РАЗРАБОТКА БИОМЕТРИЧЕСКОГО ПРОГРАММНОГО РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОФИСНОЙ ИНФРАСТРУКТУРЕ

Д.С. Калининский, *магистрант*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2023-7-1-197-202

Аннотация. *Данная научная статья посвящена разработке и реализации биометрического программного решения для усиления безопасности в офисной среде. Проведенный анализ требований и особенностей аутентификации с использованием биометрии лица позволил определить ключевые функциональные характеристики системы. Реализованы модули биометрической аутентификации, контроля доступа и мониторинга, а также подготовлено руководство по интеграции решения в офисную инфраструктуру. Работа имеет ценность для специалистов в области информационной безопасности и может служить основой для дальнейшего развития и улучшения систем безопасности в офисных пространствах.*

Ключевые слова: *биометрия лица, аутентификация, офисная безопасность, информационная безопасность, программное решение, интеграция, C#.*

Исследование требований, предъявляемых к программному продукту для аутентификации посредством биометрического распознавания лица

Программный продукт, предназначенный для аутентификации через биометрическое распознавание лица, должен соответствовать следующим критериям [1-4]:

1. Надежность: система должна способна корректно определять пользователя на основе его биометрической информации, исключая возможность ошибочной аутентификации.

2. Безопасность: система должна гарантировать надлежащий уровень защиты персональных данных пользователей. Биометрические данные необходимо шифровать, чтобы исключить возможность их неправомерного использования.

3. Быстродействие и производительность: система должна обеспечивать быструю и эффективную работу, не затрачивая много времени пользователя на процесс аутентификации.

4. Практичность в использовании: система должна быть простой в обращении для пользователей любого уровня технической подготовки и не должна требовать специфических навыков.

5. Адаптивность: система должна быть гибкой, способной адаптироваться под разнообразные условия эксплуатации, такие как освещение и фоновые звуки.

6. Масштабируемость: система должна обладать способностью масштабирования и быть способной обработать большое число пользователей.

7. Компатибельность: система должна быть совместимой с текущей инфраструктурой и программным обеспечением, применяемым в организации.

Соответствие данным требованиям позволит разработать эффективную систему аутентификации на базе биометрии лица, которая будет надежной, безопасной и удобной для использования [5-7].

Разработка модулей и компонентов системы

Для функционирования программной системы, чья архитектура была рассмотрена ранее, требуется разработать пользовательский интерфейс, соответствующий поставленным требованиям.

В начале была создана форма, которая служит для аутентификации специалиста по информационной безопасности компании, чтобы он мог настраивать работу программного обеспечения (ПО). Для этого была разработана форма, показанная на рисунке 1.

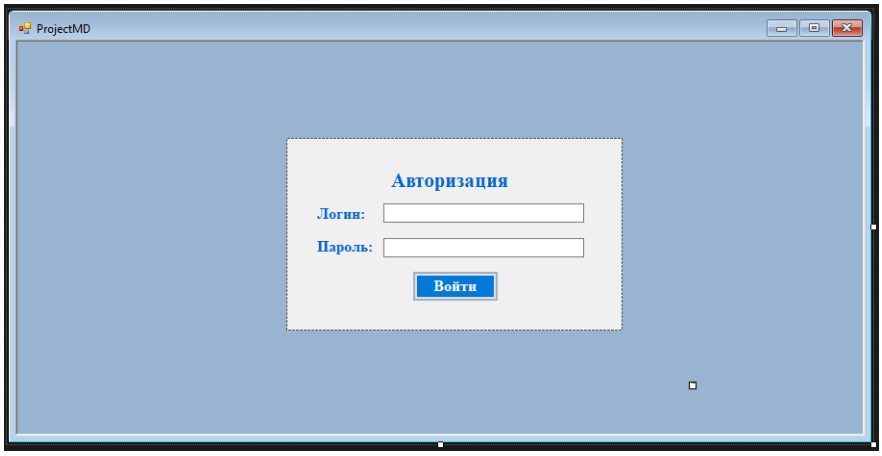

Рис. 1. Начальное окно приложения

Эта форма содержит 2 поля: «Логин» и «Пароль» для аутентификации пользователя, а также кнопку «Войти», которая выполняет проверку введенных данных и позволяет перейти к следующему окну.

Затем требуется форма, где будет представлен функционал программного комплекса (рис. 2).

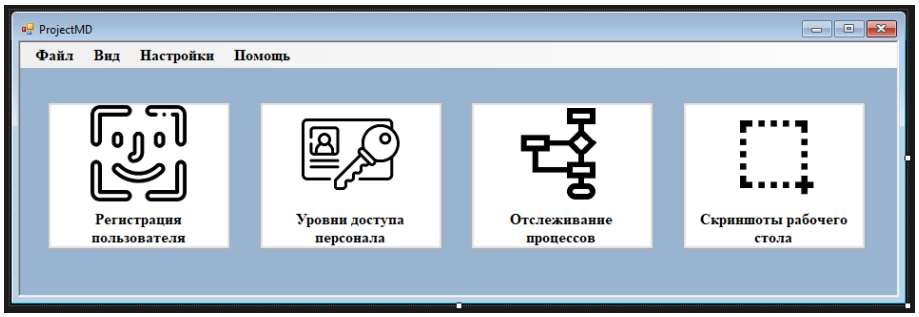

Рис. 2. Меню приложения с выбором функционала

В этой форме реализованы 4 кнопки:

1. Регистрация пользователя;
2. Уровни доступа персонала;
3. Мониторинг процессов;
4. Снимки экрана.

Вышеперечисленные кнопки переводят пользователя в соответствующие формы с требуемым функционалом. Форма также содержит меню, состоящее из следующих пунктов:

1. Файл;
2. Вид;
3. Настройки;
4. Помощь.

Вышеперечисленные функции, которые выполняют вспомогательные функции для более комфортного использования приложения.

Следующая форма используется для сбора биометрических данных пользователя и его регистрации в приложении (рис. 3).

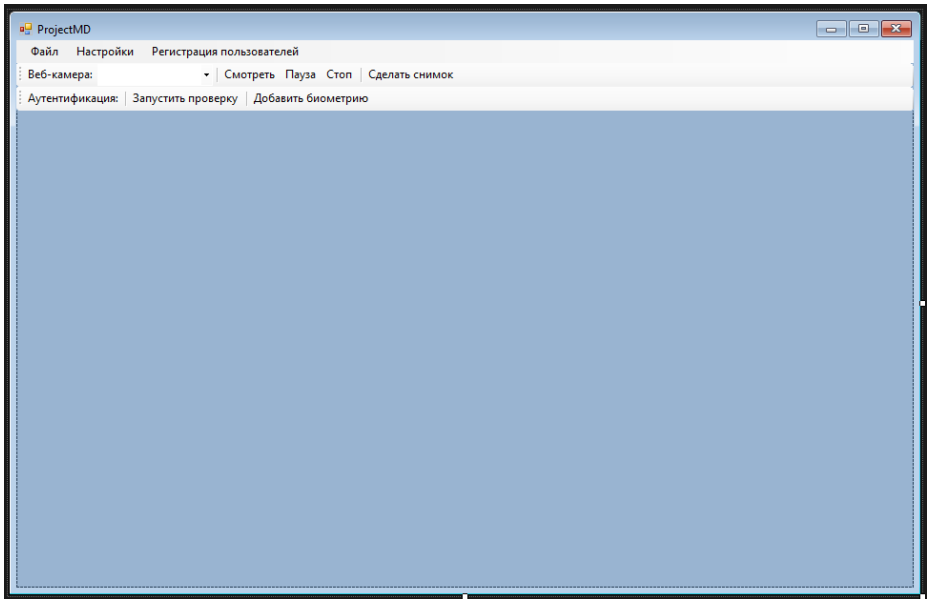

Рис. 3. Окно регистрации пользователя

Эта форма имеет широкий функционал: в ней присутствует форма для выбора камеры, кнопки для ее настройки и кнопки для добавления биометрии пользователя и начала проверки.

Форма «Уровни доступа персонала» содержит функционал, необходимый для создания уровней доступа в компании и распределения приложений, к которым имеет доступ каждый уровень (рис. 4).

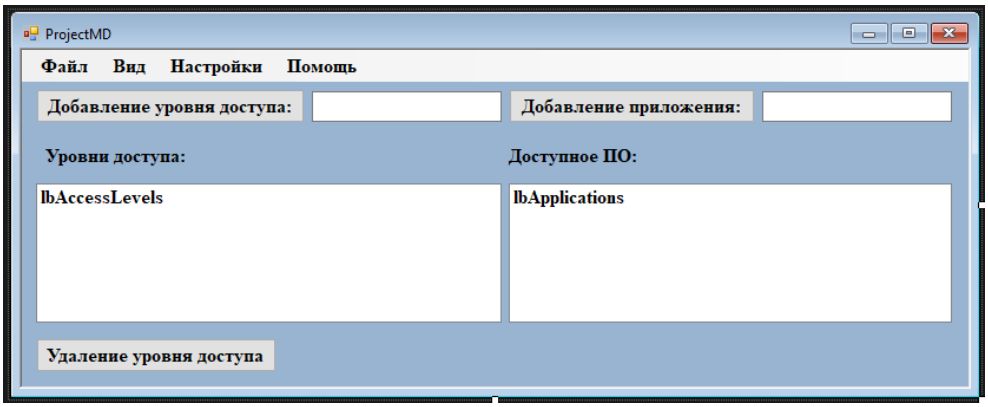

Рис. 4. Окно уровней доступа персонала

В этой форме находятся два текстовых поля для названия уровня доступа и приложения, а также два списка для визуального отображения созданных уровней доступа и приложений, к которым они имеют доступ. На форме также присутствует кнопка для удаления уровней в случае их случайного добавления или если они больше не нужны.

Затем следует форма для отслеживания процессов, интерфейс которой представлен на рисунке 5.

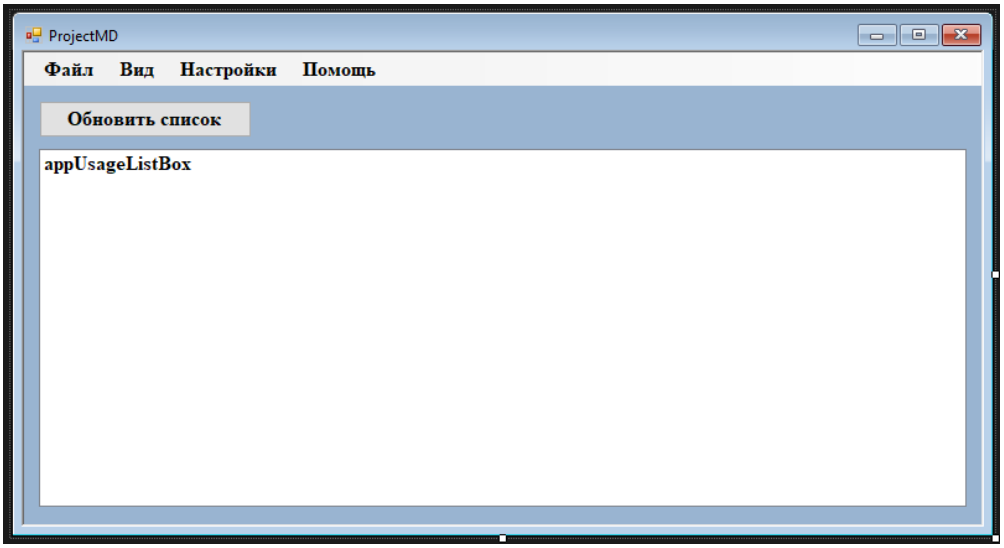

Рис. 5. Окно отслеживания процессов

В данной форме есть одна кнопка для обновления списка процессов, которые были или в данный момент запущены; эти процессы отображаются в списке ниже.

Следующая форма – «Скриншот рабочего стола», где находятся настройки и сохраненные снимки экрана (рис. 6).

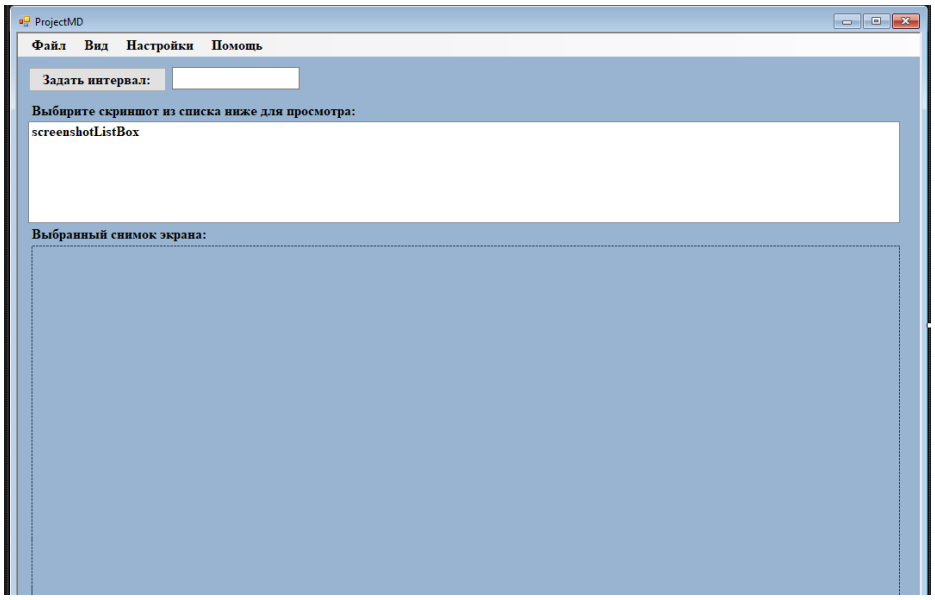

Рис. 6. Окно скриншотов рабочего стола

Оно содержит поле для задания частоты создания скриншотов, а также поле со списком сохраненных скриншотов и поле для просмотра выбранного скриншота.

Кроме уже описанных форм, в проекте имеется дополнительная форма, используемая при сохранении биометрических данных лица пользователя. Она нужна для корректного отображения изображения. Эта форма содержит две кнопки: для сохранения данных и отмены. Также здесь есть поле для предварительного просмотра изображения, чтобы пользователь мог убедиться в его качестве (рис. 7).

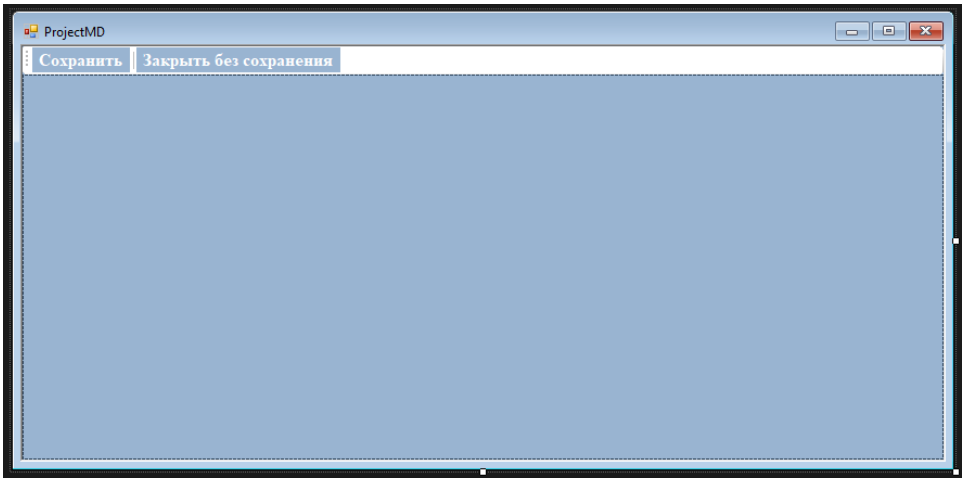

Рис. 7. Окно для сохранения биометрических данных лица сотрудника

Внедрение программного решения в офисную среду

Интеграция представляет собой ключевой этап, так как она обеспечивает взаимодействие программного решения с другими системами и элементами офисной инфраструктуры [8].

На первом этапе интеграции анализируется текущая офисная инфраструктура. Исследуются характеристики и составляющие инфраструктуры, такие как сетевые ресурсы, серверы, рабочие станции и другие устройства. Также проанализируются существующие системы безопасности и программные решения, которые уже применяются в офисе [9].

Затем определяются необходимые действия для внедрения программного решения. Учитываются требования к безопасности, совместимость с уже работающими системами и возможность взаимодействия с ними. Выявляются интерфейсы и протоколы обмена данными между программным решением и другими элементами инфраструктуры [10].

После этого выполняется настройка и конфигурация программного решения с учетом особенностей офисной среды. Задаются необходимые параметры, определяются права доступа и настраиваются соответствующие элементы системы. Также обеспечивается совместимость с уже применяемыми программными решениями и проводится тестирование взаимодействия.

После окончания настройки и конфигурации проводится первичное тестирование программного решения в офисной среде. Проверяются работоспособность, совместимость и безопасность при реальном использовании. Во время тестирования выявляются возможные проблемы и вносятся необходимые исправления [11, 12].

После завершения тестирования и устранения обнаруженных проблем выполняется окончательное внедрение программного решения в офисную инфраструктуру. После успешного внедрения сотрудникам офиса предоставляется инструкция по использованию программного решения, и проводится обучение персонала.

Заключение

В процессе реализации созданного программного решения для обеспечения безопасности офиса, использовался язык программирования C#. Изначально был выполнен анализ требований к программе, способной осуществлять аутентификацию с помощью биометрии лица, что дало возможность выявить основные функции и характеристики будущей системы.

После этого были разработаны различные модули и составляющие системы, включая модули для биометрической аутентификации, контроля доступа, мониторинга и других ключевых функциональных блоков. Для реализации этих модулей применялись соответствующие алгоритмы и технологии.

Затем было составлено руководство для внедрения созданного программного решения в офисную инфраструктуру. Этот процесс включал в себя взаимодействие с уже существующими системами и элемен-

тами офисного окружения, такими как базы данных, серверы аутентификации и другие ключевые компоненты инфраструктуры. Эта интеграция будет способствовать эффективному взаимодействию нового решения с текущими ресурсами и гарантировать его надежную работу в реальных условиях офиса.

Библиографический список

1. Федеральная служба безопасности (ФСБ). – [Электронный ресурс]. – Режим доступа: https://www.fsb.ru/. Дата доступа: 18 мая 2023 г.
2. SANS Institute. – [Электронный ресурс]. – Режим доступа: https://www.sans.org/.
3. National Institute of Standards and Technology (NIST). – [Электронный ресурс]. – Режим доступа: https://www.nist.gov/.
4. OWASP (Open Web Application Security Project). – [Электронный ресурс]. – Режим доступа: https://owasp.org/.
5. CISA (Cybersecurity and Infrastructure Security Agency). – [Электронный ресурс]. – Режим доступа: https://www.cisa.gov/.
6. Microsoft Security. – [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/security.
7. IBM Security. – [Электронный ресурс]. – Режим доступа: https://www.ibm.com/security.
8. Cisco Security. – [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/security/index.html.
9. Kaspersky Lab. – [Электронный ресурс]. – Режим доступа: https://www.kaspersky.com/.
10. Symantec. – [Электронный ресурс]. – Режим доступа: https://www.symantec.com/.
11. McAfee. – [Электронный ресурс]. – Режим доступа: https://www.mcafee.com/.
12. Ross, D.A. Introduction to Cybersecurity: Understanding and Applying Principles and Practices. Wiley, 2018.

DEVELOPMENT OF A BIOMETRIC SOFTWARE SOLUTION FOR SECURITY IN OFFICE INFRASTRUCTURE

D.S. Kalininskiy, *Graduate Student*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *This scientific article is devoted to the development and implementation of a biometric software solution to enhance security in the office environment. The analysis of the requirements and features of authentication using facial biometrics made it possible to determine the key functional characteristics of the system. Modules for biometric authentication, access control and monitoring have been implemented, and a guide for integrating the solution into the office infrastructure has been prepared. The work is of value to information security professionals and can serve as a basis for further development and improvement of security systems in office spaces.*

Keywords: *facial biometrics, authentication, office security, information security, software solution, integration, C#.*