ВНЕДРЕНИЕ ЕДИНОЙ СИСТЕМЫ АВТОРИЗАЦИИ В ОБРАЗОВАТЕЛЬНУЮ ЭКОСИСТЕМУ: ИНТЕГРАЦИЯ И БЕЗОПАСНОСТЬ

Сайидов Фарух Асатуллоевич
Министерства высшего образования, науки и инноваций Управление внедрения и цифровизации информационно-коммуникационных технологий, ведущий специалист
(Тел.: (71) 55-520-08-08 (209) e-mail: f.sayidov@edu.uz)
Саитов Шукрулло Лутфулло угли
Министерства высшего образования, науки и инноваций Управление внедрения и цифровизации информационно-коммуникационных технологий, главный специалист
(Тел.: (71) 55-520-08-08 (209), e-mail: sh.saitov@edu.uz)
Пирманов Охунжон Бахриддин угли
Министерства высшего образования, науки и инноваций Управление внедрения и цифровизации информационно-коммуникационных технологий, главный специалист
(Тел.: (71) 55-520-08-08 (210) e-mail: o.pirmanov@edu.uz)
Носиров Хуршед Абдираймович
Министерства высшего образования, науки и инноваций Управление внедрения и цифровизации информационно-коммуникационных технологий, ведущий специалист
(Тел.: (71) 55-520-08-08 (210) e-mail: x.nosirov@edu.uz
https://doi.org/10.5281/zenodo.10644094

ARTICLE INFO
Qabul qilindi: 01-February 2024 yil
Ma'qullandi: 05- February 2023 yil
Nashr qilindi: 10- February 2023 yil
KEY WORDS
Единая система авторизации, образовательная экосистема, безопасность данных, Single Sign-On, интеграция образовательных платформ, цифровизация образования, управление доступом, конфиденциальность информации, удобство пользователя, межплатформенное взаимодействие.

ABSTRACT
Статья посвящена разработке и внедрению единой системы авторизации в образовательную экосистему, что включает в себя создание безопасного и удобного доступа к различным образовательным ресурсам для студентов, преподавателей и административного персонала. Основное внимание уделяется обеспечению безопасности данных, упрощению процесса взаимодействия между различными платформами и сервисами, а также рассматриваются вызовы и решения, связанные с интеграцией такой системы. Это направлено на повышение эффективности управления образовательными процессами и улучшение пользовательского опыта.

Введение

Современные образовательные экосистемы стремятся к созданию унифицированных и взаимосвязанных сред, которые облегчают доступ к

образовательным ресурсам и услугам. Единая система авторизации является ключевым элементом такой экосистемы, позволяя участникам образовательного процесса использовать одни и те же учетные данные для доступа к разнообразным ресурсам и сервисам.

Основная часть

Что представляет собой технология Single Sign-On?

Технология Single Sign-On (SSO) - это метод аутентификации, который позволяет пользователю входить в несколько приложений и веб-сайтов с использованием единого набора учетных данных.

Принцип работы SSO

SSO работает на основе создания доверительных отношений между приложением-провайдером услуг и системой управления доступом, например, One ID, с использованием обмена сертификатами для подтверждения идентификации пользователя. В SSO идентификационная информация представлена в виде токенов, содержащих данные о пользователе, такие как email или имя пользователя.

Процесс аутентификации обычно включает следующие шаги:

1. Пользователь заходит на веб-сайт или в приложение.
2. Приложение отправляет запрос на аутентификацию с информацией о пользователе в систему SSO.
3. Система SSO проверяет, был ли пользователь уже аутентифицирован. Если да, доступ предоставляется немедленно.
4. В противном случае, пользователю необходимо пройти аутентификацию.
5. После успешной аутентификации система SSO отправляет токен обратно приложению.
6. Приложение проверяет токен и предоставляет доступ пользователю. (Рисунок 1.)

Рисунок 1. Структура процесса аутентификации

Токен в контексте SSO

В контексте Single Sign-On (SSO), токен служит средством передачи проверенной информации о пользователе между системами. Этот элемент содержит данные, такие как ПИНФЛ пользователя и информацию о системе-источнике токена. Для обеспечения доверия к токену со стороны принимающей системы, он оснащается цифровой подписью. Такая подпись гарантирует, что токен был выдан надежным источником, и подтверждается при помощи сертификата, выданного в процессе первичной настройки системы. (Рисунок 2.)

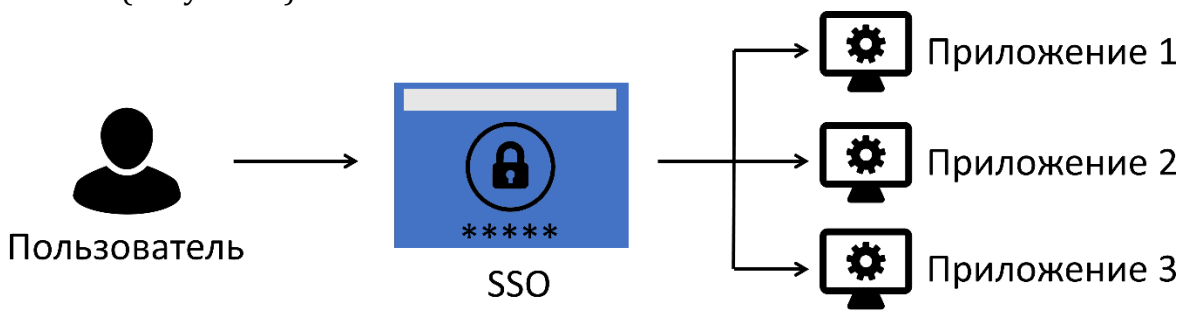

Рисунок 2. Структура единой авторизации к приложениям.

Безопасность SSO

Безопасность технологии Single Sign-On (SSO) зависит от множества факторов и контекста ее использования. SSO обладает рядом преимуществ, которые делают ее привлекательной для внедрения. Эта технология упрощает управление учетными записями, позволяя пользователям запомнить лишь один сложный пароль вместо множества разных. Это значительно ускоряет доступ к нужным приложениям и сервисам, сокращает время на восстановление забытых паролей и позволяет

администраторам более эффективно управлять политиками безопасности, такими как сложность пароля и многофакторная аутентификация.

С другой стороны, SSO может повысить риски безопасности, так как единственные учетные данные становятся "ключом" ко всем приложениям и сервисам. В случае компрометации этого единственного набора данных, злоумышленник получит доступ ко всей системе. Поэтому крайне важно выбрать решение SSO, которое предусматривает дополнительные меры безопасности, такие как двухфакторная аутентификация и защищенные соединения.

Внедрение SSO

Реализация SSO требует тщательного планирования и ответов на ключевые вопросы: кто являются пользователями системы, какие у них потребности, какое решение подходит лучше - локальное или облачное, какие функции безопасности необходимы, с какими системами должна быть интеграция и требуется ли доступ к API. Также важно разграничивать SSO и менеджеры паролей. В то время как менеджеры паролей просто хранят и автоматически вводят учетные данные для различных сервисов, SSO обеспечивает бесперебойный доступ ко всем системам после однократной аутентификации, устанавливая доверительные отношения между различными приложениями и сервисами.

В чем разница между программным обеспечением единого входа и решением SSO?

При изучении различных опций технологии единого входа (SSO) вы можете столкнуться с разными терминами, такими как "программное обеспечение SSO", "решение SSO" или "провайдер SSO". Эти различия зачастую обусловлены маркетинговым позиционированием компаний. Термин "программное обеспечение" обычно подразумевает решение, предназначенное для установки и использования в локальной среде, разработанное для выполнения специфического набора функций. В отличие от этого, "программный продукт" подразумевает более гибкое решение с возможностями настройки и масштабирования для адаптации к различным потребностям. Обращение к "провайдеру" означает выбор компании, которая предлагает или использует программный продукт, как, например, One ID, который является поставщиком услуг SSO.

Типы SSO

Существуют различные типы технологий единого входа (SSO), каждый из которых предназначен для решения определенных задач в контексте аутентификации и управления идентификационными данными. Некоторые из наиболее распространенных типов SSO включают:

Federated Identity Management (FIM): Этот подход позволяет создавать доверительные отношения между различными доменами или системами, обеспечивая пользователю возможность использовать одни и те же учетные данные для доступа к ресурсам во всех этих системах.

OAuth: Протокол открытой авторизации, который позволяет приложениям безопасно делегировать доступ к учетным записям без необходимости раскрывать пароль пользователя. OAuth широко используется для авторизации в веб-приложениях и мобильных приложениях.

OpenID Connect (OIDC): Слой аутентификации, построенный поверх OAuth 2.0. Он позволяет клиентским приложениям верифицировать идентичность пользователя на основе аутентификации, выполненной сервером аутентификации.

Security Assertion Markup Language (SAML): Стандарт обмена аутентификационными и авторизационными данными между сторонами, особенно между поставщиком идентичности и поставщиком услуг. SAML широко используется в корпоративных SSO решениях для обеспечения доступа к различным веб-приложениям и сервисам.

Same Sign-On (не путать с SSO): Хотя этот термин иногда используется как синоним SSO, он фактически относится к системам, где пользователи могут использовать одни и те же учетные данные для доступа к разным системам, но требуется повторный вход в каждую систему отдельно.

Каждый из этих подходов имеет свои особенности, преимущества и сферы применения, и выбор конкретного типа SSO зависит от требований к безопасности, интеграции и удобству использования в данной организации или проекте. (Рисунок 3.)

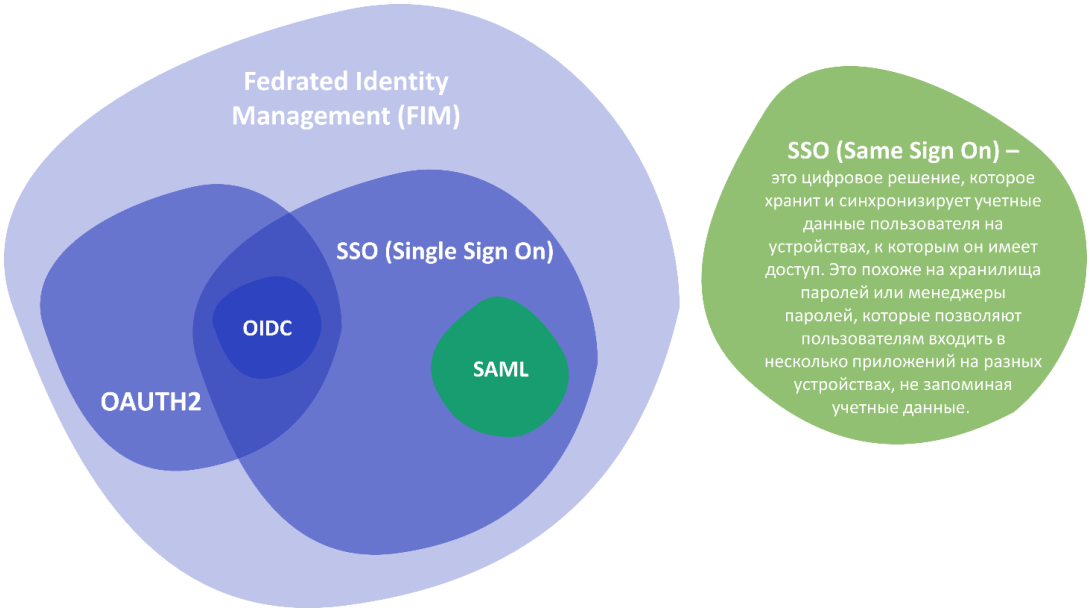

Рисунок 3. Типы SSO.

Как работает система единого входа как услуга?

SSO работает аналогично множеству других онлайн-приложений. Платформы вроде One ID, которые предоставляются через облачные сервисы, классифицируются как решения единого входа в формате "Программное обеспечение как услуга" (SaaS).

Что такое App-to-App (приложение-приложение) SSO?

App-to-App SSO относится к механизму, который позволяет передавать учетные данные пользователя между различными приложениями в рамках одной экосистемы, как это делается в SAP Cloud, где этот процесс используется для обеспечения бесперебойного доступа пользователя к разным приложениям без необходимости повторной аутентификации. Этот подход имеет сходства с принципами, лежащими в основе OAuth 2.0, хотя и не является стандартизированным протоколом или методом и в настоящее время специфичен только для SAPCloud.

Интеграция существующих систем

Одной из основных задач при внедрении единой системы авторизации является

интеграция с различными образовательными платформами и информационными системами, уже используемыми в образовательной сфере. Необходимо обеспечить совместимость и взаимодействие всех компонентов экосистемы.

В экосистеме образования ключевую роль играет интеграция различных источников данных, включая персональные паспортные данные, информацию о текущем образовании и дипломные данные. Эти данные автоматически импортируются и обновляются из баз данных различных государственных органов и образовательных учреждений, обеспечивая надежность и актуальность информации, доступной в системе. Такой подход не только повышает эффективность образовательного процесса, но и способствует более глубокой интеграции образовательной экосистемы с другими социальными и административными системами.

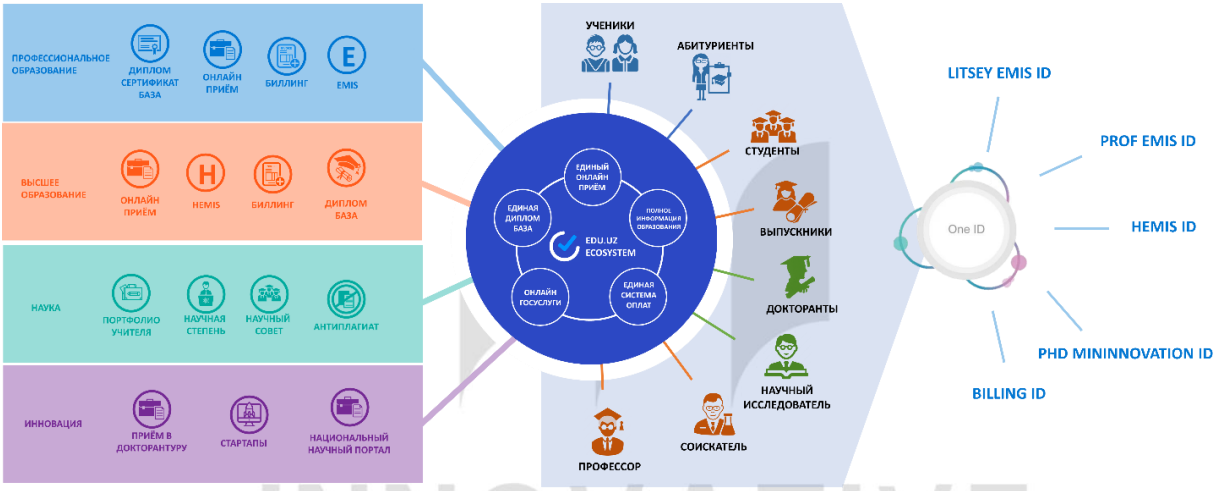

Рисунок 4. Интеграция ONE ID с экосистемой образования.

В центре внимания экосистемы образования находится система единой авторизации One ID, обеспечивающая безопасный и удобный доступ к широкому спектру веб-сайтов и порталов. (Рисунок 4.) One ID интегрируется с государственными и коммерческими организациями, предоставляя пользователям единый ключ к образовательным и административным услугам. Эта система является основой для создания безопасной и интегрированной образовательной среды, в которой каждый пользователь может легко получить доступ к необходимым ресурсам без необходимости многократного ввода учетных данных.

Адаптация и персонализация

Экосистема образования обеспечивает автоматическую адаптацию доступных ресурсов в зависимости от уровня образования и индивидуальных потребностей пользователя. Это означает, что ученики, студенты, преподаватели и научные деятели получают доступ к информации и услугам, которые наиболее релевантны именно для их образовательного и профессионального контекста. Интеграция различных баз данных и систем управления образовательной информацией позволяет системе предоставлять актуальные и персонализированные данные каждому пользователю.

Безопасность и приватность

Безопасность является критически важным аспектом единой системы авторизации. Необходимо реализовать механизмы шифрования, аутентификации и защиты данных, а также предусмотреть возможность восстановления доступа и

управления правами пользователей.

Интеграция образовательной экосистемы с системой единой авторизации One ID представляет собой значительный шаг в обеспечении удобства и безопасности доступа к образовательным ресурсам. Система One ID, ориентированная на удобство пользователей, позволяет им получать доступ ко множеству веб-сайтов и порталов государственного и хозяйственного управления, а также к ресурсам коммерческих организаций с использованием единых учетных данных.

One ID упрощает процесс управления учетными записями, снижая риск взлома и несанкционированного доступа благодаря централизации. Это уменьшает количество точек уязвимости и облегчает контроль за безопасностью данных.

Система автоматически адаптирует доступные ресурсы в соответствии с уровнем образования и потребностями пользователя, что не только повышает эффективность образовательного процесса, но и способствует защите информации от ненужного распространения.

Интеграция образовательной экосистемы с One ID подчеркивает стремление к созданию безопасного и интегрированного образовательного пространства, где каждый пользователь может эффективно и безопасно использовать доступные образовательные и научные ресурсы

Перспективы развития

Перспективы развития единой системы авторизации в образовательной экосистеме включают в себя внедрение новых технологий аутентификации, например, на основе биометрии, развитие механизмов машинного обучения для повышения безопасности и адаптация системы к постоянно изменяющимся требованиям образовательной среды.

Заключение

Внедрение единой системы авторизации в образовательной экосистеме представляет собой сложную, но крайне важную задачу, решение которой позволит создать более интегрированную, безопасную и удобную среду для всех участников образовательного процесса. Такая система станет основой для дальнейшей цифровизации и инноваций в образовании, способствуя повышению качества и доступности образовательных ресурсов и услуг.

Использованные литературы:

1. Демидова А. Ю., Жуков А.В. Технология Single Sign On: инструменты централизованной аутентификации для функциональной системы сервисов. Инженерный вестник Дона, 2020, №3

2. Информация с сайта Onelogin. По ссылке https://www.onelogin.com/learn/how-single-sign-on-works

3. ИБРАГИМОВА Н. Р. Единая образовательная экосистема в России: пути развития. «Молодой учёный» №7 (454)