ТЕХНИЧЕСКИЕ НАУКИ
TECHNICAL SCIENCES

Научная статья
УДК 004.654
ББК 32.972.134
Р 93
DOI: 10.53598/2410-3225-2022-4-311-45-51

CRUD-модель безопасности как базовый элемент контроля и управления доступом к данным в информационных системах

(*Рецензирована*)

Александр Александрович Рыбанов

Волжский политехнический институт (филиал) Волгоградского государственного технического университета, *Волжский*, *Россия*, *rybanoff@yandex.ru*

Аннотация. *CRUD-модель является одним из способов описания взаимосвязей между процессами обработки данных и элементами данных в отношении их создания, чтения, обновления и удаления. Предлагается расширение двумерного представления CRUD-модели до трехмерной CRUD-модели безопасности путем введения дополнительного измерения, описывающего права и привилегии пользователей баз данных. Рассмотрена реализация CRUD-модели безопасности на основе технологии ROLAP. Предлагаемый подход ориентирован на процессы управления доступом в рамках технологий разработки и защиты баз данных.*

Ключевые слова: *CRUD, модель безопасности, права доступа, привилегии доступа, управление доступом*

Original Research Paper

CRUD model of security as a basic element of data access control management in information systems

Aleksandr A. Rybanov

Volzhsky Polytechnical Institute, *Branch of the Volgograd State Technical University*, *Volzhskiy*, *Russia*, *rybanoff@yandex.ru*

Abstract. *The CRUD model is one of the ways to describe the relationships between data processing and data elements with respect to their creation, reading, updating, and deletion. The article proposes expanding the two-dimensional representation of the CRUD model to a three-dimensional CRUD security model by introducing an additional dimension describing the rights and privileges of database users. The implementation of the CRUD model of security based on ROLAP technology is considered. The approach proposed in the article is focused on access control management processes within the framework of database development and protection technologies.*

Keywords: *CRUD, security model, access rights, access privileges, access control management*

Введение. Развитие технологий, прогресс и увеличение потока информации влияют также на развитие предприятий и требуют быстрых изменений в их информационных системах [1, 2]. При проектировании и реализации информационных систем разработчики должны обеспечить каждого потенциального пользователя возможностью соответствующего доступа к информации. Поскольку база данных является ядром

информационной системы [3, 4], то соответствующие спецификации прав доступа на уровне базы данных позволяют обеспечить наличие надлежащих прав доступа и в информационной системе. При разграничении доступа для каждого потенциального пользователя четко определяется список элементов базы данных и прав доступа к ним. По мере усложнения физической схемы базы данных возрастает и сложность обеспечения доступа к информации только авторизованных пользователей. В работе [5] описаны проблемы, с которыми сталкиваются администраторы информационных систем и предприятия при ротации кадров. Учитывая численность персонала предприятия и количество информации, администраторы информационных систем нуждаются в эффективных инструментах мониторинга и регулирования процесса управления доступом сотрудников предприятия к данным. Таким образом, актуальной является задача контроля управления правами доступа к данным информационной системы, которые необходимы сотрудникам предприятия для выполнения их работы.

CRUD-модель. Традиционная CRUD-модель [6–8] является одним из способов описания взаимосвязей между процессами обработки и элементами данных в отношении их создания, чтения, обновления и удаления. CRUD-модель формируется в виде таблицы, в которой в верхней части перечисляются элементы данных (поля и таблицы базы данных), а в левой части отражается список использующих их процессов базы данных (представлений, хранимых процедур и функций, триггеров, событий), ориентированных на обработку элементов данных. На рисунке 1 показан пример CRUD-модели.

Наименование процесса	Тип процесса	COUNTER	CUSTOMER	EMPLOYEE	PRODUCT	SALES_ORDER_ITEMS	SALES_ORDER
ALL_SALES_ORDER_ITEMS_DETAILS	View			R	R	R	R
ALL_PRODUCTS	View				R		
ALL_ORDERS_BY_EMPLOYEE	View						R
EMPLOYEE_COUNT	Trigger			R			
TRG_ORDER	Trigger				R		
CUSTOMERS.InsertCustomer	Procedure		C				
CUSTOMERS.UpdateCustomerName	Procedure		U				
CUSTOMERS.DeleteCustomerById	Procedure		D				
EMPLOYEES.OrdersByEmployee	Procedure		R	R		R	R
PRODUCTS.ProductsByCustomer	Procedure		R		R	R	R
PRODUCTSBYCUSTOMER	Procedure		R		R	R	R
pfc_updateprep	Event	RU					
itemchanged	Event				R		
demopfc.pbl.d_tab_customer	Datawindow Object		RU				
demopfc.pbl.d_tab_sales_order	Datawindow Object		R	R	R	R	R
demopfc.pbl.d_ff_sales_order	Datawindow Object		R	R			RU
demopfc.pbl.d_tab_employee	Datawindow Object			RU			

Доступ к полю или таблице

Процесс доступа к полю или таблице

Тип доступа (Create, Read, Update, Delete)

Рис. 1. Пример CRUD-модели

Fig. 1. Example of CRUD model

Взаимосвязи между процессами базы данных и элементами данных описываются следующими комбинациями доступа: создание (**C**reate), чтение (**R**ead), обновление (**U**pdate) или удаление (**D**elete). Таким образом, описываются все представления, хра-

нимые процедуры и функции, триггеры и события базы данных, которые выполняют создание, чтение, обновление или удаление в одном или нескольких элементах данных. В SQL этим комбинациям доступа соответствуют операторы Insert (создание записей), Select (чтение записей), Update (редактирование записей), Delete (удаление записей). Знание процессов Create, Read, Update и Delete (CRUD) помогают разработчикам баз данных, а также администраторам информационных систем на предприятиях в создании эффективных процессов манипулирования и управления данными. Как видно из приведенного выше примера, CRUD-модель представляет собой двухмерное описание взаимосвязей между процессами обработки и данными в отношении создания, чтения, обновления и удаления данных.

CRUD-модель безопасности. По мере цифровизации бизнеса все больше внимания уделяется безопасности с точки зрения индивидуальных и групповых прав доступа к данным для конкретных процессов в информационных системах. Права доступа, также называемые разрешениями или привилегиями, определяют типы доступа пользователя или группы к защищаемому объекту. Проблемы, связанные с контролем доступа, включают в себя определение и документирование соответствующих прав доступа, связанных с пользователями и группами [8].

В основу CRUD-модель безопасности положено понятие гиперкуба данных. Гиперкуб данных содержит одно или более измерений и представляет собой упорядоченный набор ячеек (рис. 2). Каждая ячейка определяется одним и только одним набором значений измерений – меток. Ячейка может содержать данные – меру или быть пустой. Под измерением будем понимать множество меток, образующих одну из граней гиперкуба.

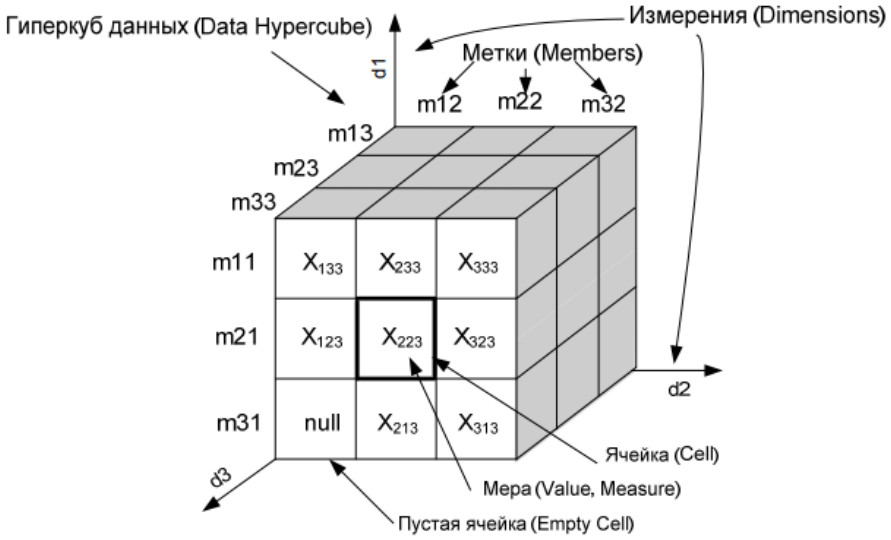

Рис. 2. Гиперкуб данных

Fig. 2. Data hypercube

Для получения доступа к данным пользователю необходимо указать одну или несколько ячеек путем выбора значений измерений, которым соответствуют необходимые ячейки. Процесс выбора значений измерений будем называть фиксацией меток, а множества выбранных значений измерений – множеством фиксированных меток.

Пусть

$D = \{d_1, d_2, \ldots, d_n\}$ – множество измерений гиперкуба;

$M_{d_i} = \{m_{1i}, m_{2i}, \ldots, m_{ki}\}$, где $i = \overline{1,n}$ – множество меток измерения d_i;

$M = M_{d_1} \cup M_{d_2} \cup \ldots \cup M_{d_n}$ – множество меток гиперкуба;

$D' \subseteq D$ – множество фиксированных измерений;

$M' \subseteq M$ – множество фиксированных меток.

Гиперкуб данных обозначим как множество ячеек $H(D,M)$, соответствующее множествам D, M. Подмножество гиперкуба данных, соответствующее множествам фиксированных значений D', M', будем обозначать как $H'(D',M')$. Каждой ячейке гиперкуба данных $h \in H$ соответствует единственно возможный набор меток измерений $M_h \subset M$. Ячейка может быть пустой (не содержать данных) или содержать значение показателя – меру. Для получения доступа к данным пользователю необходимо указать одну или несколько ячеек путем выбора значений измерений, которым соответствуют необходимые ячейки. Процесс выбора значений измерений будем называть фиксацией меток, а множества выбранных значений измерений – множеством фиксированных меток.

Предлагается расширение двумерного представления CRUD-модели до трехмерной CRUD-модели безопасности путем введения дополнительного измерения *Пользователь*, описывающего права и привилегии пользователей баз данных. Используя это измерение, системные аналитики и аналитики безопасности могут осуществлять мониторинг и документировать соответствующие права доступа для пользователей или групп к процессам обработки и данным информационной системы. Структура CRUD-модели безопасности приведена на рисунке 3.

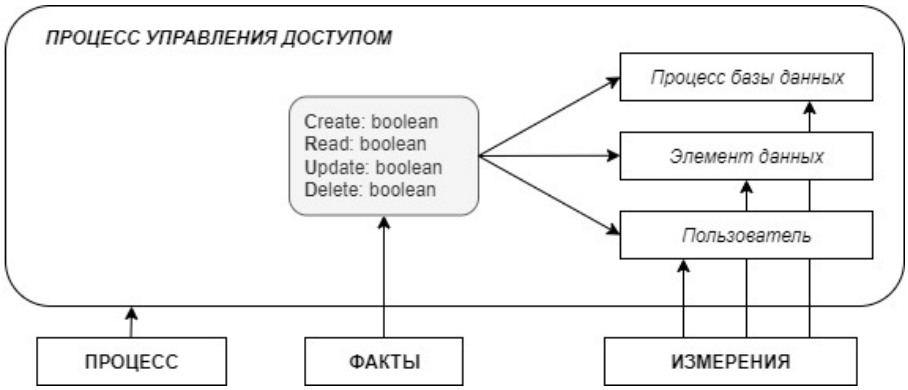

Рис. 3. Структура CRUD-модели безопасности

Fig. 3. Structure of the CRUD security model

Объектами CRUD-модели безопасности являются:

1) *Измерения* – это последовательность значений одного из анализируемых параметров процесса управления доступом. Например, для параметра «Пользователь» это список пользователей или групп, для параметра «Элемент данных» – список полей и таблиц базы данных. Каждое значение измерения может быть представлено координатой в многомерном пространстве, например (*Пользователь*, *Элемент данных*, *Процесс базы данных*);

2) *Атрибут измерения* – свойство измерения, то есть точки в пространстве. Атрибут помогает администратору базы данных полнее описать исследуемое измерение. Например, для измерения «Процесс базы данных» атрибутами могут выступить «Тип процесса» (представление, хранимая процедура, хранимая функция и т.п.), «Вычислительная сложность процесса», «Среднее время выполнения процесса»;

3) *Факт* – значение, соответствующее измерению. Факты – это данные, отражающие возможность доступа: создание (**C**reate), чтение (**R**ead), обновление (**U**pdate) или удаление (**D**elete);

4) *Ссылка на измерение* – установленная связь между двумя и более измерениями. Некоторые понятия, соответствующие измерениям, могут образовывать иерархию,

например таблицы базы данных включают записи, записи – поля. В этом случае первое измерение содержит ссылку на второе, второе – на третье и т.д.;

5) *Процесс* – совокупность измерений, фактов и атрибутов, описывающих действия по управлению доступом;

6) *Атрибут процесса* – свойство, справочное значение, относящееся к процессу.

Описанная выше структура CRUD-модели безопасности может быть реализована на основе технологии ROLAP. На рисунке 4 представлена реализация CRUD-модели безопасности в виде схемы «звезда». Но при наличии ссылок на измерения возможна реализация и в виде схемы «снежинка».

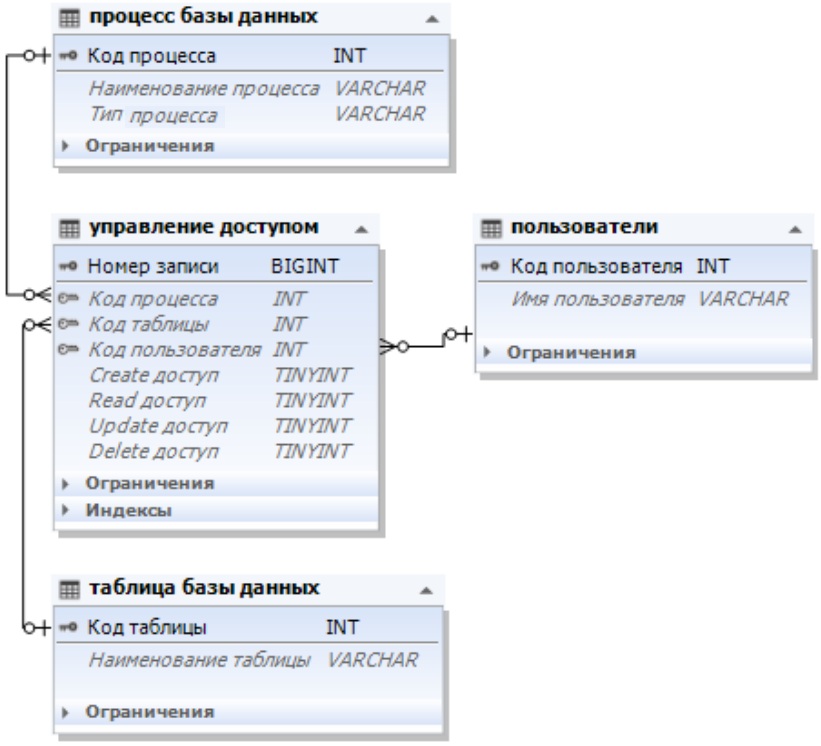

Рис. 4. CRUD-модель безопасности в виде схемы «звезда»

Fig. 4. CRUD security model in the form of a “star” scheme

При использовании схемы «звезда» центральной является таблица фактов процесса управления доступом, с которой связаны все таблицы измерений. Таким образом, информация о каждом измерении располагается в отдельной таблице, что упрощает их просмотр, а саму схему делает логически прозрачной и понятной администратору информационной системы. В целях проведения апробации была создана тестовая CRUD-модель безопасности в аналитической платформе Deductor (рис. 5).

Схема построения CRUD-модели на основе технологии ROLAP (рис. 4) позволяет использовать ряд специальных операций, к которым относятся: формирование среза, вращение, агрегация и детализация. Используя операции вращения, можно получать спецификации прав доступа с различных точек зрения:

– спецификации типов доступа пользователей к процессам базы данных, использующим элементы данных;

– спецификации типов доступа, которые пользователи имеют к элементам данных.

CRUD-модель безопасности может быть использована при разработке процессов управления доступом для приложений информационных систем, для которых вся обработка данных вынесена в объекты базы данных (представления, хранимые процедуры и

функции, триггеры, события).

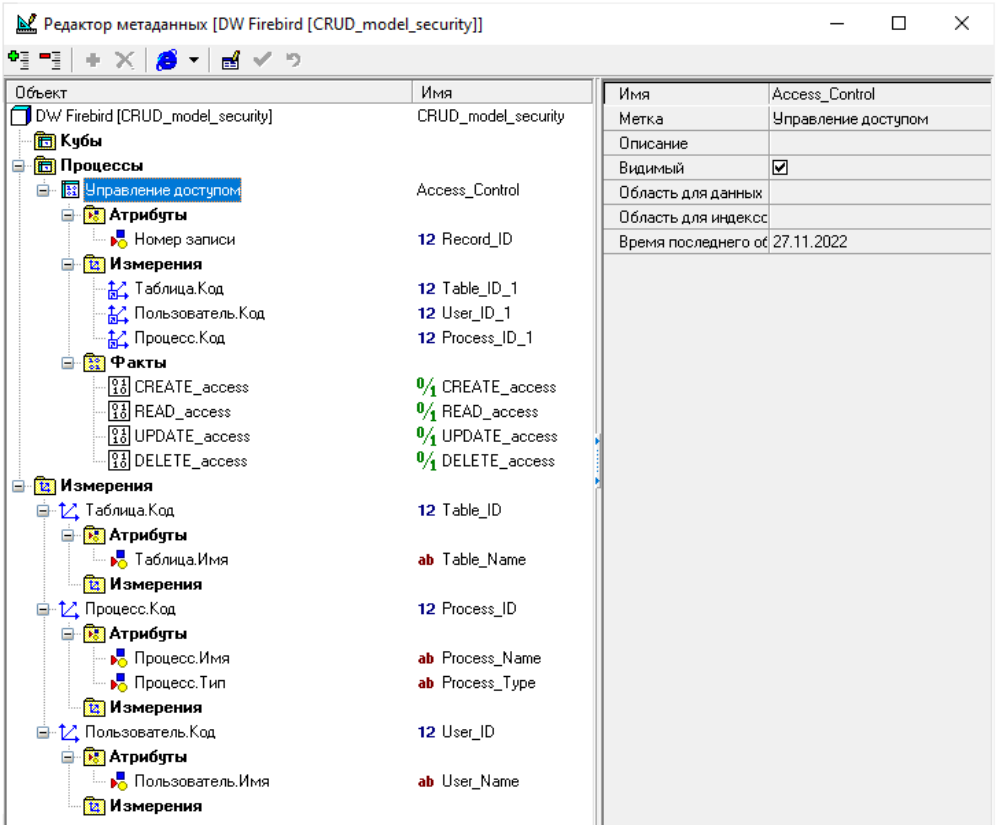

Рис. 5. Метаданные CRUD-модели безопасности в Deductor

Fig. 5. Metadata of CRUD security model in Deductor

CRUD-модель безопасности обеспечивает удобный механизм для первоначальной спецификации прав доступа. Модели системного анализа, такие как диаграммы потоков данных или сценарии использования, помогают определить роли или группы, которые выполняют пользователи в информационной системе, определяя, таким образом, типы доступа, необходимые для процессов базы данных и элементов данных. В зависимости от конкретных возможностей информационной системы или системы управления базами данных более точные спецификации типов доступа, возможно, находятся за пределами CRUD-модели.

Заключение. Применение CRUD-модели безопасности дает следующие потенциальные преимущества для определения и документирования прав доступа:

– обеспечивает возможность четкого представления прав доступа в табличном формате;

– служит для администраторов информационных систем по вопросам безопасности основой для оценки осуществления прав доступа в целях обеспечения надлежащего уровня защиты информации и системы;

– легко адаптируется к различным типам защищаемых объектов базы данных, включая поля, записи, таблицы.

Примечания

1. Poniszewska-Maranda A. Management of access control in information system based on role concept // Scalable Computing: Practice and Experience. 2011. No. 12 (1). P. 35–49.

2. Спивак С.И., Морозкин Н.Д., Лукьянов Л.А. Метаобъектный подход к моделированию бизнес-процессов предприятия в рамках единой ERP-системы // Системы и средства ин-

форматики. 2019. № 2. С. 113–121.

3. Черняев А.О., Рыбанов А.А. Разработка и исследование алгоритмов автоматизированного проектирования логических схем реляционных баз данных // В мире научных открытий. 2010. № 4-11 (10). С. 128–129.

4. Кузьмин А.А., Рыбанов А.А. Исследование методов количественной оценки схем реляционных баз данных // Успехи современного естествознания. 2011. № 7. С. 137–138.

5. Kamens M. Making user access policies work for you // Network World. 2007. No. 24 (12). P. 33.

6. Brandon D. CRUD matrices for detailed object oriented design // Journal of Computing Sciences in Colleges. 2002. No. 18 (2). P. 306–322.

7. Бажан В.Е. Применение документно-ориентированных баз данных в CRUD-приложениях // Молодежь. Наука. Инновации. 2021. № 1. С. 259–261.

8. Lunsford D.L., Collins M.R. The CRUD Security Matrix: A Technique for Documenting Access Rights // In Proceedings of the 7th Annual Security Conference. Las Vegas; New York, 2018.

References

1. Poniszewska-Maranda A. Management of access control in information system based on role concept // Scalable Computing: Practice and Experience. 2011. No. 12 (1). P. 35–49.

2. Spivak S.I., Morozkin N.D., Lukyanov L.A. Metaobject approach for modeling enterprise business processes inside single ERP system // Informatics Systems and Tools. 2019. No. 2. P. 113–121.

3. Chernyaev A.O., Rybanov A.A. Development and research of algorithms for automated design of relational databases logical schemas // In the World of Scientific Discoveries. 2010. No. 4-11 (10). P. 128–129.

4. Kuzmin A.A., Rybanov A.A. Research of quantitative methods for relational database schemes // Successes of Modern Natural Science. 2011. No. 7. P. 137–138.

5. Kamens M. Making user access policies work for you // Network World. 2007. No. 24 (12). P. 33.

6. Brandon D. CRUD matrices for detailed object oriented design // Journal of Computing Sciences in Colleges. 2002. No. 18 (2). P. 306–322.

7. Bazhan V.E. Application of document-oriented databases in CRUD-applications // Youth. Science. Innovations. 2021. No. 1. P. 259–261.

8. Lunsford D.L., Collins M.R. The CRUD Security Matrix: A Technique for Documenting Access Rights // In Proceedings of the 7th Annual Security Conference. Las Vegas; New York, 2018.

Статья поступила в редакцию 28.11.2022; *одобрена после рецензирования 15.12.2022*; *принята к публикации 16.12.2022*.

The article was submitted 28.11.2022; *approved after reviewing 15.12.2022*; *accepted for publication 16.12.2022*.