ЕДИНАЯ ТОЧКА ВХОДА В ЛИЧНЫЙ КАБИНЕТ

А.В. Билевич, *студент*
Научный руководитель: *Л.В. Макуха, старший преподаватель*
Сибирский федеральный университет
(Россия, г. Красноярск)

DOI:10.24412/2500-1000-2023-5-1-50-53

Аннотация. *При использовании нескольких ресурсов для одной организации встает вопрос эффективности администрирования и управления ими, ведь использование отдельных баз данных для каждого ресурса не оптимально и неудобно как для клиентов, так и для администраторов. Поэтому данная статья посвящена проектированию и реализации схемы, где процесс аутентификации каждого из ресурсов осуществляется через LDAP-сервер. Благодаря разработанной схеме, данные пользователя хранятся в одной базе и управляются едино, унифицированность схемы позволяет добавлять неограниченное количество новых ресурсов, а объем работы для администраторов уменьшился пропорционально количеству веб-ресурсов.*

Ключевые слова: *LDAP, веб-ресурс, аутентификация, учетная запись, пользователь, обмен данными, авторизация, личный кабинет.*

В связи с развитием технологий, большинство образовательных учреждений стремится к информатизации образования, предпочитая планировать, организовывать и контролировать учебный процесс, интегрированный с электронными ресурсами, в замену тому, чтобы использовать методы, связанные с бумажным носителем. В связи с множеством ресурсов, поднимается вопрос эффективности управления безопасностью и контроля учетных записей. В результате анализа текущей IT-инфраструктуры ФБГОУ ВО «Красноярский государственный аграрный университет», стало известно, что используется множество ресурсов, доступ к которым независим между собой и пользователь вынужден регулярно проходить аутентификацию на каждом из них, то есть для каждого пользователя существует несколько несвязанных с собой учетных записей. В связи с этим, помимо того, что пользователь должен помнить логин и пароль от каждого ресурса для получения доступа к своей учетной записи, зачастую используются простые данные для ввода и запоминания. В результате этого, аккаунт становится уязвимым к атакам, и заполучить данные пользователя не составляет большого труда. Также использование нескольких учетных записей может повлечь за собой противоречивость данных.

Помимо неудобств со стороны пользователя ресурса, такая схема неудобна и для администрирования. Так, при зачислении студента, учетные записи создаются администратором для каждого ресурса отдельно, а регистрация на них для нового пользователя недоступна в соответствии с требованиями к ресурсам. В таком случае объем работы увеличивается пропорционально количеству веб-ресурсов, учетную запись для которых необходимо добавить. Также, безопасностью для каждого ресурса необходимо управлять отдельно, что является минусом такой организации хранения данных пользователей. Поэтому решение вышеописанных проблем является актуальным, решить которые можно с помощью создания единой точки входа.

В настоящий момент функционируют следующие площадки, для которых, планируется объединить учетные записи студента, а именно веб-клиент электронной почты от RoundCube доступная по адресу mail.kgau.ru, электронная информационно-образовательная среда на базе 3KL Русский Moodle доступная по адресу e. kgau.ru и внутренний портал КрасГАУ, личный кабинет студента на базе

1С:Предприятие доступный по адресу portal.kgau.ru.

Одним из способов решения поставленной проблемы является изменение схемы аутентификации с использованием клиент-серверного протокола доступа к каталогам – LDAP [1], благодаря которому администрирование и управление веб ресурсами станет эффективнее и удобнее, так как он более ориентирован для настройки аутентификации, сравнения и управления учетными записями.

Текущая схема аутентификации для студента выглядит следующим образом, указанном на рисунке 1, а схема администрирования указана на рисунке 2.

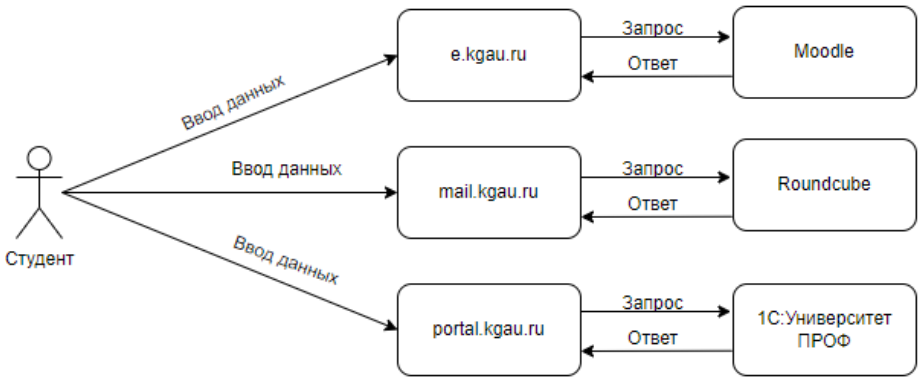

Рис. 1. Схема входа в личный кабинет

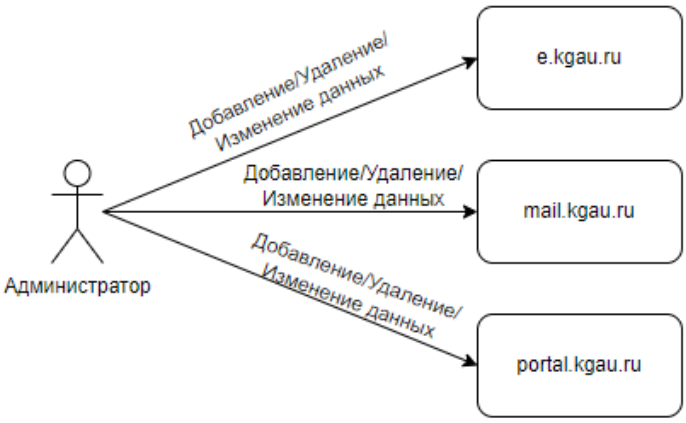

Рис. 2. Схема администрирования учетных записей

Измененная схема аутентификации, составленная с учетом проведенного анализа указана на рисунке 3.

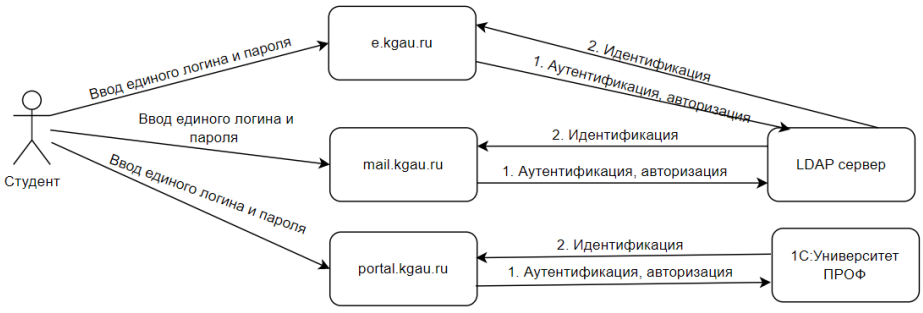

Рис. 3. Измененная схема входа в личный кабинет

Для реализации такой схемы в качестве LDAP-сервера было решено использовать специализированный дистрибутив, базирующийся на Linux – Zentyal 7.0, так как он написан для решения подобных задач и содержит в себе необходимый пакет серверного программного обеспечения, в который также входит встроенный модуль управления LDAP [2].

После развертывания и настройки, LDAP-сервер был интегрирован с системой Moddle и почтой. Это было сделано с помощью указания адреса сервера, проведения минимальных настроек и сопоставления необходимых атрибутов для работы процесса идентификации.

Для управления учетными записями портала, используется модуль «Управление ЭИОС» внутри системы 1С:Университет ПРОФ [3]. Помимо того, что данный модуль отвечает за выполнение входа в аккаунт на portal.kgau.ru, дописанные процедуры позволяют вносить изменения пользователей для LDAP-сервера в ту же форму, что используется для управления учетными записями портала. Таким образом, после внесения изменений, данные с единой формы используются как для портала, так и в процессе обмена данными с LDAP-сервером. В обмене с LDAP-сервером участвуют следующие данные: ФИО, адрес почты, логин, пароль и группа доступа. После передачи данных LDAP-серверу, он формирует запрос на внесение данных в базах Moodle и почты. Такой алгоритм используется при администрировании, упрощая этот процесс и уменьшая объем выполняемой работы по сравнению предыдущим используемым алгоритмом. Также, каждый из ресурсов имеет свою внутреннюю базу, однако ранее она использовалась для аутентификации, авторизации, и идентификации пользователя, но в измененной схеме, внутренняя база служит только для их идентификации.

В соответствии с данной схемой, при попытке входа в аккаунт, выбранный ресурс обратится к LDAP-серверу с целью проверить соответствие логина и пароля в базе данных и при успешной аутентификации, следующим шагом является авторизация, то есть определение прав пользователя. После чего сервер возвращает токен веб-ресурсу, далее с использованием внутренней базы данных происходит идентификация и выполняется вход в аккаунт. Данный алгоритм применим к ресурсам почты и электронно-образовательных курсов.

При попытке входа в аккаунт на портале, процессы аутентификации, авторизации и идентификации будут происходить с помощью 1С:Университет ПРОФ, т.к. обращение к LDAP не имеет смысла, в связи с тем, что база 1С:Университет ПРОФ является центром управления учетным записями.

После изменения схемы входа в личный кабинет, администратору для внесения изменений данных пользователей, достаточно изменить данные только в системе 1С:Университет ПРОФ, после чего изменения будут применены для всех веб-ресурсов.

Таким образом, благодаря изменению схемы, хоть и для обычного пользователя ничего не изменилось, кроме использования единого логина и пароля, для администратора объем работы уменьшился в три раза, а все данные пользователя хранятся в одной базе и управляются едино. Это также несет в себе ряд преимуществ для системы, такие как эффективность контроля, уменьшение избыточности и исключение противоречивости данных, а также прозрачность расположения. Более того, текущая схема входа в личный кабинет унифицирована и позволяет добавлять другие веб-ресурсы, которые также будут использовать базу 1С:Университет ПРОФ для управления учетными записями, а процесс входа и управление учетными записями будет аналогичным как для moddle и почты.

Библиографический список

1. Понятие и обзор LDAP // Интернет-проект Pro-LDAP.ru. – 2009. – [Электронный ресурс]. – Режим доступа: https://pro-ldap.ru/tr/zytrax/ch2/ (дата обращения: 24.03.2023).

2. Zentyal 7.0 // Официальная документация zentyal.org. – 2021. – [Электронный ресурс]. – Режим доступа: https://doc.zentyal.org/es/ (дата обращения: 24.03.2023).

3. Отраслевые и специализированные решения 1С: Предприятие // «Создание ЭИОС вуза на платформе «1С: Предприятие». – 2023. – [Электронный ресурс]. – Режим доступа: https://solutions.1c.ru/news/975899/(дата обращения: 29.03.2023).

SINGLE POINT OF ENTRANCE TO PERSONAL ACCOUNT

A.V. Bilevich, *Student*
Supervisor: *L.V. Makukha, Senior Lecturer*
Siberian Federal University
(Russia, Krasnoyarsk)

Abstract. *When using several resources for one organization, the question arises of the effectiveness of administration and management, because the use of separate databases for each resource is not optimal and inconvenient for both clients and administrators. Therefore, this article is devoted to the design and implementation of a scheme where the authentication process for each of the resources is carried out through an LDAP server. Thanks to the developed scheme, user data is stored in one database and managed unified, the unification of the scheme allows you to add an unlimited number of new resources, and the amount of work for administrators has decreased in proportion to the number of web resources.*

Keywords: *LDAP, web resource, authentication, account, user, data exchange, authorization, personal account.*