УДК 004.632
DOI 10.22213/2410-9304-2017-4-49-54

Р. Р. Юсупов, магистрант
С. В. Вологдин, доктор технических наук, доцент
ИжГТУ имени М. Т. Калашникова
А. П. Бельтюков, доктор физико-математических наук, профессор
Удмуртский государственный университет

ОРГАНИЗАЦИЯ ДОСТУПА К ДАННЫМ НА ОСНОВЕ БИНАРНЫХ ПРАВИЛ В ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЕ ТЕСТИРОВАНИЯ

В данной статье рассматривается один из уровней защиты информации, а именно модель контроля доступа к данным, в которой реализуется принцип работы системы разграничения прав на основе бинарных правил. Актуальность данной темы обосновывается в наше время необходимостью ограничения доступа к данным практически в любых системах, где имеется какая-либо организационная структура среди пользователей. Целью данной работы является повышение безопасности хранимых данных путем ограничения доступа к ним. Принцип работы системы состоит в том, что у каждого пользователя есть право или набор прав, которые определяют уровень доступа к информации для данного пользователя. Совокупность прав представляется в виде двоичного числа, где длина числа определяется количеством всевозможных прав. Для апробации этого подхода по разграничению прав была использована интеллектуальная система тестирования (ИСТ), в которой данный подход представлен как один из модулей ИСТ. Итогом всей работы является реализация алгоритма предоставления доступа к данным на основе бинарных правил, которая поможет значительно повысить уровень безопасности системы, в которой данный алгоритм будем применен. Представленный материал будет полезен для специалистов по информационной безопасности.

Ключевые слова: конфиденциальность данных, ИТ, защита данных, интеллектуальные системы, база данных, информационная безопасность.

Количество пользователей сети Интернет с каждым днем растет. По данным, изложенным в докладе ООН Global Broadband Progress [1] от 18.09.2017, количество пользователей интернета в мире составляет 3,58 миллиарда человек. С ростом числа пользователей растет и количество различных веб-ресурсов. И для каждого такого ресурса необходимо тщательно продумать политику безопасности для обеспечения защиты данных. Одним из уровней защиты в многопользовательских системах является создание модели контроля доступа. Данная модель подразумевает разграничение прав доступа пользователей к данным системы. Она определяет то, что субъекты, в нашем случае пользователи, могут выполнить с объектами системы (например, какими-либо данными системы). Разграничив области доступа, мы решаем множество проблем, например таких, как несанкционированный доступ к информации или, еще хуже, порча самой системы. Контроль доступа позволяет не только разграничить права, но и отследить, кто и в какой момент времени выполнил ту или иную операцию с объектами, т. е. позволяет вести протоколирование действий [2].

В связи с высокой актуальностью темы разграничения прав было решено разработать собственную систему доступа к данным на основе бинарных правил. И в качестве демонстрации работы данной системы рассмотрим ее применение в интеллектуальной системе тестирования.

Принцип работы системы доступа к данным на основе бинарных правил состоит в том, что у каждого пользователя есть право или набор прав, которые определяют уровень доступа к информации для данного пользователя. Совокупность прав представляется в виде двоичного числа, где длина числа определяется количеством всевозможных прав. Каждому праву выделяется один бит. Если пользователь обладает данным правом, то бит равен единице, иначе равен нулю.

Например, в системе определено 3 права: создание (первый бит), чтение (второй бит), удаление (третий бит). Имеется пользователь с двоичным кодом доступа *110*. Следовательно, пользователь обладает правами на создание и чтение, но не имеет права удалять.

Также в такую строку доступа можно добавить ограничивающее право, например черный список. Количество прав в данной системе ограничено 64 битами, что, в целом, достаточно для любой системы. Для проверки существования права, а также для изменения, добавления или удаления ее используются битовые операции. Например, возьмем вышеприведенную строку доступа *110*. Для того чтобы проверить,

обладает ли пользователь тем или иным правом, используется побитовый оператор «*И*», т. е. строка проверки пользователя на наличие права чтения будет выглядеть следующим образом: *(110) & (10),* в результате вернется число *010*, что, в свою очередь, будет подтверждать наличие права чтения.

На основании набора прав можно сформировать роли, например, если брать вышеприведенные права, а именно: чтение, создание, удаление. Всеми этими правами будет обладать пользователь с ролью администратора, а пользователь только с правом чтения будет обладать ролью, допустим, тестируемого. Количество всевозможных ролей определяется по формуле 2^n, где n – длина строки доступа (количество прав).

Рассмотрим данный вид разграничения прав относительно интеллектуальной системы тестирования. Сама система тестирования представляет собой программный комплекс в виде веб-приложения, который позволяет автоматизировать процедуры установления и измерения индивидуально-психологических отличий пользователей. Основными задачами системы являются:

1. Оценка индивидуально-психологических отличий абитуриентов при поступлении в вуз и помощь в выборе направления обучения.

1.1. Помощь в определении направления обучения в вузе (факультет, кафедра, специальность) студента, основываясь на его способностях, желаниях и эмоционально-психологической предрасположенности.

1.2. Определение прогноза успеваемости абитуриента по выбранной специальности на основании его текущих знаний и навыков к обучению.

2. Оценка индивидуально-психологических отличий студентов на протяжении обучения в вузе.

2.1. Оценка знаний студента по той или иной дисциплине.

2.2. Исследование определенных психологических качеств и свойств личности студентов и преподавателей при помощи использования психологических тестов.

Для решения поставленных задач в системе реализован адаптивный вид тестирования [3]. Удобство данного вида достигается за счет его эффективности по сравнению с традиционным видом тестирования [4]. Например, такой тип тестирования обладает возможностью определения знаний обучающегося за минимальное количество заданных вопросов. При выполнении одного и того же адаптивного теста тестируемые с высоким уровнем подготовки и тестируемые с низким уровнем подготовки увидят совершенно разные наборы вопросов: первый увидит большее число сложных вопросов, а последний – легких.

В данной системе данными, к которым необходимо разграничить доступ, являются тесты. Пользователь в системе не будет обладать одними и теми же правами ко всем тестам, т. е. относительно каждого теста пользователь будет обладать разными правами либо права могут вообще отсутствовать. Также каждая строка доступа будет иметь дату окончания действия.

В системе предусмотрены следующие права:

• *Редактирование*. Данное право включает в себя возможности создания, изменения и удаления теста. За наличие у пользователя данного права будет отвечать первый бит.

• *Чтение*. Данное право позволяет проходить данный тест. За наличие у пользователя данного права будет отвечать второй бит.

• *Просмотр результатов.* Данное право разрешает просмотр и работу с полученными данными по прохождению теста пользователями. За наличие у пользователя данного права будет отвечать третий бит.

• *Назначение прав.* Данное право позволяет назначать или изменять права других пользователей по отношению к данному тесту. За наличие у пользователя данного права будет отвечать четвертый бит.

• *Публикация*. Данное право позволяет публиковать тест для прохождения его пользователями системы. За наличие у пользователя данного права будет отвечать пятый бит.

• *Черный список*. Данное право является ограничивающим, если пользователь обладает данным правом, то происходит автоматическая блокировка других прав, а также запрещается какой-либо иной доступ к тесту. За наличие у пользователя данного права будет отвечать шестой бит.

На основе прав доступа определены типовые роли в ИСТ (см. табл. 1).

Таблица 1. **Описание ролей доступа**

Роль	Описание	Права	Строка доступа
Тестируемый	Пользователь, который имеет право только на прохождение теста	Чтение	010000
Тьютор	Пользователь, который курирует данный тест, анализирует результаты теста и консультирует тестируемых	Чтение, просмотр результатов	011000
Автор	Пользователь, который придумал данный тест	Чтение, просмотр результатов, публикация	011010
Редактор	Пользователь, который вводит новый тест в систему и следит за его состоянием	Редактирование, чтение, публикация	110010
Администратор	Пользователь, обладающий полными правами на тест	Редактирование, чтение, просмотр результатов, назначение прав, публикация	111110
Заблокированный	Пользователь, которому полностью закрыт доступ к тесту, даже при наличии других прав	Любые права, черный список	*****1

Данный список ролей является не окончательным, он может быть расширен или изменен администратором системы в соответствии с частными требованиями к системе.

Доступ к данным тестов предоставляется только зарегистрированным пользователям. В настоящее время в системе тестирования предусмотрено два вида тестов:

• открытые (тесты, доступ к которым (на правах чтения) имеют все зарегистрированные пользователи, не входящие в черный список по отношению к проходимому тесту);

• закрытые (тесты, для доступа к которым обязательно наличие прав к проходимому тесту, кроме черного списка).

Для реализации данного подхода было создано 4 таблицы базы данных (БД) с помощью СУБД MySQL [5]:

• таблица «Users» – информация о пользователях системы, а также данные для авторизации (см. табл. 2);

• таблица «Test» – содержит информацию о созданных тестах (см. табл. 3);

• таблица «Access» – хранит информацию об уровни доступа пользователя к определенным тестам (см. табл. 4);

• таблица «UserGroup» – справочная таблица, хранит информацию о ролях (см. табл. 5).

Таблица 2. **Описание полей таблицы «Users»**

Наименование поля	Тип поля	Описание
id	int	Идентификатор пользователя. Поле является ключевым и автоинкрементным.
name	varchar	Имя пользователя
login	varchar	Логин пользователя для авторизации в системе
pass	varchar	Хэш пароля пользователя

Таблица 3. **Описание полей таблицы «Test»**

Наименование поля	Тип поля	Описание
id	int	Идентификатор теста. Поле является ключевым и автоинкрементным.
id_category	int	Идентификатор категории, в котором находится тест
title	varchar	Название теста
text	text	Описание теста
date	date	Дата создания теста
status	tinyint	Определяет статус теста, т. е. опубликованный или черновой
weight	int	Определяет значимость теста относительно других тестов
id_first_TB	int	Идентификатор первого тестового блока
limit_access	tinyint	Флаг, определяющий открытый или закрытый тест

Таблица 4. **Описание полей таблицы «Access»**

Наименование поля	Тип поля	Описание
id	int	Идентификатор уровня доступа. Поле является ключевым и автоинкрементным
id_user	int	Идентификатор пользователя
id_test	int	Идентификатор теста
code_access	bit	Строка доступа к тесту
date	date	Срок окончания действия прав пользователя

Таблица 5. **Описание полей таблицы «UserGroup»**

Наименование поля	Тип поля	Описание
id	int	Идентификатор роли. Поле является ключевым и автоинкрементным
name	varchar	Наименование роли
code_access	bit	Строка доступа к тесту

Взаимосвязь расмотренных таблиц БД представлена на рис. 1.

Рассмотрим алгоритм доступа к данным теста (см. рис. 2).

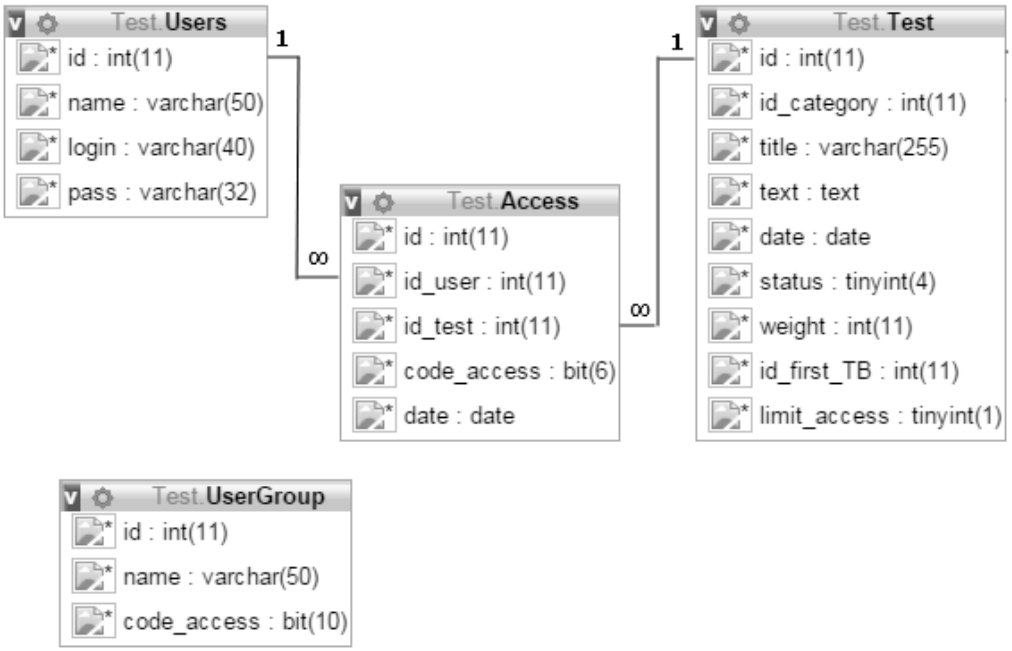

Рис. 1. Структура БД

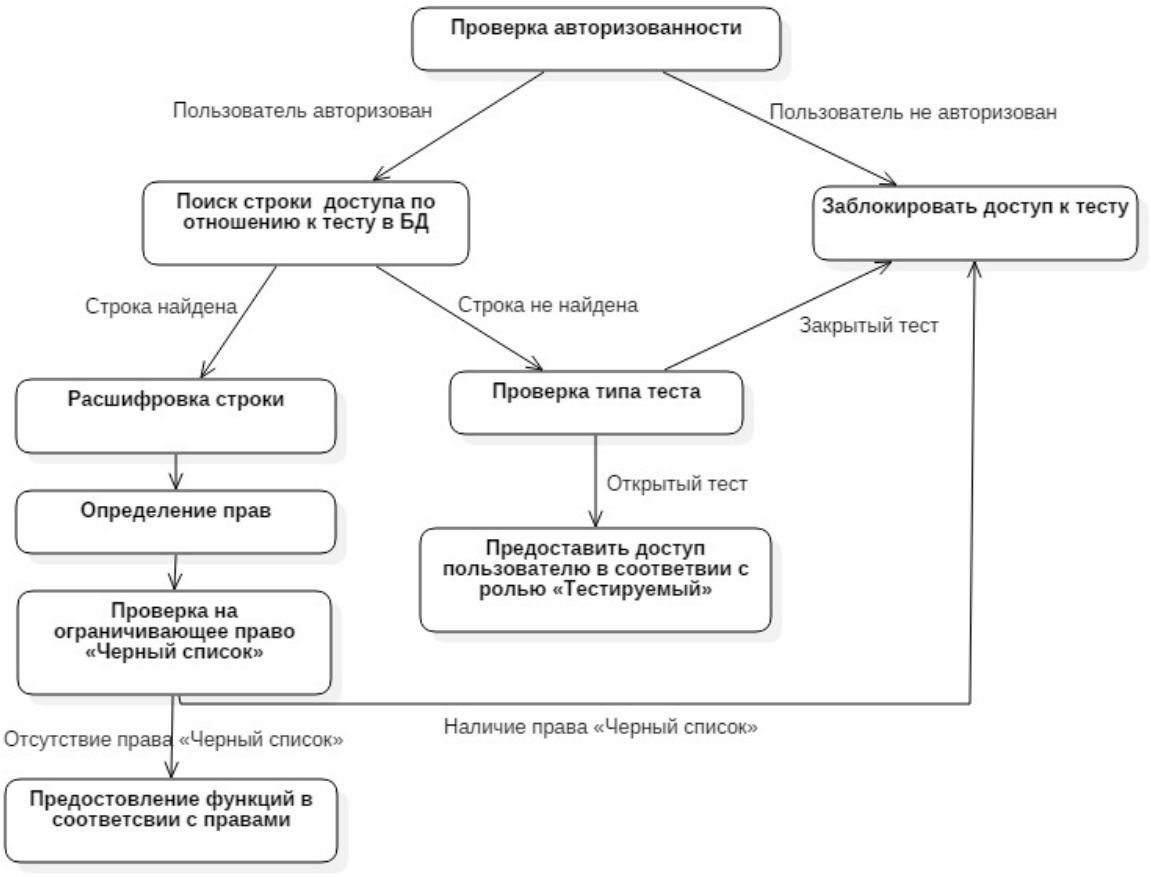

Рис. 2. Алгоритм доступа к данным теста

На первом этапе осуществляется проверка авторизованности. Для доступа к тесту необходима будет обязательная регистрация и авторизация в системе, поэтому первоначально система будет определять зарегистрирован ли и авторизован ли пользователь в системе. В случае авторизованности сохраняет в сессии id пользователя и переходит к следующему этапу, иначе блокирует доступ к тесту.

Второй этап: поиск строки доступа по отношению к тесту в БД. На данном этапе система при помощи SQL [6] запроса, в котором передает id пользователя и id теста, запрашивает из БД информацию о наличии строки доступа к тесту. В случае отсутствия строки доступа система проверяет тест на открытость, т. е. имеет ли тест пометку ОТКрытый. Если тест открыт, то предоставляется доступ пользователю в соответствии с ролью «Тестируемый». Если строка найдена, то система переходит к следующему шагу.

Третий этап: расшифровка строки. Полученная строка доступа из БД расшифровывается согласно вышеописанной схеме и определяет права пользователя. Далее, если пользователь имеет право «Черный список», то система блокирует доступ к данным теста, иначе предоставляет доступ в соответствии с правами.

Рассмотрев работу системы доступа к данным на основе бинарных правил в интеллектуальной системе тестирования, можно выделить ее основные преимущества:

• малый объем информации, хранимый в БД, для обеспечения работы системы;

• возможность создания большого количества прав и генерации на основе комбинаций из этих прав ролей;

• за счет довольно простого алгоритма и малого количества действий с данными достигается высокая скорость работы.

Необходимо отметить, что представленный подход к разграничению прав соответствует современным требованиям в области защиты данных. В дальнейшей работе планируется совершенствовать работу ИСТ путем наращивания функциональных возможностей системы, создания эргономичного интерфейса.

Библиографические ссылки

1. The state of broadband 2017: broadband catalyzing sustainable development // International Telecommunication Union (ITU). 2017. URL: https:// www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROAD-BAND.18-2017-PDF-E.pdf (дата обращения: 12.10.2017).

2. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учеб. пособие для вузов. М. : Горячая линия – Телеком, 2013. 338 с.

3. *Аванесов В. С.* Форма тестовых заданий : учеб. пособие. 2-е изд. М. : Центр тестирования, 2005. 155 с.

4. *Дружинина Е. В., Вологдин С. В.* Разработка руководства пользователя информационной системы тестирования школьников // Вестник ИжГТУ имени М. Т. Калашникова. 2015. № 2. С. 86–87.

5. *Sheeri K. Cabral, Keith Murphy*. MySQL Administrator's Bible. Indianapolis: Wiley Publishing, 2009. 888 c.

6. Beaulieu Alan. Learning SQL. Sebastopol: O'Reilly Media, 2009. 312 c.

References

1. The state of broadband 2017: broadband catalyzing sustainable development // International Telecommunication Union (ITU). 2017. availale at https:// www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROAD-BAND.18-2017-PDF-E.pdf (accessed October 12, 2017).

2. Devyanin P. N. (2013). *Modeli bezopasnosti komp'yuternykh sistem. Upravlenie dostupom i informatsionnymi potokami* [Models of security of computer systems. Management of access and information flows]. Moscow: Goryachaya liniya – Telekom. 338 p. (in Russ.).

3. Avanesov V. S. (2005). *Forma testovykh zadanii* [Form of test tasks]. Moscow: Tsentr testirovaniya. 155 p. (in Russ.).

4. Druzhinina E. V., Vologdin S. V. (2015). *Vestnik IzhGTU imeni M. T. Kalashnikova* [Bulletin of Kalashnikov ISTU], no. 2, pp. 86-87 (in Russ.).

5. *Sheeri K. Cabral, Keith Murphy*. MySQL Administrator's Bible. Indianapolis: Wiley Publishing, 2009. 888 c.

6. Beaulieu Alan. Learning SQL. Sebastopol: O'Reilly Media, 2009. 312 c.

* * *

R. R. Yusupov, Master's Degree Student, Kalashnikov ISTU
S. V. Vologdin, DSc in Engineering, Professor, Kalashnikov ISTU
A. P. Beltyukov, DSc (Physics and Mathematics), Professor, Udmurt State University

Organization of Data Access Based on Binary Rules in an Intelligent Testing System

In this paper, we consider one of the levels of information security, namely the data access control model, which implements the principle of the system of delineation of rights based on binary rules. Nowadays the relevance of this topic is justified because of

need to restrict access to data in any virtually system where there is any organizational structure among users. The purpose of this work is to improve the security of stored data by limiting access to it. The principle of the system is that each user has a right or set of rights that determine the level of access to information for the user. The set of rights is represented in the form of a binary number, where the length of the number is determined by the number of all possible rights. To test this approach for delineation of rights, an intelligent testing system (ITS) was used, in which this approach is presented as one of the ITS modules. The final result of this work is the implementation of the algorithm for providing access to data based on binary rules, which will help to increase the level of security of the system, in which this algorithm will be applied. The presented material will be useful for information security specialists.

Keywords: data confidentiality, IT, data protection, intelligent systems, database, information security.

Получено: 20.10.17