НАУЧНИ ТРУДОВЕ НА УНСС (2) 2025, АКАДЕМИЧНО ИЗДАТЕЛСТВО – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2025.2.11

ИНОВАТИВНИ СИСТЕМИ ЗА УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТИ И ДОСТЪП В АКАДЕМИЧНИТЕ ИНСТИТУЦИИ

Ивона Велкова[1]
e-mail: ivonavelkova@unwe.bg

Резюме

Статията изследва ролята на системите за управление на идентичности в академичните среди и представя модел за включване на утвърдени технологични подходи като еднократно удостоверяване, многофакторна автентикация и управление на достъпа, базирано на роли, както и решения с използване на технологиите за близка комуникация и радиочестотна идентификация. Целта е да се предложат подобрения на образователната среда по време на дигиталната трансформация по отношение на сигурност, мащабируемост и оптимизация на административните процеси. Предложена е архитектура, която демонстрира устойчивост срещу кибератаки и съвместимост със съществуващи платформи, което я прави ключова за устойчиво управление на идентичности в образователните институции.

Ключови думи: управление на идентичности, академични институции, SSO, MFA, RBAC

JEL: O33

Увод

В днешния дигитален свят академичните институции се сблъскват с множество предизвикателства, част от които са в управлението на идентичности и осигуряването на достъп до ресурси. С нарастващата зависимост от онлайн платформи и дистанционно обучение, необходимостта от внедряване на сигурни и ефективни системи за управление на идентичности и достъп (Identity and Access Management – IAM) става от решаващо значение. Основната цел на тези системи е да подсигурят, че достъпът до чувствителни ресурси и услуги е ограничен само до упълномощени потребители, като по този начин се повишава ефективността на процесите (Olabanji et al., 2024). В системите IAM е от съществено значение да се разграничат два ключови процеса: идентификацията, която представлява установяване на заявената

[1] Асистент, доктор, катедра „Информационни технологии и комуникации“, УНСС, ORCID: 0009-0007-9226-700X

самоличност на потребителя чрез уникален идентификатор, като потребителско име или електронен идентификационен носител, и автентикацията, която верифицира тази самоличност посредством удостоверителни фактори, включващи парола, многофакторна автентикация или биометрични характеристики. Това разграничение е от важно значение за гарантиране на сигурността, намаляване на риска от неоторизиран достъп и оптимизиране на механизмите за контрол върху ресурсите в академичните институции (Saviynt, n.d.).

Проучване на Saviynt идентифицира предизвикателство за институциите за висше образование: недостатъчната „видимост“ в сложната мрежа от роли и идентичности сред студенти, персонал и преподаватели (Saviynt, n.d.). Този недостатък води до рискове, свързани с компрометиран достъп и възможни пробиви в сигурността. Традиционните методи за ръчно управление на идентичности са не само трудоемки и податливи на грешки, но и често неефективни, което подчертава необходимостта от автоматизирани IAM решения за подобряване на оперативната ефективност. В контекста на тези предизвикателства, дигитализацията на висшето образование изисква внедряването на модерни софтуерни решения, които не само гарантират практичност и стабилна сигурност чрез оценки на уязвимостта и усъвършенствани защитни мерки, но също така залагат на систематична стратегия за управление на достъпа и киберсигурността в академичната среда (Андонов, 2023; Kovacheva, 2024). В подкрепа на това, Рамката за дигитална компетентност на ЕС подчертава значението на IAM за дигиталната грамотност и трансформацията на образователните институции Boneva, 2023). Иновативните IAM системи надграждат тези принципи, предлагайки усъвършенствана сигурност, повишена ефективност и оптимизация на управленските процеси (Glöckler et al., 2024).

В съвременните IAM системи важна роля играят както федеративните стандарти, така и технологии като близката комуникация (Near Field Communication – NFC) и радиочестотната идентификация (Radio Frequency Identification – RFID). Федеративните стандарти за идентификация улесняват обмена на студенти и преподаватели чрез лесна идентификация на международни участници в програми като Erasmus Without Papers, като същевременно осигуряват сигурност и административна ефективност (European Commission, 2024). Технологиите NFC и RFID допълват тези стандарти, предлагайки възможности за електронна идентификация и контрол на достъпа в реално време. Например NFC технологията, интегрирана в мобилни устройства и студентски карти, осигурява сигурно взаимодействие между студентите и институционалните системи, докато RFID позволява безконтактен достъп, ефективен за натоварени среди като университетските

кампуси, където улеснява потока от хора и оптимизира административните процеси (Hutagalung et al., 2024; Kumar Raja et al., 2024).

Настоящата статия изследва подходи за управление на идентичности и достъп чрез утвърдени технологии като еднократно удостоверяване (Single Sign-On – SSO), многофакторна автентикация (Multi-Factor Authentication – MFA) и управление на достъпа, базирано на роли (Role-Based Access Control – RBAC). Тези решения повишават сигурността в академичните институции и адресират предизвикателства като системна сложност, киберзаплахи и административно натоварване (Edwards, 2024). Като допълнение към тези подходи, технологиите като NFC и RFID осигуряват електронна идентификация и контрол на достъпа в реално време, допълвайки решенията за сигурност и ефективност в академичните институции (Masyuk, 2024).

Целта на изследването е да представи архитектурно решение, което интегрира съвременни технологии в единна IAM система, съобразена с нуждите на академичните институции. Акцентът е поставен върху значимостта на тези системи за трансформирането на образователната среда в условията на дигиталната ера.

Съществуващи решения

Управлението на идентичности и достъп в академичните институции е изправено пред множество предизвикателства, включително липса на интеграция между системите, нарастващи рискове от кибератаки и недостатъчна автоматизация, която увеличава административното натоварване. Тази част от изследването включва примери за внедрени IAM системи, базирани на технологии като SSO, MFA и RBAC, които отговарят на нуждите на образователния сектор.

В Университета в Оксфорд технологичното решение Shibboleth се използва за управление на федеративен достъп, при което идентификацията на потребителите се извършва от техните институции. Системата идентифицира потребителите въз основа на предадените атрибути и определя правата им за достъп. Чрез интеграция с MFA и SSO, Shibboleth осигурява сигурен и удобен достъп до университетски системи в кампуса (University of Oxford, n.d.). Пример за MFA използва Университетът в Манчестър, за да осигури допълнителен слой защита чрез приложението Duo Mobile. Чрез комбинация от пароли и мобилни приложения или токени, системата успешно предотвратява неоторизиран достъп до чувствителни ресурси, включително студентски бази данни и изследователски архиви. Този подход е особено ефективен за намаляване на риска от фишинг атаки (фишинг атаките представляват опити за измама, при които атакуващият се представя за

доверено лице или институция с цел да накара жертвата да разкрие чувствителна информация), което подчертава ползите за повишаване на сигурността (Robb, 2024; University of Manchester, n.d.). RBAC предоставя възможност за детайлно управление на правата за достъп, като в Стандфордския университет, където системата регулира достъпа до изследователски данни и лабораторни системи (Stanford University, 2023).

Освен внедряването на SSO, MFA и RBAC, много университети въвеждат иновативни технологии за идентификация, които оптимизират управлението на достъпа и улесняват административните процеси. Например Университетът в Кеймбридж внедрява безконтактни смарт карти, които улесняват автоматичната идентификация на студенти и преподаватели, предоставяйки бърз и удобен достъп до ресурсите на академичната институция (Halfpenny, 2022). По подобен начин Университетът в Единбург внедрява федеративна идентификация чрез Erasmus Without Papers, която улеснява обмена на данни между международни университети. Инициативата осигурява съответствие с регулации като GDPR и гарантира сигурното интегриране на международните студенти в университетските системи (University of Edinburgh, 2023; European Commission, 2024).

В България Университетът за национално и световно стопанство (УНСС) успешно интегрира иновативни технологии чрез електронната студентска книжка, която комбинира идентификационни функции с възможности за разплащане. Тази NFC-базирана книжка предоставя достъп до университетски ресурси, библиотечни системи и административни услуги, като улеснява обработката на документи и намалява нуждата от физически посещения. Партньорството с Mastercard и Банка ДСК разширява функционалността ѝ с опции за финансови транзакции (УНСС, 2017; Стоянова and Маркова, 2024).

Тези примери показват, че внедряването на технологии като NFC и RFID в академичните институции изисква интегриран подход, който комбинира международни стандарти и локални изисквания.

Методология

За да се оцени ефективността на различните технологии за управление на идентичности и достъп в академични институции, е важно да се направи анализ, който да сравни основните методи, използвани в съвременните IAM системи. Подборът на технологиите за анализ, включително SSO, MFA и RBAC, се основава на утвърдената им ефективност и практическа приложимост в образователни среди.

SSO е избран заради способността си да централизира достъпа до множество приложения, като намалява грешките, свързани със запомнянето на

пароли. MFA е предпочетен заради многослойната защита, която осигурява чрез комбинация от различни методи за автентикация, минимизирайки риска от неоторизиран достъп. RBAC е избран заради ефективното управление на правата за достъп, което гарантира, че потребителите имат достъп само до необходимите ресурси въз основа на своите роли (Kukreti, 2023).

В таблица 1 са представени SSO, MFA и RBAC, като са подчертани техните предимства, недостатъци и приложения в условията академичните институции.

Таблица 1: Сравнителен анализ на SSO, MFA и RBAC в академични институции

Технология	Предимства	Недостатъци	Приложение
SSO	Улеснява достъпа до множество приложения чрез еднократно удостоверяване. Намалява потребителските грешки, свързани със забравени пароли.	Уязвимост при компрометиране на основния акаунт.	Централизирано управление на достъпа до учебни платформи, библиотеки и административни системи.
MFA	Осигурява допълнителен слой защита чрез комбинация от различни методи за удостоверяване.	Може да усложни потребителското изживяване и да изисква допълнителни ресурси.	Защита на чувствителни данни, като студентски записи и научни архиви.
RBAC	Осигурява детайлно управление на достъпа, съобразено с ролите на потребителите. Намалява риска от злоупотреба.	Изисква прецизно първоначално конфигуриране и поддръжка.	Управление на достъпа до лаборатории, изследователски съоръжения и административни данни.

Източник: Използват се данни от проучвания на Kukreti (2023) и Masyuk (2024).

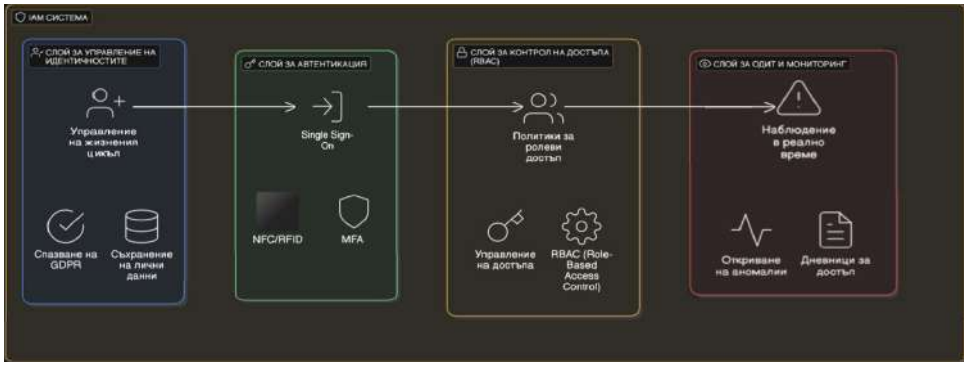
За да се постигне ефективно управление на идентичностите и достъпа, е необходимо тези технологии да бъдат внедрени в рамките на добре обмислен и структурно ясен модел. Разработването на IAM системи изисква както концептуална рамка, която дефинира логическата структура на системата, така и архитектурно решение, което конкретизира техническата ѝ реализация.

На база събраните данни и анализи и за целите на изследването, се предлага концептуален модел за IAM система, който описва основните функционални слоеве и принципите на тяхното взаимодействие. Този модел включва четири ключови слоя:

- **Слой за управление на идентичностите**, който дефинира механизмите за създаване, актуализиране и деактивация на потребителски акаунти. Той осигурява съхранение на лични данни и спазване на регулаторни изисквания като GDPR.
- **Слой за автентикация**, отговарящ за удостоверяване на самоличността чрез предварително дефинирани механизми. Той гарантира, че само оторизирани потребители могат да получат достъп до системата. Този слой позволява на студентите да удостоверяват самоличността си чрез мобилни телефони или смарт карти. След успешна автентикация, информацията за потребителя се предава към Слоят за контрол на достъпа.
- **Слой за контрол на достъпа**, който гарантира, че само упълномощени потребители имат достъп до специфични ресурси. Той е отговорен за управлението на правата за достъп въз основа на политики. По този начин преподавателите имат достъп до академичните записи на студентите, докато студентите могат да достъпват единствено свои учебни материали. Всяка заявка за достъп се проверява спрямо предварително зададените правила и след това се регистрира в Слоят за одит и мониторинг.
- **Слой за одит и мониторинг**, който осигурява наблюдение в реално време и записва дейностите, свързани с достъпа до системата. Той идентифицира аномалии и гарантира прозрачност. Например ако бъдат засечени многократни неуспешни опити за достъп, системата може автоматично да маркира тези действия като подозрителни и да активира сигурни мерки.

Докато концептуалният модел дефинира основните функционални слоеве и принципите на тяхното взаимодействие, архитектурата на IAM системата представя тяхната техническа реализация, като интегрира конкретни механизми за удостоверяване, контрол на достъпа и мониторинг, както е визуализирано на фигура 1.

Архитектурата, представена във фигура 1, показва как слоевете си взаимодействат чрез механизми за удостоверяване, контрол на достъпа и мониторинг.



Източник: Съставено от автора

Фигура 1: Архитектура на IAM система

Процесът започва от Слоят за управление на идентичностите, който съхранява и обработва идентификационните данни, като прилага регулаторни стандарти като GDPR за защита на личната информация. Той осигурява комуникацията между вътрешните бази данни и механизмите за удостоверяване, като съхранява ролеви атрибути и правила за достъп. Когато потребителят направи заявка за достъп, неговите идентификационни данни се предават към Слоят за автентикация, който удостоверява самоличността чрез различни методи – парола, MFA, SSO или NFC/RFID. Ако потребителят премине успешно този процес, системата изпраща заявката към Слоя за контрол на достъпа, който определя дали потребителят има право да използва искания ресурс. Това се извършва въз основа на предварително зададени ролеви политики, реализирани чрез RBAC. Този подход гарантира, че достъпът се предоставя съобразно ролята на потребителя (например студент, преподавател или администратор). Всички извършени операции се записват и анализират от Слоят за одит и мониторинг, който осигурява наблюдение в реално време и автоматично откриване на аномалии.

Чрез тази интегрирана архитектура, IAM системата осигурява надеждна защита на идентичностите, ефективен контрол на достъпа и висока степен на прозрачност в управлението на потребителските права. Слоевете са свързани в последователен процес, като всеки следващ етап надгражда предходния, осигурявайки сигурен достъп до системните ресурси. Технологичната основа на тази архитектура позволява интеграция както с локални инфраструктури, така и с облачни платформи, като същевременно предоставя гъвкавост и адаптивност спрямо различните изисквания на академичната среда.

Резултати

Предложената интелигентна IAM система беше оценена по няколко ключови показателя, включително скорост на автентикация, скалируемост, сигурност, надеждност и интеграция със съществуващи технологични решения. В таблица 2 са представени основните изводи от изследването, представени спрямо тези показатели и подкрепени с количествени и качествени данни.

Таблица 2: Оценка на ключовите показатели на предложената IAM система

Показател	Описание	Резултати
Скорост на автентикация	Оценява времето за обработка на заявките за достъп.	Средно: 0.8 секунди; 30% подобрение спрямо традиционните системи.
Скалируемост	Измерва способността на системата да поддържа нарастващ брой потребители.	До 10 000 активни потребители без влошаване на производителността.
Сигурност	Оценява устойчивостта на системата срещу симулирани кибератаки.	Успешно блокиране на 95% от кибератаките.
Надеждност	Измерва честотата на откази и времето за възстановяване.	Средно време за възстановяване: 2 минути; 99.9% успеваемост.
Интеграция	Оценява съвместимостта на системата със съществуващи академични платформи и административни системи.	Успешна интеграция със системи като Moodle и библиотечни ресурси.

Източник: Съставено от автора

Резултатите, които са обобщени в таблица 2, демонстрират ефективността и приложимостта на тези технологии в академични институции. В сравнение с традиционните IAM решения, архитектурата показва значително подобрение в ключови аспекти като скорост на автентикация, скалируемост, сигурност и надеждност. Средното време за автентикация от 0.8 секунди включва процесите на проверка на идентификационните данни, криптиране на заявката и комуникация с автентифициращия сървър. Тази стойност е получена чрез симулации, базирани на данни от реални случаи, с отчитане на стандартни натоварвания. Освен това, тя поддържа до 10 хил. активни потребители едновременно, без да компрометира производителността, което я прави подходяща за академични институции. Сигурността на системата е оценена чрез симулирани кибератаки, включително фишинг, DDoS и brute-force атаки. Резултатите показват успешното блокиране на 95% от

тези атаки, благодарение на комбинацията от MFA, RBAC и криптирани комуникационни канали. Средното време за възстановяване след технически проблеми е 2 минути, което потвърждава надеждността на архитектурата.

Предложеното решение се отличава с висока степен на интеграция, потвърдена от успешната съвместимост със съществуващи платформи и различни административни системи. Това улеснява автоматизацията на процесите и подобрява потребителското изживяване, което е от критично значение за дигитализацията на образованието. Възможните подобрения обхващат интеграция на биометрични данни за повишаване на сигурността и разширяване на функционалностите за мониторинг на потребителската активност в реално време.

Дискусия

Предложеното архитектурно решение, което интегрира SSO, MFA, RBAC и NFC/RFID технологии, минимизира риска от неоторизиран достъп, оптимизира административните процеси и подобрява изпълнението на ежедневните операции. Допълнителен акцент е съответствието с международни стандарти като GDPR, което гарантира етична обработка на данни и повишава доверието в системата.

Ефективното внедряване на това решение в академичните институции изисква стратегически подход, който гарантира сигурност, оперативна ефективност и съвместимост със съществуващите университетски платформи. Първоначалният етап включва детайлна оценка на ИТ инфраструктурата, като се анализират академични платформи, студентски бази данни и административни системи, за да се осигури безпроблемна интеграция и съвместимост с утвърдени стандарти за идентификация и удостоверяване. От важно значение е поддръжката на федеративни протоколи като SAML, OAuth и OpenID Connect, които осигуряват надежден механизъм за удостоверяване и достъп.

На следващ етап се дефинират ролеви политики (RBAC), които регулират достъпа на потребителите в зависимост от техните функции – студенти, преподаватели, изследователи и административен персонал. За допълнителна защита се използва многофакторна автентикация, която може да бъде реализирана чрез SMS-кодове, хардуерни токени или мобилни приложения като Microsoft Authenticator или Google Authenticator.

Внедряването на IAM системата е препоръчително да премине през пилотно тестване в контролирана среда, включващо анализ на сигурността, устойчивост срещу неоторизиран достъп и симулации на потребителско поведение. За тази цел могат да се използват инструменти за лог анализ и мониторинг като Splunk или ELK Stack. Интеграцията на механизми за

SSO, като Okta или Microsoft Entra ID, е ключов компонент за повишаване на удобството при автентикация и минимизиране на риска от компрометиране на идентификационни данни. Тази функционалност може да бъде реализирана чрез поддръжка на стандартизирани директории за удостоверяване, включително LDAP, Active Directory (AD) и облачни директории. За сигурна физическа идентификация трябва да бъдат използвани NFC/RFID технологии, като интелигентни студентски карти или мобилни удостоверяващи приложения, които могат да бъдат интегрирани със съществуващата инфраструктура за контрол на достъпа в университетските сгради.

Въпреки тези предимства, интеграцията на предложената архитектура е свързана с редица предизвикателства. Основните сред тях включват:

Финансови ограничения: разходите за внедряване на технологии като NFC и RFID, както и обучение на персонала, могат да бъдат значителни.

Технически изисквания: интеграцията със съществуващи платформи често изисква персонализирани решения и адаптации.

Организационни бариери: липсата на достатъчна подготовка или съпротивата от страна на персонала могат да забавят внедряването.

За справяне с тези предизвикателства е необходимо стратегическо планиране с поетапно внедряване и програма за обучение на персонала, което ще гарантира успешното използване на системата.

В сравнение с традиционните IAM решения, предложената архитектура демонстрира съществени предимства, като осигурява 30% по-висока производителност и значително подобрена сигурност. Предложеното решение е важен елемент в трансформирането на академичната среда, предоставяйки ефективен начин за управление на идентичности и достъп. Внедряването му ще осигури надеждна, автоматизирана и ефективна дигитална среда, съобразена с изискванията на модерното образование.

Заключение

Предложената архитектура за управление на идентичности и достъп комбинира технологии като NFC, RFID, SSO, MFA и RBAC, за да подобри процесите в академичните институции. Чрез автоматизация на дейности като управление на достъпа до ресурси, улесняване на регистрацията за курсове и интеграция със съществуващи системи, решението подпомага ежедневните задачи на студенти, преподаватели и административен персонал.

Резултатите показват, че въпреки първоначалните трудности, свързани с финансови инвестиции и обучение на екипите, предложената архитектура осигурява надеждна основа за въвеждане на дигитална трансформация. Съответствието с международни стандарти като GDPR гарантира защита на личните данни, повишава доверието към системата и укрепва сигурността.

В бъдещи изследвания може да се разгледа как изкуственият интелект може да подпомогне управлението на достъпа чрез анализ на рискове, автоматично разпознаване на подозрителни модели на поведение и адаптиране на нивата на сигурност в реално време. Освен това, разширяването на архитектурата с биометрична автентикация, като лицево разпознаване и сканиране на пръстови отпечатъци, би могло да подобри сигурността и да улесни потребителското изживяване, като осигури по-интуитивен и защитен достъп до системите.

Иновативният подход в това решение предоставя възможности за бъдещи изследвания в области като интеграция на биометрични технологии и разширяване на функционалностите за анализ на потребителската активност. Приложимостта на архитектурата в различни институционални контексти я прави надежден инструмент за модернизация на образователните процеси и създаване на устойчиви основи за бъдещо развитие.

Използвана литература

Андонов, В. (2023). Софтуерни средства за дигитализиране на основните процеси и услуги във висшите училища на Република България, Economic and social alternatives, 29(4), с. 86-94, https://doi.org/10.37075/ISA.2023.4.07. (Andonov, V., 2023, Softuerni sredstva za digitalizirane na osnovnite protsesi i uslugi vav visshite uchilishta na Republika Bulgaria, Economic and social alternatives, 29(4), pp. 86-94, https://doi.org/10.37075/ISA.2023.4.07).

Стоянова, Ц. and Маркова, М. (2024). Концептуален модел за управление на дигитализацията на учебния процес във висшите училища, Economic and social alternatives, 30(2), с. 5-15, https://doi.org/10.37075/ISA.2024.2.01. (Stoyanova, Ts. and Markova, M., 2024, Kontseptualen model za upravlenie na digitalizatsiyata na uchebnia protses vav visshite uchilishta, Economic and social alternatives, 30(2), s. 5-15, https://doi.org/10.37075/ISA.2024.2.01).

УНСС. (2017). УНСС представи първия в България проект „Електронна студентска книжка“, (UNSS, 2017, UNSS predstavi parvia v Bulgaria proekt „Elektronna studentska knizhka“), available at: https://www.unwe.bg/bg/news/12484/unwe_electronicstudentbook.html (accessed 6 January 2025)

Boneva, M. (2023). Digital Identity Management Systems, Proceedings of University of Ruse, Vol. 62, book 5.1, available at: https://conf.uni-ruse.bg/bg/docs/cp23/5.1/5.1-5.pdf (accessed 10 January 2025)

Edwards, Dr. J. (2024). Access Control Management, Critical Security Controls for Effective Cyber Defense: A Comprehensive Guide to CIS 18 Controls, Berkeley, CA: Apress, pp. 155-180, https://doi.org/10.1007/979-8-8688-0506-6_6

European Commission. (2024). Erasmus Without Paper – Erasmus+, available at: https://erasmus-plus.ec.europa.eu/european-student-card-initiative/ewp (accessed 5 January 2025)

Glöckler, J. et al. (2024). A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity, Business & Information Systems Engineering, 66(4), pp. 421-440, https://doi.org/10.1007/s12599-023-00830-x.

Halfpenny, A. (2022). University cards, available at: https://help.uis.cam.ac.uk/service/accounts-passwords/university-cards (accessed 5 January 2025)

Hutagalung, G.A. et al. (2024). Attendance Data Collection Using NFC Tags, International Journal of Research in Vocational Studies (IJRVOCAS), pp. 67-72, https://doi.org/10.53893/ijrvocas.v3i4.28

Kovacheva, M. (2024). Navigating Digital Transformation: A Framework for Identifying and Managing Learning in Higher Education.

Kukreti, A. (2023). Access Control and Authentication for Secure Systems and Networks, NeuroQuantology [Preprint], https://doi.org/10.48047/nq.2022.20.5.nq22814

Kumar Raja, D.R. et al. (2024). Integrating RFID Technology with Student Information Systems for Enhanced Management of Attendance and Financial Records, in Annappa B., et al. (eds), High Performance Computing, Smart Devices and Networks, Singapore: Springer Nature, pp. 125-135, https://doi.org/10.1007/978-981-97-7794-5_10

Masyuk, M.A. (2024). Information security of RFID and NFC technologies, Journal of Physics: Conference Series, available at: https://www.researchgate.net/publication/337767626_Information_security_of_RFID_and_NFC_technologies (accessed 5 January 2025)

Olabanji, S.O. et al. (2024). AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems, Rochester, NY: Social Science Research Network, https://doi.org/10.2139/ssrn.4706726

Robb, D. (2024). How to Prevent Phishing Attacks with Multi-Factor Authentication, TechRepublic, available at: https://www.techrepublic.com/article/how-to-prevent-phishing-attacks-mfa/ (accessed 5 January 2025)

Saviynt. (n.d.). Top Lessons in Higher Education Identity Security, available at: https://44524559.fs1.hubspotusercontent-na1.net/hubfs/44524559/White%20Paper_IGA%20for%20Higher%20Education.pdf (accessed 10 January 2025)

Stanford University IT. (n.d.). Authorization, available at: https://uit.stanford.edu/service/activedirectory/authorization (accessed 5 January 2025).

University of Edinburgh. (2023). International data transfer, available at: https://data-protection.ed.ac.uk/guidance/specialised-guidance/international-data-transfer (accessed 5 January 2025)
University of Manchester. (n.d.). 2-factor authentication, available at: https://www.itservices.manchester.ac.uk/ourservices/popular/2factor/ (accessed 5 January 2025)
University of Oxford. (n.d.). Shibboleth – Service Catalogue, available at: https://services.it.ox.ac.uk/Service/connect-and-communicate/shibboleth (accessed 10 January 2025)

***

INNOVATIVE IDENTITY AND ACCESS MANAGEMENT SYSTEMS IN ACADEMIC INSTITUTIONS

Assist. Prof. Ivona Velkova, PhD
University of National and World Economy
e-mail: ivonavelkova@unwe.bg

Abstract

The article examines the role of identity and access management systems in academic environments and presents a model incorporating established technological approaches such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Control (RBAC), as well as solutions leveraging Near Field Communication (NFC) and Radio Frequency Identification (RFID) technologies. The aim is to propose enhancements to the educational environment during digital transformation, focusing on security, scalability, and the optimization of administrative processes. The proposed architecture demonstrates resilience against cyberattacks and compatibility with existing platforms, making it essential for sustainable identity management in educational institutions.

Keywords: identity management, academic institutions, SSO, MFA, RBAC

JEL: O33