ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ ОБУЧАЮЩЕГОСЯ ПРИ РЕАЛИЗАЦИИ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ В РЕЖИМЕ ОНЛАЙН-ОБУЧЕНИЯ

А. В. Мешков, В. В. Новикова
ФГАОУ ВО «НИУ ИТМО»
Санкт-Петербург, Россия
zay4ka251@yandex.ru, novikova.vladlen@yandex.ru
С. Н. Девицына,
Кафедра информационной безопасности ФГАОУ ВО «СевГУ»
Севастополь, Россия
devitsyna@mail.ru
Е. И. Прохоренко
Кафедра информационно-телекоммуникационных технологий НИУ «БелГУ»
Белгород, Россия
prokhorenko@bsu.edu.ru

Аннотация. Применение двухфакторной аутентификации обучающегося при реализации контрольно-оценочных мероприятий является актуальной и важной задачей, решение которой представлено в виде разработки программного обеспечения, основанного на использовании биометрических характеристик учащихся учебного заведения. Применение ПО «Двухфакторная аутентификация» и его интеграция в действующие системы контроля обучающихся повысят эффективность проведения прокторинга.

Ключевые слова: *информационные технологии; аутентификация; онлайн-обучение*

Информационные технологии повсеместно используются для повышения качества образовательного процесса. За последние два года образовательные системы претерпели особенные изменения, связанные с COVID-19. Образовательные учреждения были вынуждены прибегнуть к использованию различных информационных технологий для продолжения образовательного процесса в дистанционном формате в целях предотвращения распространения коронавирусной инфекции. Для контрольно-оценочных мероприятий в режиме онлайн-обучения используются прокторинговые системы, позволяющие проводить в онлайн-режиме экзамен или тестирование.

В прокторинговых системах для подтверждения личности и получения доступа к тестированию обучающийся предъявляет документ, удостоверяющий личность, это, как правило, студенческий билет или паспорт. Администратор, который сопровождает тестирование, сверяет фотографию в документе с человеком, сидящим перед камерой, и на основании этого действия делает вывод о дальнейшем исходе событий — допуске обучающегося к аттестации либо запрете. Такой способ аутентификации является небезопасным, т. к. не исключена возможность сговора с ответственным за прокторинг (внутренний нарушитель), а также задействует дополнительные ресурсы.

Для обеспечения информационной безопасности при проведении контрольно-оценочных мероприятий в режиме онлайн-обучения, автоматизации процесса и точности идентификации обучающегося используют различные критерии для входа в систему и доступа к ресурсам. Такой способ называется многофакторным и имеет очевидные преимущества перед однофакторной аутентификацией.

В приведенном исследовании показано, что использование уникальных характеристик человека — его биометрических данных — и выбор типов биометрик для многофакторной аутентификации — актуальная задача, решение которой позволит образовательным организациям не только повысить эффективность образовательного процесса путём строгого соблюдения регламента, но и оптимизировать бизнес-процессы.

Целью разработки является совершенствование прокторинговой системы путём внедрения интеллектуальной многофакторной биометрической аутентификации субъекта. Как показал анализ информационных источников, наиболее популярным способом является идентификация субъекта по изображению лица. На предприятиях, в учреждениях и организациях для реализации систем безопасности широко используются системы контроля и управления доступом и, в частности,

видеонаблюдение. Для образовательного процесса также используется видеонаблюдение с помощью веб-камер. Так как однофакторные системы менее надежны, принято решение подобрать виды биометрик и их комбинации для повышения эффективности аутентификации субъекта при условии ограничения ресурсов, в том числе, с учетом финансового фактора. Проведен анализ эффективности использования разных комбинаций биометрик. В результате выбрана пара: изображение лица и образец голоса субъекта. Программное решение представляет собой элемент двухфакторной аутентификации на основе анализа и сравнения с полученными образцами биометрических данных пользователя [6].

Для разработки данного ПО был использован высокоуровневый язык программирования общего назначения с динамической типизацией и автоматическим управлением памятью — Python. Для реализации модуля аутентификации по изображению лица субъекта были использованы следующие инструменты:

— face_recognition — библиотека для распознавания лица;

— cv2 — библиотека компьютерного зрения;

— pickle — модуль, реализующий алгоритм сериализации и десериализации объектов;

— os — модуль, предоставляющий функции для работы с операционной системой;

— numpy — пакет, включающий методы линейной алгебры и массивы;

— tkinter — пакет Python, предназначенный для работы с библиотекой Tk. Библиотека Tk содержит компоненты графического интерфейса пользователя;

— pathlib — модуль, добавляющий функции, связанные с манипуляциями над файлами и папками (создание файлов и т. д.);

— glob — модуль для поиска всех путей, совпадающих с заданным шаблоном в соответствии с правилами, используемыми оболочкой Unix.

Для реализации модуля идентификации по образцу голоса субъекта были использованы следующие инструменты:

— pyAudio — библиотека для работы со звуком;

— wave — модуль для работы с.wav-файлами;

— matplotlib — библиотека для создания визуализации (графики и т. д.);

— librosa — пакет для обработки звука (анализа аудиодорожки);

— numpy — пакет, включающий в себя методы линейной алгебры и массивы;

— py Audio — библиотека для работы со звуком.

Также в разработанном продукте реализовано логирование данных для последующей обработки администратором прокторинговой системы с помощью модуля для работы с архивами — zipfile.

Программа проводит успешную аутентификацию по изображению лица даже при наличии на субъекте головных уборов, очков, бороды, а по голосу — даже при наличии посторонних звуков, шумов. Это преимущество дают алгоритмы машинного обучения, которые позволяют из большого массива данных выявлять требующиеся биометрики и точно идентифицировать субъект.

Разработанное ПО позволяет проходить процедуру идентификации и аутентификации с помощью изображения лица и образца голоса субъекта. В заданные интервалы времени программа сравнивает изображение лица обучающегося, который сидит перед камерой, с образцом, который хранится в базе данных, для проверки подлинности. Программа ведёт логирование для администратора с целью последующего анализа прошедшей сессии, чтобы оценить легитимность действий обучающегося.

Таким образом, программа «Двухфакторная аутентификация» позволяет контролировать аномальную активность субъекта, предотвращая попытки обхода проверки подлинности, а также может быть проинтегрирована в действующие системы прокторинга, повышая эффективность работы при контрольно-оценочных мероприятиях в режиме онлайн-обучения.

Библиографический список

1. ГОСТ Р ИСО/МЭК 19794-5–2013 Информационные технологии (ИТ). Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица (с Изменением N 1)

2. Тумбинская М. В., Асадуллин Н. Ф., Муртазин Р. Р. Моделирование аутентификации пользователей по динамике нажатий клавиш в промышленных автоматизированных системах. Программные продукты и системы. — 2020. — № 2. — С. 266–275.

3. Sengar S. S., Hariharan U., Rajkumar K. Multimodal Biometric Authentication System using Deep Learning Method. 2020 International Conference on Emerging Smart Computing and Informatics (ESCI). pp. 309–312 (2020).

4. Кузнецов Д. А., Дамм В. А., Кузнецов А. В., Басов О. О. Применение многомодальной аутентификации на объектах критической информационной инфраструктуры. Научный результат.

5. Информационные технологии. — 2019. — Том 4, № 3. — С. 48–56.

6. Laamanen M., Ladonlahti T., Uotinen S. Acceptability of the eauthentication in higher education studies: views of students with special educational needs and disabilities. International Journal of Educational Technology in Higher Education. n. 18, a. n. 4 (2021).

7. Devitsyna S. N., Tamara E., Meshkov A. V. Developing Facial Recognition Software to Control Access to Campus Facilities. Innovative Approaches in Computer Science within Higher Education: Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education. pp. 68–76 (2019).