**УДК 004.056.53**

# О ПРИМЕНЕНИИ МЕТОДОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПО БИОМЕТРИКАМ

**Мешков А.В.** ФГАОУ ВО «Севастопольский государственный университет»
**Научный руководитель – кандидат технических наук, доцент Девицына С.Н.**
ФГАОУ ВО «Севастопольский государственный университет»

**Аннотация.** Показаны результаты анализа эффективности методов многофакторной аутентификации по биометрикам субъекта, выбран метод и тип биометрик, приведены результаты программной реализации двухфакторной аутентификации на основе распознавания изображения лица и образца голоса человека. Объектом исследования являются биометрические данные, полученные с помощью фото- и аудиофиксации, методы и системы обработки изображений лица и образцов голоса. Разработаны и представлены программные решения для обеспечения многофакторной аутентификации субъекта.

**Введение.** Информационные технологии (IT) повсеместно используются для повышения уровня защищённости информации в организации. Многие компании относятся к категории объектов с пропускным режимом, поэтому вопросы идентификации и аутентификации являются актуальными, и их решение значительно влияет на безопасность не только объекта, но и информационных ресурсов, и, безусловно, самих сотрудников.
Для доступа на территорию используются различные системы контроля и управления доступом (СКУД), а также фото- и видеофиксация, металлодетекторы и турникеты. При использовании информационных систем организации субъектам, для получения доступа к сервисам, необходимо пройти этап аутентификации. Для повышения точности идентификации и безопасности системы в целом, как правило, используются разные критерии и несколько рубежей для входа или доступа к объекту. Такой способ называется многофакторным и имеет очевидные преимущества перед однофакторной аутентификацией.
Одним из самых распространённых методов дополнительной защиты является ввод одноразового пароля, полученного с помощью специального программного обеспечения (ПО) или посредством телекоммуникационной сети. Так как ПО может быть атаковано злоумышленниками, а сим-карта продублирована в центре оказания услуг телефонной связи какого-либо оператора, соответственно, данные могут быть скомпрометированы и использованы в дальнейшем для совершения мошеннических операций, эти методы становятся уязвимыми. В приведенном исследовании показано, что использование уникальных характеристик человека – его биометрических данных, и выбор типов биометрик для многофакторной аутентификации – актуальная задача, решение которой позволит организации не только повысить защищенность информации и поддерживающей инфраструктуры, но и оптимизировать расходы на внедрение средств защиты.

**Основная часть.** Целью разработки является совершенствование системы защиты информации в организации путем использования интеллектуальной системы 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. Так как однофакторные системы менее надежны, принято решение подобрать виды биометрик и их комбинации для повышения эффективности идентификации субъекта при условии ограничений 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 двухфакторную аутентификацию на основе анализа и сравнения с полученными образцами биометрических данных пользователя.

Для разработки данного ПО был использован высокоуровневый язык программирования общего назначения с динамической типизацией и автоматическим управлением памятью – Python. Кроме того, использованы технологии искусственного интеллекта при обучении нейросети распознаванию биометрик субъекта. Для реализации биометрической идентификации и аутентификации были использованы следующие инструменты:

1. По изображению лица:
   - dlib – библиотека на C++, которая реализует нейросети и face_recognition;
   - face_recognition – модуль для распознавания лица;
   - numpy – методы линейной алгебры и массивы;
   - hdf5py – библиотека для работы с файлами стандарта HDF5;
   - OpenCV – библиотека компьютерного зрения.
2. По образцу голоса:
   - speech_recognition – библиотека для распознавания речи;
   - librosa – для обработки звука;
   - numpy – методы линейной алгебры и массивы;
   - pocketsphinx – библиотека для распознавания речи (оффлайн);
   - Google Speech Recognition – модуль для распознавания речи (онлайн);
   - PyAudio – модуль для работы со звуком.

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 дает нейросеть, которая обучена на большом массиве данных, и позволяет на основе технологий искусственного интеллекта выявлять требующиеся биометрики и точно идентифицировать субъект.

**Выводы.** Разработано программное обеспечение, позволяющее имитировать двухфакторную аутентификацию по биометрикам. Практическое применение разработки возможно не только для аутентификации сотрудников и получения доступа к информационной системе или на территорию объекта. ПО может выявлять нарушителей доступа, тем самым позволяя предотвратить ряд угроз, например, таких как террористические акты или проникновение на охраняемую территорию неустановленных лиц. В силу того, что для внедрения и эксплуатации данного ПО не требуется значительное финансирование, затраты на реализацию разработанного решения не превышают стоимость защищаемой информации, соответственно, ПО может найти своё место на рынке программных продуктов для обеспечения безопасности, в том числе информационной, на предприятиях малого и среднего бизнеса, в государственных учреждениях, учебных заведениях и т.д. Интеграция в существующие системы безопасности позволит повысить эффективность их использования за счет точности идентификации субъекта и дополнительных возможностей контроля территории.

Мешков А.В. (автор)

Девицына С.Н. (научный руководитель)