СТЕНД ДЛЯ ИССЛЕДОВАНИЯ НАДЕЖНОСТИ УСТРОЙСТВ БИОМЕТРИЧЕСКОЙ ЗАЩИТЫ

Малахов К.М., Сеньков В.А.,
студенты 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Буевич А.Э., канд. техн. наук, доцент

Ключевые слова. Экспериментальный стенд, несанкционированный доступ, биометрическая защита, надежность, информационная безопасность.

Keywords. Experimental stand, unauthorized access, biometric protection, reliability, information security.

Работа посвящена разработке и исследованию экспериментального стенда для тестирования биометрического навесного замка, предназначенного для обеспечения высокой степени защиты объектов от несанкционированного доступа. В условиях растущих требований к безопасности персональных данных и физических объектов традиционные механические замки становятся недостаточно надежными, что обуславливает необходимость перехода к современным системам биометрической идентификации. Отсутствие стандартизированных методов оценки надежности биометрических систем создает серьезные риски для конечных пользователей и препятствует развитию отрасли в целом. В условиях, когда биометрические замки все чаще используются для защиты критически важных объектов, необходимость разработки научно обоснованной методологии комплексной оценки их надежности приобретает первостепенное значение.

Цель исследования – разработка методологии и конструкции стенда для комплексной оценки надежности устройств биометрической защиты, обеспечивающего объективную и воспроизводимую оценку безопасности навесных биометрических замков на основе единого подхода, учитывающего биометрические, криптографические и механические аспекты.

Материалы и методы. Работа основана на результатах анализа научно-технической информации по устройствам биометрической защиты; экспериментальных работ по исследованию систем биометрической идентификации; использовании методов компьютерного моделирования.

Результаты и их обсуждение. Биометрические системы могут быть классифицированы по физиологическим и поведенческим характеристикам пользователей. Физиологические признаки включают отпечатки пальцев, радужную оболочку глаза, лицо, ДНК, венозный узор кисти, отпечаток ладони. Поведенческие признаки охватывают почерк, голос, походку, динамику набора текста. Для навесных замков наибольшее распространение получили системы, основанные на идентификации по отпечаткам пальцев, что обусловлено их оптимальным соотношением точности, стоимости и удобства использования. Современные биометрические замки используют два основных типа сенсоров для сканирования отпечатков пальцев: оптические и емкостные.

В работе представлено техническое решение, основанное на использовании отпечатков пальцев в качестве биометрического ключа. Система включает в себя микроконтроллер для обработки данных, емкостной сенсор отпечатков пальцев, систему световой индикации и защищенное хранилище биометрических шаблонов. Взаимодействие между модулями осуществляется через централизованную шину данных с использованием протокола CAN (Controller Area Network), обеспечивающего надежную передачу информации в условиях электромагнитных помех. Ключевым элементом архитектуры является управляющий контроллер, который координирует работу всех модулей и обеспечивает синхронизацию измерений. Для тестируемого навесного биометрического замка реализована специальная адаптерная пластина, обеспечивающая механическое и электрическое соединение с испытательным стендом.

Архитектура стенда позволяет проводить комплексное тестирование как аппаратной, так и программной составляющих биометрического замка в различных условиях эксплуатации.

На рисунке изображен стенд для исследования биометрического замка.

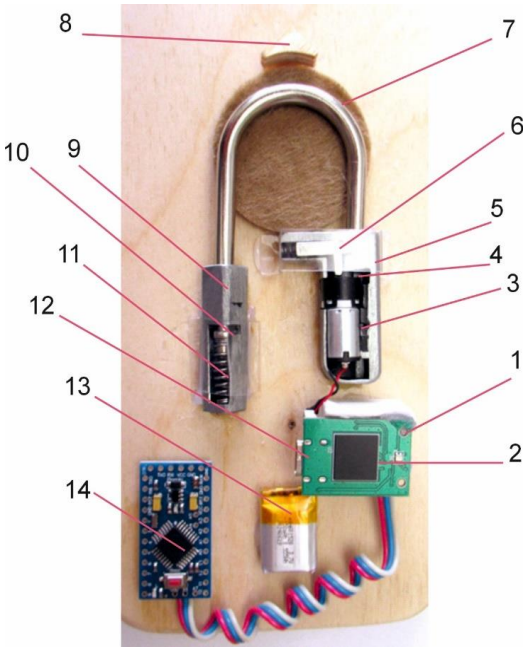

Рисунок – Стенд для исследования биометрического замка: 1– контроллер управления биометрическим модулем, 2– биометрический модуль, 3 – двигатель, 4 – кулачок, 5 – контейнер, 6- штифт замка, 7 – дужка, 8 – упор, 9 – корпус, 10 – фланец, 11 – пружина, 12 – соединительный разъем, 13 – источник питания, 14 – управляющий модуль.

Представленный на рисунке 1 экспериментальный стенд предназначен для комплексного тестирования характеристик навесного биометрического замка. Система смонтирована на деревянной платформе и включает следующие ключевые компоненты

Контроллер управления биометрическим модулем (элемент 1) представляет собой микропроцессорную систему на базе 8-битного AVR-микроконтроллера (например, Arduino Nano или аналогичное решение на базе ATmega328P). Данный компонент выполняет функции центрального управляющего ядра системы. Архитектурно контроллер позволяет реализовать многоуровневую систему безопасности, включающую механизм блокировки после 7-и неудачных попыток верификации, что соответствует рекомендациям NIST IR 8223 (2018) по защите от переборных атак. Время реакции системы на несанкционированные попытки доступа составляет менее 200 мс.

Биометрический модуль (элемент 2) представляет собой специализированную систему обработки биометрических данных, построенную на базе емкостного сенсора.

Исполнительный механизм (элемент 3) - двигатель 3 с кулачком 4 является актуатором, отвечает за перемещение штифта замка 6. Механизм заключен в прозрачный пластиковый контейнер (элемент 5), что позволяет визуально контролировать процесс срабатывания. Ток потребления двигателя достигает 185 мА, что составляет 46.8% от общего энергопотребления системы (по данным экспериментов).

Механическая часть замка (элементы 7–11) состоит из дужки 7, которая имеет арочную форму для крепления на объекте защиты; упора 8, который обеспечивает фиксацию элемента 7 при открывании; корпуса 9 из нержавеющей стали. Внутри корпуса изготовлено отверстие, которое обеспечивает подвижность, за счет пружины 11, удержание дужки 7 за счет фланца 10.

Соединительный разъем 12 (USB-Type-C) предназначен для зарядки и программирования системы.

Источник питания (элемент 13) – литий-полимерная батарея (маркировка "+XH601520 3.7V") обеспечивает энергонезависимую работу системы. Емкость аккумуля-

тора составляет 505 мА·ч, что обеспечивает время автономной непрерывной работы около 60 минут при полной зарядке.

Управляющий модуль (элемент 14) – плата с микроконтроллером (например, Arduino Nano) выполняет функции контроллера отладки, который позволяет, в режиме отладки, координирующего работу всех компонентов. На плате установлены датчики состояния (LED-индикаторы) и интерфейсы для связи с внешними устройствами. Плата обеспечивает сбор данных о параметрах работы системы (напряжение, ток, температура) и передачу их в цифровую обработку.

Конфигурация стенда позволяет моделировать различные сценарии эксплуатации, включая воздействие температуры, влажности и механических нагрузок.

Данная конфигурация служит основой для дальнейших исследований в области биометрической безопасности, включая разработку алгоритмов защиты от spoof-атак и оптимизацию энергоэффективности.

Разработанный стенд обеспечивает поддержку до 15-и зарегистрированных пользователей с возможностью быстрого добавления и удаления биометрических шаблонов. Основные технические характеристики системы включают точность верификации на уровне 98% при среднем качестве сканирования отпечатка, время обработки запроса менее 1-ой секунды и устойчивость к температурным колебаниям в диапазоне от -10°C до +50°C. Система реализует двухэтапный алгоритм верификации: первичная обработка изображения отпечатка с выделением ключевых точек и последующее сравнение с шаблонами в защищенном хранилище с использованием адаптивного порога принятия решения.

Особенностью разработанного стенда является возможность проведения тестов на устойчивость к различным типам атак, включая попытки подмены биометрических данных (spoof-атаки), воздействие внешних помех и анализ криптографической защищенности хранения биометрических шаблонов. Проведенные исследования позволили выявить основные уязвимости системы и предложить методы их устранения, в частности, внедрение дополнительных проверок качества отпечатка и механизмов защиты от подделки.

В работе предложена математическая модель оценки надежности биометрической системы, основанная на вероятностном анализе ошибок первого и второго рода. Модель учитывает такие параметры, как качество сканирования (FQI), порог принятия решения и статистические характеристики распределения биометрических признаков. Экспериментальные данные подтвердили адекватность предложенной модели, что позволяет использовать ее для прогнозирования надежности биометрических систем на этапе проектирования.

Особое внимание уделено анализу энергопотребления системы и разработке алгоритмов энергосбережения, что критически важно для автономных устройств. В результате оптимизации удалось снизить потребляемую мощность на 35% без ущерба для производительности и безопасности системы.

Заключение. Практическая значимость работы заключается в создании методики комплексной оценки надежности биометрических замков, которая может быть применена при разработке и сертификации подобных устройств. Полученные результаты подтверждают, что предложенная система обладает достаточной надежностью для применения в бытовых и коммерческих целях, включая защиту частной собственности, контроль доступа в помещения и обеспечение безопасности персональных данных.

Работа вносит вклад в развитие методов биометрической защиты и может быть использована при создании стандартов оценки надежности подобных устройств, что особенно актуально в свете растущих требований к кибербезопасности и защите персональных данных в современном мире.