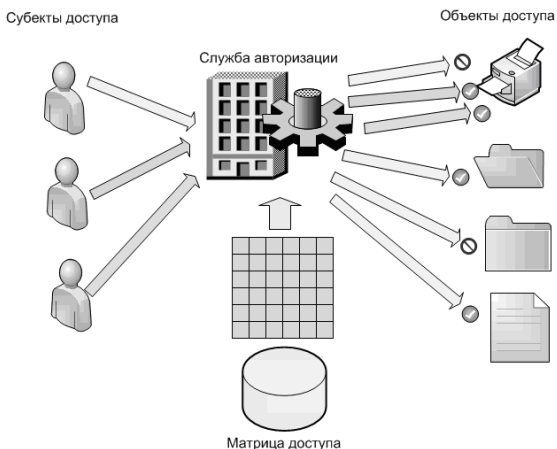


Рисунок 2 - Дискреционное управление доступом

Логическая защита в СУБД представляет собой набор привилегий или ролей по отношению к защищаемому объекту. К логической защите можно отнести и владение таблицей (представлением). Данные о логической защите находятся в системных таблицах базы данных и отделены от защищаемых объектов (от таблиц или представлений).

Информация о зарегистрированных пользователях базы данных хранится в ее системном каталоге.

В процессе сеанса работы пользователя все его действия непосредственно связываются с результатом идентификации. Отсоединение

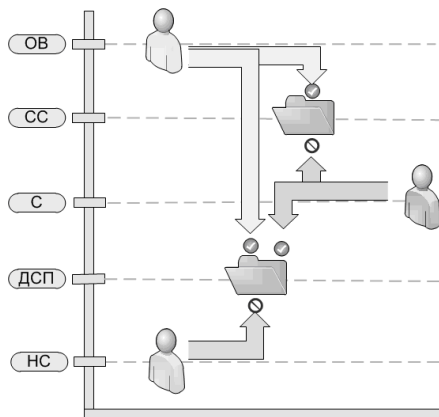


Рисунок 3 - Мандатное управление доступом

пользователя может быть как нормальным, так и насильственным. Во втором случае пользователь будет проинформирован об этом, и все его действия аннулируются до последней фиксации изменений, произведенных им в таблицах базы данных.

Однако дискреционная защита является довольно слабой, так как доступ ограничивается только к именованным объектам, а не собственно к хранящимся данным.

Мандатное управление доступом — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности

Существуют достоинства и недостатки мандатного управления доступом.

Достоинства:

- простота построения общей схемы доступа;
- простота администрирования.

Недостатки:

- проблема разграничения пользователей одного уровня;
- пользователь не может назначать доступ к объекту.

Таким образом, конфигурация, к которой имеет доступ хотя бы один программист, не может считаться безопасной.

Библиографический список

1. Давыдова, Л.А. Информационные системы в экономике в вопросах и ответах: учебное пособие / Л.А. Давыдова. - М.: ТК Велби, Издательство Проспект, 2006. –280с.
2. Соловьёв, А.В. Информационное общество: полифония культурных форм / А.В. Соловьёв. – Рязань, 2007. – 184с.
3. ИБ в современных системах управления базами данных (дискреционная и мандатная защита) [Электронный ресурс].- URL: <http://compress.ru>

INFORMATION SECURITY IN MODERN CONTROL SYSTEMS DATABASE*Ignateva M.A.*

Key words: *information security, database, database management systems.*

This paper analyzes the features of the solution of information security problems in modern database management systems, ensuring reliable and efficient performance database system.