УДК 004.056.53

Разработка системы аутентификации для автоматизированной информационной системы «Кафедра»

Архипов Владислав Русланович
Камчатский государственный технический университет
Студент

Аннотация
В статье предлагается теоретический материал по возможности использования системы аутентификации пользователей в автоматизированной информационной системе «Кафедра» (АИС «Кафедра»). Приведены способы и методы аутентификации. Произведен выбор хеш-функции, планируемой для использования.
Ключевые слова: аутентификация, безопасность, конфиденциальная информация, хеш, хеш-функция.

Development of authentication system for automated information system "Department"

Arhipov Vladislav Ruslanovich
Kamchatka State Technical University
Student

Abstract
The article proposes theoretical material on the possibility of using the user authentication system in the automated information system "Department" (AIS "Department"). Ways and methods of authentication are given. The hash function planned for use has been selected.
Keywords: authentication, security, confidential information, hash, hash function.

Введение

Стабильность работы любой автоматизированной информационной системы (АИС) в основном зависит от ее защищенности перед внешними и внутренними угрозами. Современные АИС разрабатываются с многоуровневой защитой, которая для каждой АИС подбирается индивидуально, учитывая специфику данной системы.

Методы и способы обеспечения безопасности направлены на защиту отдельных компонентов АИС. Они подразделяются на программные, аппаратные, программно-аппаратные, физические, правовые и организационные [1]. В данной статье речь пойдет о программных методах защиты, в частности о системе аутентификации, и применении этого подхода в АИС «Кафедра», разработанной для ФИТЭУ ФГБОУ ВО «КамчатГТУ».

Аутентификация пользователей

Необходимость в ограничении доступа к информации вызвана тем, что часть её является конфиденциальной, например, номера телефонов или результаты успеваемости студентов, преподавателей.

Существует множество методов аутентификации. Основными из них являются аутентификация по паролю, электронной подписи, флеш-карте, биометрическим данным и местоположению.

Так же этот процесс разделяют по количеству используемых методов аутентификации:

- однофакторная;
- двухфакторная;
- многофакторная.

В первом используется только один метод, например, пароль. Во втором – два, это может быть пароль и отпечаток пальца. Соответственно последний способ включает в себя два или более методов аутентификации [2].

В АИС «Кафедра» за процедуру аутентификации отвечает специальный модуль регистрации пользователей. В данной системе каждый пользователь имеет свой логин и пароль, которые известны только ему. Перед началом работы каждый пользователь должен пройти регистрацию в системе – ввести логин и пароль. После этого администратор предоставляет ему определённый доступ к системе. Регистрационные данные каждого пользователя хранятся в базе данных (Рисунок 1). Но пароли хранятся не в открытом виде, так как при взломе базы данных они будут скомпрометированы, а в виде хеш-значений (хешей). Хеш (hash - с англ. «мешанина») — это результат выполнения хеш-функции, которая осуществляет преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины. Особенность хеша заключается в том, что исходные данные из него получить практически невозможно.

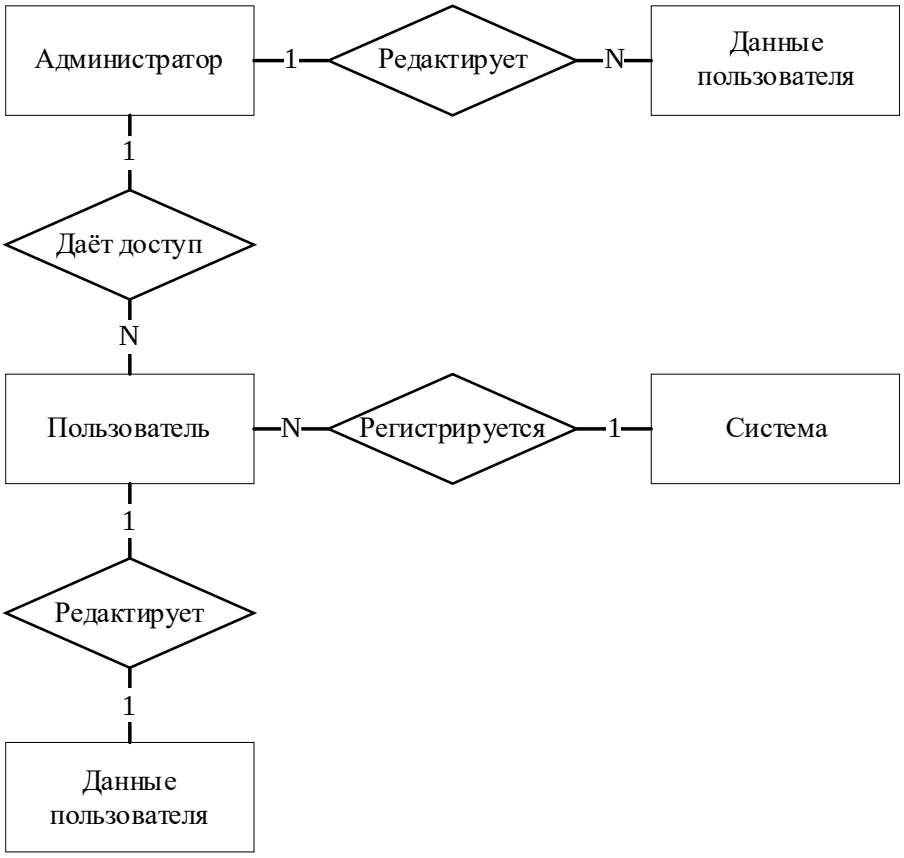

Рисунок 1 – ER-диаграмма системы регистрации

Блок регистрации пользователя

Для начала работы с системой пользователю необходимо зарегистрироваться в системе введя такие регистрационные данные, как логин, пароль, ФИО, номер телефона, адрес электронной почты и дополнительные сведения о себе. Эти данные сохраняются в базе данных в таблице «users» (Таблица 1).

Таблица 1 – Физическая модель таблицы «users»

Наименование поля	Назначение поля	Ключ	Тип поля		Ограничение
			Тип данных	Размер	
id_user	Идентификатор пользователя	*	smallint	5	>0
login	Логин пользователя		varchar	20	≠NULL
password	Хеш пароля пользователя		varchar	255	≠NULL
username	ФИО пользователя		varchar	100	
email	Электронная почта пользователя		varchar	100	≠NULL

phone	Номер телефона пользователя		varchar	25	
note	Заметка о пользователе		varchar	255	
access	Уровень доступа пользователя		char	3	
date	Дата регистрации пользователя		datetime	8	
ip	Ip-адрес пользователя		varchar	16	≠NULL
hash	Идентификатор сессии		varchar	255	≠NULL
timestamp	Дата последнего изменения данных пользователя		timestamp	4	

Блок авторизации пользователя

После регистрации в системе и получения доступа от администратора пользователь может войти в систему через специальные блок авторизации, введя свои логин и пароль.

Блок изменения данных пользователя

После успешного входа в систему пользователь может помимо работы с подсистемами АИС «Кафедра» изменить свои регистрационные данные (кроме логина).

Если пользователь является администратором, то он может менять как свои данные, так и данные другого пользователя, найдя его по логину.

Аутентификация в АИС «Кафедра»

Ранее для хеширования паролей использовался алгоритм хешировани MD5. На данный момент в нём были найдены коллизии (совпадения результатов для разных входных данных), поэтому он является небезопасным. На основе этого принято решение изменить алгоритм хеширования паролей в библиотеке.

В качестве замены выступил алгоритм хеширования bcrypt, который рекомендуется к использованию в документации языка программирования PHP. Изменение алгоритма потребует смены паролей всех пользователей системы для обеспечения их безопасности.

Для реализации этого используются функции языка PHP «password_hash» и «password_verify». Первая формирует хеш на основе полученной строки, которая содержит пароль пользователя. Вторая проверяет соответствует ли введённый пароль пользователя хешу, хранящемуся в базе данных [3].

Во время регистрации пользователь вводит все необходимые данные, которые затем записываются в базе данных в таблице «users» (Таблица 1).

Заключение

Таким образом, обеспечение безопасности пользователей АИС «Кафедра» является важной задачей при разработке системы. А использование современных методов защиты информации — это неотъемлемая часть данной задачи. Поэтому изменение алгоритма хеширования необходимо для обеспечения стабильной работы системы.

Библиографический список

1. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос, ПБОЮЛ Н.А. Егоров, 2001. 264 с.
2. Скородумов А.В. Многофакторная аутентификация – лучше меньше, да лучше: // Журнал "Information Security/ Информационная безопасность" #6, 2015. URL: https://lib.itsec.ru/articles2/Oborandteh/mnogofaktornaya-autentifikatsiya-luchshe-menshe--da-luchshe (Дата обращения: 27.06.2023)
3. Официальный сайт скриптового языка PHP. URL: https://www.php.net (Дата обращения: 27.06.2023).