

МЕТОДЫ И СРЕДСТВА ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Красиньков Д.В.

ФГБОУ ВО «Мелитопольский
государственный университет», Мелитополь,
e-mail: anna.dyachenko597@mail.ru

Научный руководитель: Дяченко А.С.

Введение

Дистанционное обучение стало важной частью образовательного процесса, особенно в последние годы, когда пандемия COVID-19 ускорила переход к онлайн-образованию. В условиях онлайн-обучения одним из ключевых аспектов является необходимость обеспечения безопасности данных и идентификации участников образовательного процесса. Идентификация пользователей в таких системах помогает не только защитить личные данные студентов и преподавателей, но и улучшить качество образовательного процесса, персонализировать обучение, а также предотвратить мошенничество и академическое недобросовестное поведение. В условиях нарастающей цифровизации образовательных платформ вопрос идентификации становится все более актуальным. Традиционные методы, такие как использование логина и пароля, не могут обеспечить достаточный уровень безопасности, особенно с учетом возросшей угрозы утечек данных и атак. Поэтому современные системы дистанционного обучения обращаются к более надежным методам, таким как многократная аутентификация, биометрические технологии и поведенческая аналитика. Однако внедрение этих технологий сопряжено с рядом проблем, таких как высокие затраты на оборудование и вопросы защиты конфиденциальности пользователей. В данном исследовании рассматриваются современные методы идентификации пользователей в системах дистанционного обучения, их преимущества и недостатки, а также возможности для улучшения безопасности и персонализации в образовательных платформах.

Цель исследования – провести анализ современных методов и средств идентификации пользователей в дистанционном обучении, оценке их эффективности, а также выявлении тенденций и проблем, связанных с внедрением этих технологий в образовательный процесс.

Материал и методы исследования

Для достижения поставленной цели был использован комплексный подход, включающий теоретический и эмпирический анализ. На первом этапе исследования был проведен обзор научной литературы, посвященной различным методам идентификации пользователей в систе-

мах дистанционного обучения. Исследовались как традиционные, так и новейшие подходы, такие как биометрия, многократная аутентификация и поведенческая аналитика. Анализировались различные примеры успешных реализаций этих технологий в ведущих образовательных учреждениях и на популярных образовательных платформах.

Кроме того, для проведения эмпирической части исследования были проанализированы данные о текущем состоянии внедрения методов идентификации в несколько образовательных платформ, таких как Moodle, Blackboard, Coursera и другие. Рассматривались примеры использования биометрических данных (распознавание лиц, отпечатков пальцев) и двухфакторной аутентификации на этих платформах. В процессе анализа также был рассмотрен опыт ряда университетов, внедривших системы идентификации с использованием биометрии и многократной аутентификации.

Результаты исследования и их обсуждение

Первоочередным, для нашего исследования, считаем необходимость анализа общего понимания современных методов и средств идентификации пользователей. Проведенное исследование позволило утверждать, что на сегодняшний день существует несколько методов идентификации пользователей, каждый из которых имеет свои преимущества и недостатки, рассмотрим каждый из них отдельно:

1. Парольная аутентификация – классический метод, который используется в большинстве образовательных платформ. Однако безопасность паролей может быть под угрозой в случае использования слабых или легко угадываемых комбинаций. Уязвимость этого метода выявляется также при возможных утечках данных.

2. Многократная аутентификация (MFA) – обеспечивает более высокий уровень безопасности. Включает в себя не только ввод пароля, но и дополнительные шаги подтверждения, такие как одноразовые коды, отправляемые на мобильные устройства, или использование токенов. Это значительно снижает вероятность взлома, но может создавать неудобства для пользователей из-за дополнительных шагов в процессе авторизации.

3. Биометрическая аутентификация – включает использование отпечатков пальцев, распознавания лиц, радужной оболочки глаз и других биометрических данных. Этот метод представляет собой один из самых надежных способов идентификации. Например, университеты и образовательные учреждения в странах Азии начали активно внедрять системы распознавания лиц на экзаменах для предотвращения мошенничества.

4. Аутентификация на основе поведения пользователя – методы, использующие поведение пользователя (анализ скорости набора текста, характер движений мыши) для проверки личности. Эти методы пока находятся на стадии разработки, но их внедрение в будущем может значительно улучшить точность идентификации, особенно в сочетании с другими методами.

Как мы можем наблюдать, анализ научной литературы о современном состоянии разработок вопроса идентификации показывает достаточно широкий спектр подходов к идентификации пользователя, однако, научные исследования показывают, что вопрос идентификации пользователей в образовательных платформах все больше ориентируется на многофакторные и биометрические системы. Например, исследования, проведенные в США и Европе, показывают рост использования технологий распознавания лиц в университетах для предотвращения подмены личности на экзаменах. Однако многие исследования также подчеркивают важность соблюдения конфиденциальности данных пользователей, что делает необходимым развитие безопасных методов хранения и обработки биометрической информации.

Современные работы также акцентируют внимание на взаимодействии разных систем аутентификации. Например, комбинация биометрии и многократной аутентификации может обеспечить значительно более высокий уровень безопасности по сравнению с использованием одного метода. Также обсуждается важность интеграции этих технологий в единую систему, чтобы обеспечить бесшовный и удобный опыт для пользователей.

Одним из примеров успешного внедрения биометрической аутентификации является система, использующая распознавание лиц для входа на экзамены, которая внедрена в ряде университетов в Китае. Эта технология позволяет не только обеспечить безопасность, но и предотвратить случаи мошенничества, такие как сдача экзаменов за других студентов.

В Европе некоторые университеты начали использовать системы идентификации на базе отпечатков пальцев для контроля доступа к учебным помещениям и лабораториям. В некоторых странах, таких как Южная Корея и Япония, активно используются биометрические системы для онлайн-экзаменов.

Технологии в области биометрической идентификации продолжают развиваться. Одной из перспективных технологий является распознавание голоса, которое в сочетании с другими методами может создать еще более надежную систему безопасности. Также развивается поведенческая биометрия, которая будет использовать данные о том, как человек взаимодействует с устройствами.

Кроме того, в будущем можно ожидать более широкое внедрение искусственного интеллекта для повышения точности и надежности систем идентификации, а также использование блокчейн-технологий для обеспечения безопасности и неизменности данных.

Для ограничения исследования, нами был сконцентрирован вектор исследования на образовательных платформах, доступных учебным учреждениям на бесплатной основе, в связи с недостаточным уровнем финансирования ВУЗов и других учреждений на примере платформ Moodle, Blackboard и Coursera [1].

Moodle – одна из самых популярных платформ для дистанционного обучения. В текущей версии Moodle существует стандартная возможность идентификации с использованием логина и пароля. Однако в последние годы начали развиваться и внедряться дополнения, позволяющие использовать многократную аутентификацию через SMS или через мобильные приложения. Например, в Moodle можно подключить систему двухфакторной аутентификации, которая требует от пользователя не только ввода пароля, но и одноразового кода, отправляемого на мобильный телефон или через приложения типа Google Authenticator. Также в Moodle есть возможность интеграции с биометрическими системами для аутентификации студентов, но для этого необходимо использование сторонних плагинов и дополнительных настроек [2].

Blackboard – еще одна популярная образовательная платформа, активно использующая методы многократной аутентификации и биометрии. В частности, Blackboard в рамках своей системы безопасности предлагает интеграцию с двухфакторной аутентификацией через мобильные приложения, такие как Duo Security. Однако наиболее ярким примером внедрения технологий идентификации является система «SafeAssign», использующая биометрические данные для предотвращения мошенничества на экзаменах. В этой системе используется интеграция с мобильными приложениями для контроля активности пользователей в ходе выполнения тестов и заданий.

Coursera, как одна из ведущих онлайн-образовательных платформ, активно использует аутентификацию с использованием пароля, однако в последнее время компания начала внедрять и более сложные методы, такие как двухфакторная аутентификация для пользователей, участвующих в платных курсах. Также были проведены эксперименты с биометрической аутентификацией для предотвращения использования чужих учетных записей при сдаче экзаменов в рамках программ сертификации. Биометрические технологии в Coursera пока находятся на стадии тестирования, однако компания активно исследует этот вопрос, особенно с учетом роста числа фальсификаций результатов [4].

Другие образовательные платформы для дистанционного обучения, такие как Udacity, EdX и Skillshare, также начинают внедрять системы многократной аутентификации и исследуют возможность использования биометрии. Например, платформы вроде EdX предлагают двухфакторную аутентификацию для студентов и преподавателей, а Udacity активно работает с университетами по внедрению систем распознавания лиц для предотвращения обмана на экзаменах.

Как мы можем видеть, хоть системы и имеют в своем технологическом стеке, средства идентификации пользователей, однако внедрения всего спектра пока является невозможным или же сопрягается с некоторым спектром проблем. Наибольшие проблемы при внедрении технологий идентификации в образовательный процесс связаны с конфиденциальностью и защитой персональных данных. Биометрическая информация, если она не защищена должным образом, может стать объектом утечек, что приведет к серьезным последствиям для пользователей.

Кроме того, стоимость внедрения таких технологий, как системы распознавания лиц или отпечатков пальцев, является значительным барьером для ряда образовательных учреждений, особенно в развивающихся странах [3]. Также важно учитывать, что не все студенты могут иметь доступ к современным устройствам, необходимым для биометрической идентификации.

Выводы

Современные методы идентификации пользователей в системах дистанционного обучения, такие как многократная аутентификация и биометрические технологии, значительно повышают уровень безопасности и способствуют персонализации образовательного процесса. Однако внедрение этих технологий сопряжено с рядом проблем, включая вопросы защиты персональных данных, высокую стоимость и доступность технологий для образовательных учреждений, а также необходимость соблюдения конфиденциальности информации. В будущем ожидается развитие биометрической аутентификации, поведенческой биометрии и интеграция искусственного интеллекта для повышения точности систем идентификации. Для успешного внедрения таких технологий важно разработать четкие нормативы по защите данных и снизить стоимость их внедрения в образовательный процесс.

Список литературы

1. Bukreiev D. et al. Features of the development of an automated educational and control complex for checking the quality of students. CEUR Workshop Proceedings, 2021.
2. Kruglyk V. et al. Discord platform as an online learning environment for emergencies // Ukrainian Journal of Educational Studies and Information Technology. 2020. Т. 8. №. 2. С. 13-28.
3. Козлова О.А., Протасова А.А. Использование нейронных сетей в дистанционных образовательных технологиях для идентификации обучающихся // Открытое образование. 2021. Т. 25. №. 3. С. 26-35.

4. Корепанова А.А. и др. Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях // Компьютерные инструменты в образовании. 2019. №. 3. С. 29-43.

О ВОЗМОЖНОСТЯХ ИНФОРМАЦИОННОГО ОБСЛЕДОВАНИЯ ОРГАНИЗАЦИИ

Крылов Н.В., Маркин В.В.

АНОО ВО «Воронежский институт
высоких технологий», Воронеж,
e-mail: bbosly@yandex.ru

Информационная система необходима организации для обеспечения информационно-коммуникационной поддержки ее основной и вспомогательной деятельности. Поэтому, прежде чем говорить о содержании структуры и функциях информационной системы, необходимо разобраться в целях и задачах самой организации, чтобы понять, что необходимо автоматизировать [1, 2].

В чем заключается миссия компании, то есть для чего компания была создана и к чему она стремится в своей деятельности. Каково направление ее деятельности. Какова структура компании, какие функции выполняют ее подразделения и как они взаимодействуют друг с другом. Только после ответа на все эти вопросы мы можем перейти к обсуждению того, какие функции должна выполнять корпоративная информационная система и какие аппаратные и программные средства должны быть включены для автоматизации функций, выполняемых подразделениями компании.

Ответы на эти вопросы можно получить только после подробного информационного опроса компании, целью которого является [3,4]:

Рассмотрим формулировку и описание функций каждого подразделения компании, а также задач, которые они решают;

Объясните технологию работы «как есть» в каждом отделе компании и поймите, что необходимо автоматизировать и в каком порядке;

Исходя из миссии и направлений деятельности компании, приведите описание технологии, которая работает «как надо» для каждого отдела, и связанных с этим информационных потоков;

Отобразите технологию «по мере необходимости» в структуре компании, определите ее функциональный состав и количество рабочих мест в каждом структурном подразделении компании, а также функции, которые выполняются (автоматизируются) на каждом рабочем месте;

Описание основных путей и алгоритмов прохождения входящих, внутренних и исходящих документов, а также методов их обработки.

Результаты опроса о деятельности компании, в которой разрабатывается проект корпоративной информационной системы, и модели ее информационной инфраструктуры, а также