УДК 681.3

***А.Н. Крутов***[1]

# ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ОТ НСД ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ, НАХОДЯЩИХСЯ В ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

В статье рассматривается вопрос построения систем защиты от несанкционированного доступа в информационных системах, находящихся в промышленной эксплуатации. Предлагаются две принципиальные схемы разработки системы от НСД с минимальными доработками в уже разработанной информационной системе. В качестве построения эффективной системы защиты в работе используются средства тщательного контроля доступа СУБД Oracle (Fine Grained Access Control). В зависимости от размеров исходной базы данных и возможности вносить изменения в структуру таблиц информационной системы предлагается использовать тот или иной способ построения системы защиты от несанкционированного доступа. Разработанная система защиты представляет собой относительно независимый модуль, который можно внедрять по мере необходимости.

**Ключевые слова:** базы данных, системы управления базами данных, информационные системы, несанкционированный доступ, система защиты, промышленная эксплуатация, модель безопасности, тщательный контроль доступа.

## Введение

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится достаточно широким кругом лиц [1]. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных [2; 3]. Целью является построение систем защиты от несанкционированного доступа в информационных системах, находящихся в промышленной эксплуатации. Под защитой от несанкционированного доступа понимаются недопущения в приложении доступа к просмотру и изменению информации в нарушении должностных обязанностей и полномочий сотрудника. Как показывает практика, весьма часто требуется решить задачу разграничения

[1]© Крутов А.Н., 2015

*Крутов Алексей Николаевич* (alexey.n.krutov@gmail.com), кафедра безопасности информационных систем, Самарский государственный университет, 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

доступа в информационных системах, которые уже находятся в промышленной эксплуатации. В этом случае требуется построить систему защиты от НСД с минимальными доработками. Это позволит создать по-настоящему общую защищенную систему, способную объединить весь спектр существующих информационных систем на предприятии в единое целое [4].

## 1. Классификация способов построения систем защиты от НСД

Предлагается следующая классификация способов построения систем защиты от НСД (рис. 1).

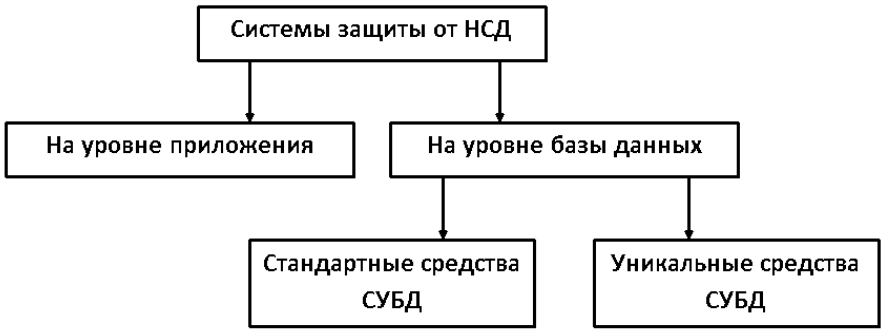


Рис. 1. Способы построения систем защиты от НСД

Защита на уровне приложения, как правило, сводится к написанию SQL-запросов с учетом идентификаторов пользователей, которые в данный момент работают с приложением. При этом в случае необходимости написания новых программных модулей приходится дублировать соответствующие механизмы безопасности. Для информационных систем, находящихся в промышленной эксплуатации, этот способ абсолютно не применим, так как требует полной переработки исходного кода программных модулей, что весьма трудоемко, а зачастую и невозможно. Защита от НСД стандартными средствами СУБД сводится к использованию механизмов безопасности, которые существуют практически в любой современной клиент-серверной СУБД. К ним относятся привилегии, позволяющие пользователям получать доступ к какому-либо объекту или операции над базой данных, представления, позволяющие ограничить доступ к части объекта, а также триггеры, позволяющие ограничить разным пользователям выполнение DML-операций над объектами базы данных.

## 2. Модель безопасности СУБД

Общая модель безопасности СУБД представлена на рис. 2.

Пользователю может быть назначена одна или несколько ролей, а роль может принадлежать одному или многим пользователям. Как пользователи, так и роли могут иметь много различных полномочий. С каждым объектом (в широком смысле этого слова) связаны определенные полномочия. Каждое полномочие относится к одному пользователю или группе и одному объекту. Когда пользователь входит

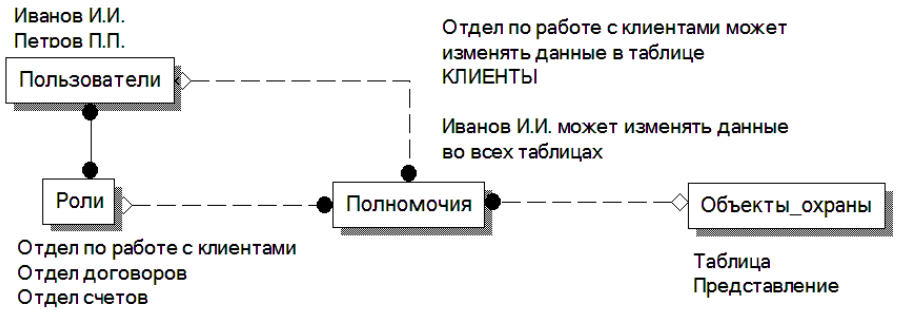


Рис. 2. Модель безопасности СУБД

в систему базы данных, СУБД ограничивает его действия полномочиями, определенными индивидуально для данного пользователя, а также для роли, назначенной данному пользователю. Использование стандартных средств защиты позволяет производить относительно легкую миграцию информационной системы с одной СУБД на другую. Для обеспечения безопасности данных на уровне отдельных записей следует использовать представления. Однако в случае, когда информационная система, данные которой следует защитить, уже находится в промышленной эксплуатации, этот способ представляется трудоемким, так как требует доработок программного кода, связанного с переходом на новые представления. Защита от НСД уникальными средствами СУБД позволяет достичь высокого уровня защищенности и производительности системы. К минусам такого способа построения можно отнести невозможность в случае необходимости быстрого перехода на другую СУБД. В настоящей работе описывается возможность разработки системы защиты данным способом с использованием СУБД Oracle версии 9i и выше. Для обеспечения безопасности используется средство Oracle, называемое Fine Grained Access Control (FGAC), которое входит в поставку версии Enterprise Edition [5]. Средства тщательного контроля доступа появились в СУБД Oracle, начиная с версии 8.1.5. Они позволяют во время выполнения динамически добавлять условие (конструкцию WHERE) ко всем запросам, обращенным к таблице или представлению базы данных. С помощью контекстов приложений можно безопасно добавлять в среду информацию (например, роль пользователя в отношении приложения) и обращаться к ней в процедуре или условии.

Средства тщательного контроля доступа позволяют с помощью одной таблицы и одной функции пакета справиться с задачей, для решения которой могло бы понадобиться несколько представлений или триггеров, или большой объем специализированной обработки в приложениях. Пакет можно изменить в любой момент, разработав новые правила защиты. При тщательном контроле доступа алгоритмы защиты, определяющие, какие данные может "видеть" пользователь, помещаются в базу данных. При этом гарантируется защита данных независимо от используемого средства доступа к ним. Средства тщательного контроля доступа позволяют отделить алгоритмы защиты от других алгоритмов работы приложения. Разработчик приложения может заняться прикладными алгоритмами, а не алгоритмами безопасного доступа к данным. Поскольку тщательный контроль доступа выполняется полностью на сервере баз данных, эти алгоритмы немедленно наследуются всеми приложениями. Даже если злоумышленник сможет перехватить SQL-запросы к базе данных, он все равно не сможет выявить особенности реализации за-

щиты, т. к. средства FGAC автоматически накладывают дополнительные условия на выдаваемые пользователю данные на уровне сервера и снаружи никак не видны. К сожалению, для того чтобы по-настоящему пользоваться возможностями FGAC, потребуется разработать соответствующее программное обеспечение для администратора, т. к. никаких приложений, ориентированных на пользователей в СУБД Oracle, не разработано.

## 3. Схемы разработки системы защиты от НСД

Предлагаются две принципиальные схемы разработки системы защиты от НСД с минимальными доработками в уже разработанной информационной системе. В первом случае (рис. 3) в таблице, доступ на просмотр к которой требуется ограничить, достаточно будет добавить одно поле, ссылающееся на таблицу уровней доступа [6].

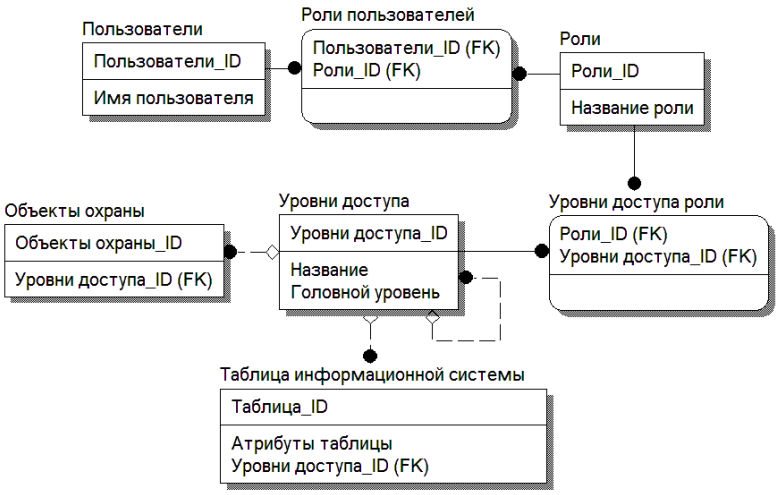


Рис. 3. Первый способ реализации защиты от НСД

Второй способ реализации системы защиты от НСД (рис. 4) не требует никаких изменений в таблицах информационной системы. Вся информация об объектах охраны и уровне полномочий по конкретным записям хранится в служебных таблицах системы безопасности.

Недостатком второго способа реализации является невозможность создания внешнего ключа из таблицы "Уровни доступа таблиц информационной системы" на сами таблицы, т. к. их в общем случае переменное количество, а поле связи в таблице только одно. Достоинство данной схемы заключается в отсутствии необходимости модифицировать структуры таблиц и исходных программных кодов информационной системы, находящейся в промышленной эксплуатации, что не нарушит ее работоспособность. Для осуществления безопасности в вышеперечисленных случаях следует использовать функцию, динамически изменяющую запрос к базе данных вида

**SELECT * FROM ТАБЛИЦА**

к запросу вида

**SELECT * FROM ТАБЛИЦА WHERE первичный ключ IN (VALUES)**

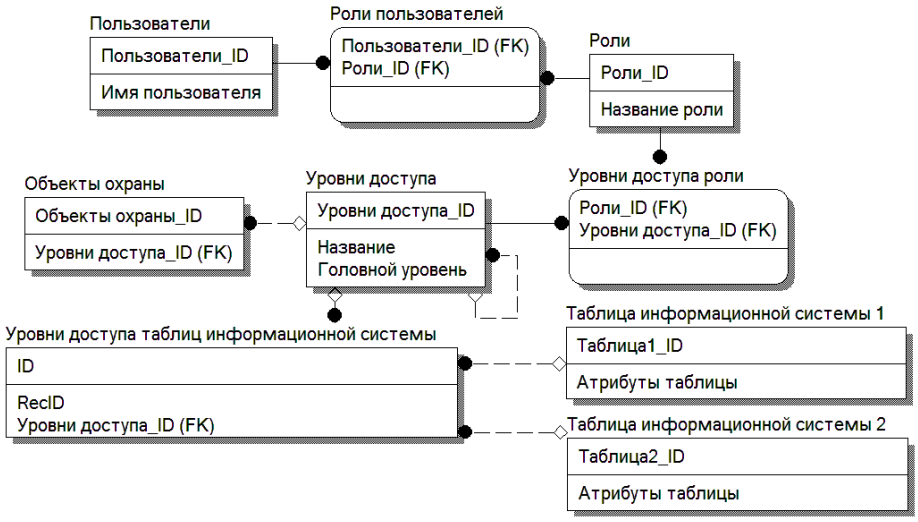


Рис. 4. Второй способ реализации защиты от НСД

Анализ вышеприведенных способов построения систем защиты от НСД показал, что при больших объемах данных второй способ реализации является более медленным. Это происходит из-за того, что информация обо всех записях, подлежащих защите, хранится в одной таблице, из-за чего доступ к ней с течением времени замедляется. Первый способ лишен данного недостатка. Кроме этого, он позволяет произвести проектирование системы с использованием внешних ключей, что положительным образом сказывается на уровне надежности данных. Поэтому для информационных систем, в которых допустимо добавление в существующие таблицы новых атрибутов, наиболее целесообразным представляется использование первого способа реализации защиты от НСД. Второй же способ реализации следует применять в случаях, когда разработанная информационная система не допускает никаких изменений в своих таблицах.

## Выводы

Проведенное исследование показало, что разработка системы защиты от несанкционированного доступа для систем, находящихся в стадии промышленной эксплуатации, вполне возможна. Предложенные в работе две принципиальные схемы построения такой системы требуют минимальной доработки уже работающих модулей информационной системы, что не приведет к нарушению их работоспособности. Таким образом, система безопасности будет представлять собой относительно независимый модуль, который можно будет внедрять в информационные системы по мере необходимости.

## Литература

[1] Базовые технологии моделирования процедур защиты информации от несанкционированного доступа / Ю.В. Соснин [и др.] // Вопросы защиты информации. 2014. № 1. С. 23–28.

[2] Утебов Д.Р., Белов С.В. Классификация угроз в системах управления базами данных // Вестник Астраханского государственного университета. 2008. № 1 (42). С. 87–92.

[3] Чичварин Н.В. Выбор методов защиты проектной документации от несанкционированного доступа // Информационные технологии. 2014. № 5. С. 41–48.

[4] Суханов А.В. Количественная оценка свойства защищенности информационных систем // Информационные технологии. 2010. № 1. С. 7–12.

[5] Кайт Т. Oracle для профессионалов. Кн. 2. Расширение возможностей и защита. 2-е изд. Киев: ООО ”ТИД ДС”, 2004. 848 с.

[6] Крутов А.Н. Построение системы защиты от несанкционированного доступа средствами СУБД Oracle // Современные информационные технологии в деятельности органов государственной власти «Информтех-2008»: материалы I Всерос. науч.-техн. конф. Курск: Курск. гос. техн. ун-т, 2008. С. 175–177.

# References

[1] Sosnin Yu.V, Kulikov G.V., Nepomnyashchikh A.V., Nashchyokin P.A. Basic technologies of modeling procedures to protect information from unauthorized access *Voprosy zashchity informatsii* [Information security systems], 1 quarter of 2014, no. 1, pp. 23–28 [in Russian].

[2] Utebov D.R., Belov S.V. Classification of threats in database management systems *Vestnik Astrahanskogo gosudarstvennogo universiteta* [Vestnik of Astrakhan State University], 2008, no. 1(42), pp. 87–92 [in Russian].

[3] Chichvarin N.V. The choice of methods of protection of the design documentation from unauthorized access. *Informatsionnye tekhnologii* [Information technologies], 2014, no. 5, pp. 41–48 [in Russian].

[4] Suhanov A.V. Quantitative evaluation of properties of the security of information systems *Informatsionnye tekhnologii* [Information technologies], 2010, no. 1, pp. 7–12 [in Russian].

[5] Kajt T. Oracle for professionals. Book 2. Empowerment and protection. Second edition. Kiev, OOO "TID"DS, 2004, 848 p. [in Russian].

[6] Krutov A.N. Building a system of protection against unauthorized access by means of DBMS Oracle *Sovremennye informatsionnye tekhnologii v deiatel'nosti organov gosudarstvennoi vlasti «Informtekh-2008»: materialy I Vseros. nauch.-tekhn. konf.; Kursk. gos. tekhn. un-t* [Modern information technologies in the activities of public authorities "Informteh 2008": materials of the 1st All-Russian scientific and national conference: Kursk State Technical University]. Kursk, 2008, pp. 175–177 [in Russian].

***A.N. Krutov***[2]

# CONSTRUCTION OF SYSTEMS OF PROTECTION FROM UNAUTHORIZED ACCESS FOR INFORMATION SYSTEMS TAMPER LOCATED IN THE INDUSTRIAL USE

The article discusses the question of construction of the systems of protection against unauthorized access to information systems that are in commercial operation. It offers two concepts of development of the system from unauthorized access with minimal modifications in the already developed information system. As a means of building an effective system of protection in the process means of careful monitoring of access database DBMS Oracle (Fine Grained Access Control) are used. Depending on the size of the source database and the possibility to modify the table structure of the information system it is offered to use one or the other method for constructing a system of protection against unauthorized access. Developed protection system is relatively independent module that can be implemented in as needed.

**Key words:** database, database management system, information systems, unauthorized access, system of protection, industrial maintenance, security model, fine grained access control.

Статья поступила в редакцию 28/ *V*/2015.

The article received 28/ *V*/2015.

[2]*Krutov Alexey Nikolaevich* (alexey.n.krutov@gmail.com), Department of Information Systems Security, Samara State University, 1, Acad. Pavlov Street, Samara, 443011, Russian Federation.