*А. Н. Ручай*

# РАЗРАБОТКА УНИВЕРСАЛЬНОГО КОМПЛЕКСА МОДУЛЕЙ ДЛЯ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА В ОС WINDOWS XP НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

## Введение

Биометрическая аутентификация является актуальным направлением современных исследований в области компьютерной безопасности, поскольку она решает целый ряд задач. Одной из таких задач может быть аутентификация в операционной системе (ОС) Windows XP, которая на данный момент все еще является самой популярной ОС в мире.

Системы разграничения доступа на основе биометрической аутентификации имеют большую практическую значимость и преимущества по сравнению с парольными системами [1, 2]:

1. В отличие от пароля биометрическая характеристика является уникальной, неотъемлемой и неотчуждаемой;

2. Затрудняется атака подбора по биометрической характеристике;

3. Биометрическая характеристика не зависит от языка ОС и кодировок символов.

В работах [2, 3] был описан разработанный комплекс модулей биометрической аутентификации для разграничения прав доступа в ОС Windows XP на примере текстозависимой верификации диктора [4, 5]. На основании данных работ можно говорить, что в настоящее время важной является задача разработки универсального комплекса модулей, реализующего разграничение прав доступа в ОС на основе любой биометрической аутентификации. Универсальность модулей заключается в том, что на их базе может быть реализована система разграничения прав доступа, не зависящая от метода аутентификации.

В данной статье будет описан разработанный универсальный комплекс модулей с открытым исходным кодом, реализующий разграничение прав доступа в ОС Windows XP на основе биометрической аутентификации.

## 1. Система биометрической аутентификации

Важным аспектом при реализации и внедрении любых биометрических систем является безопасность их использования. В работах [2, 6] представлен обзор существующих атак и мер защиты, которые относятся к биометрическим системам. Опишем биометрическую систему через общую схему биометрической аутентификации, изображенную на рис. 1. В данной схеме каждый элемент может создавать угрозу, приводящую к реализации атаки, и с каждой угрозой связан свой тип атаки и мера ее предотвращения.

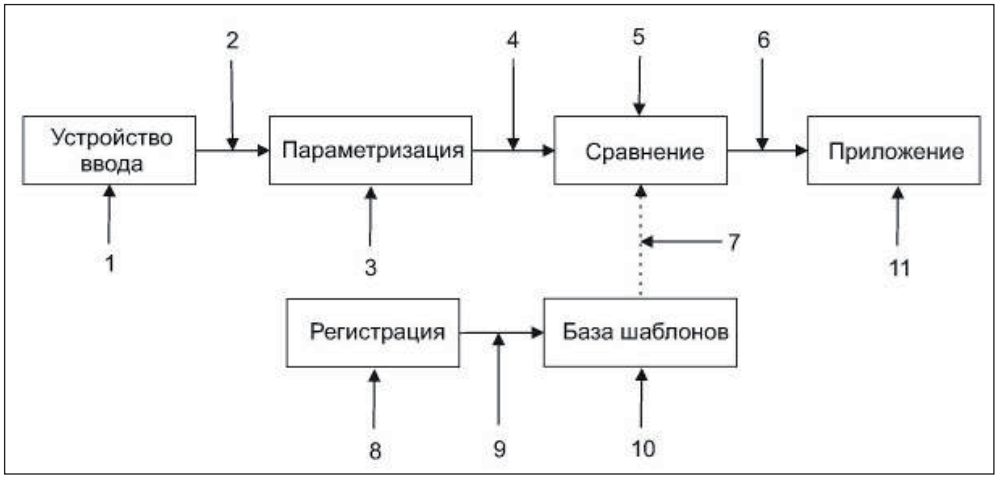


*Рис. 1. Общая схема аутентификации с обозначенными атаками*

Классифицируем все типичные атаки, связанные с уязвимостями элементов системы биометрической аутентификации:

1. Атака на устройство ввода;
2. Атака на канал связи между сенсором и биометрической системой;
3. Атака на параметризацию речевого сигнала;
4. Атака на канал передачи параметризованного сигнала;
5. Атака на элемент сравнения вектора параметра и шаблона;
6. Атака на результат сравнения;
7. Атака на канал связи с базой шаблонов;
8. Атака на элемент регистрации пользователя;
9. Атака на канал между элементом регистрации и базой шаблонов;
10. Атака на элемент базы шаблонов;
11. Атака на приложение.

Все перечисленные выше атаки, кроме атаки на устройство ввода, являются общими для всех биометрических систем. Защита от подобных атак заключается в использовании цифрового кодирования, временных меток и шифрования открытого канала передачи данных. Иными словами, необходимо создавать специальные криптографические протоколы, позволяющие устранить возможность различных атак. Также применяют специальные технологии:

- для повышения безопасности биометрических систем применяют различные подходы к организации базы данных шаблонов и к структуре шаблона;
- для повышения надежности биометрических систем используют многофакторную аутентификацию;
- для устранения проблемы конфиденциальности и защиты информации используют специальную технологию сокращения биометрических параметров и «шифрования личности».

Однако угроза атаки на устройство ввода биометрической системы является актуальной и требует дополнительных мер предотвращения.

На основе анализа существующих атак и защиты [2, 6] можно сделать вывод, что система разграничения прав доступа должна быть реализована с клиент-серверной моделью взаимодействия, что дает следующие преимущества:

- повышается общая безопасность системы;
- один мощный сервер может одновременно обслуживать множество клиентов;
- обеспечивается минимальная нагрузка на компьютер клиента;
- сводится к минимуму количество клиентских настроек;
- сервер можно переносить под любую ОС, а клиентские части останутся неизменными;
- клиентскую часть также можно написать под другую ОС, а сервер останется неизменным.

## 2. Описание разработанного комплекса модулей

Реализованный комплекс состоит из трех модулей: модуль обучения и переобучения, модуль аутентификации и модуль администрирования.

Модуль аутентификации был реализован на основе библиотеки GINA (Graphical Identification and Authentication) для ОС Windows XP. Стандартная библиотека GINA (Msgina.dll) реализует интерфейс для входа в систему по умолчанию. Однако разработчики могут включать свои GINA DLL, реализующие другие механизмы аутентификации вместо стандартного метода.

**Модуль обучения и переобучения**

1. Вводятся логин, пароль. В ОС регистрируется пользователь с выбранными правами.

2. Вводится 5—10 раз биометрическая характеристика.

3. Происходит процедура параметризации, после чего формируются шаблоны, проверяются их близость и похожесть.

4. В СУБД сохраняются имя пользователя и шаблон. Активируются статус допуска, время блокировки, пороговое значение.

5. В системе определяется пороговое значение, общее для всех пользователей. Данное значение может индивидуально меняться для каждого пользователя и может запускаться по какому-то регламенту из модуля администрирования.

6. В журнал логов заносится информация об этих событиях.

**Модуль верификации**

1. При входе в систему пользователь предъявляет логин, который был создан на этапе обучения. Система предварительно проверяет, существует ли данный пользователь в системе и базе.

2. Вводится один раз биометрическая характеристика, которая сохраняется в файл. Затем данный файл вместе с именем пользователя отправляется на сервер по безопасному протоколу SSL.

3. Сервер выполняет процедуру верификации. В случае неуспешной верификации должен быть указан номер попытки. Если неудачных попыток было больше трех, то система блокирует вход на 30 минут.

4. Ведется журнал логов с успешными и неуспешными попытками, указывается, какие пользователи заблокированы и на какое время. При необходимости может сохраняться файл с биометрической характеристикой неуспешной попытки для установления личности злоумышленника или исследования причин ложного срабатывания.

**Модуль администрирования**

1. Настройка порогового значения.

2. Получение порогового значения, может запускаться по какому-то регламенту из модуля администрирования.

3. Управление учетными данными пользователей.

4. Управление и просмотр журнала логов, создание отчетов.

Для системы аутентификации было решено использовать свободно распространяемую систему управления баз данных (СУБД). СУБД MySQL была выбрана на основе целого ряда причин: она легковесна, свободно распространяема, бесплатна, кроссплатформенна и хорошо интегрируется с множеством IDE-сред. Также удобство хранения в БД заключается в том, что возможен одновременный доступ как для модуля аутентификации, так и для модуля администрирования. Кроме того, СУБД MySQL проста в управлении и применяется повсеместно.

Зададим структуру базы данных, которая будет состоять из следующих 6 таблиц:

1. Users — основная таблица, где хранятся идентификатор пользователя, его имя и метка активности;

2. Passwords — таблица для хранения паролей пользователей;

3. Templates — таблица для хранения шаблонов пользователей;

4. Thresholds — таблица для хранения порогового значения;

5. Blocked — таблица для хранения информации о блокировании пользователей;

6. AddInfo — таблица для хранения дополнительной информации о пользователях.

Связи между таблицами в виде схемы изображены на рис. 2.

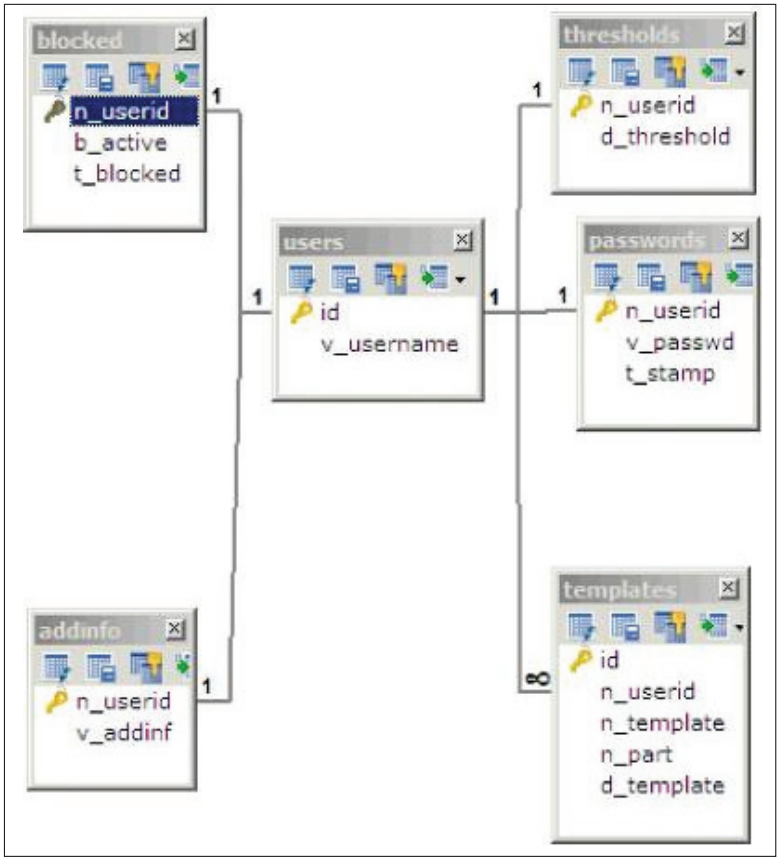


*Рис. 2. Схема базы для хранения данных аутентификации*

Система разграничения прав доступа была реализована с клиент-серверной моделью взаимодействия, в которой в качестве сервера аутентификации был выбран Windows-сервис. Сервисы могут автоматически стартовать до входа пользователя в ОС, а значит, можно использовать это решение как на компьютерах в локальной сети, так и на независимых машинах. Сервисы удобны еще и тем, что это стандартный интерфейс для служебных приложений в ОС семейства Windows NT.

Остановить или запустить сервис может лишь пользователь, обладающий необходимыми правами в ОС. Тем самым также решается проблема неавторизованного доступа к системе.

Работа сервиса заключается в том, что сначала он прослушивает порт, указанный в реестре, и если произошло соединение, то создаются новый поток и сокет, в котором передаются имя пользователя и файл с биометрической характеристикой.

Поскольку все данные передаются по сети, необходимо было обеспечить их конфиденциальность и невозможность изменения. Для этого был использован протокол безопасных сокетов OpenSSL. Также создание новых процессов было заменено на создание новых потоков, так как потоки расходуют меньшее количество памяти, а их производительность выше, поскольку в Windows поток — уже готовая последовательность команд, а процесс — лишь контейнер потоков.

Интерфейс для модуля администрирования был разработан в среде Microsoft Visual C++ 2008 SP1 с использованием MFC (Microsoft Foundation Classes).

В завершение была создана удобная среда для модифицирования всех модулей, а также общий пакет для создания конечного установщика модулей в ОС Windows XP.

**Выводы**

Были подготовлены эффективные и удобные инструменты для решения задачи развертывания системы, реализующей разграничения прав доступа пользователей в ОС Windows XP на основе любой биометрической аутентификации. Использование описанных в работе модулей позволит успешно и без приобретения дополнительных инструментов решать проблему разграничения прав доступа.

Разработанный универсальный комплекс модулей разграничения прав доступа в ОС Windows XP на основе текстозависимой верификации диктора успешно прошел тестирование на кафедре компьютерной безопасности и прикладной алгебры Челябинского государственного университета [2, 3].

## СПИСОК ЛИТЕРАТУРЫ:

1. *Болл Р. М., Коннел Дж. Х., Панканти Ш., Ратха Н. К., Сеньор Э. У.* Руководство по биометрии. М.: Техносфера, 2007. — 368 с.
2. *Ручай А. Н.* Текстозависимая верификация диктора: математическая модель, статистические исследования, комплекс программ. Saarbrucken: LAP LAMBERT Academic Publishing, 2012. — 144 с.
3. *Ручай А. Н.* Разработка комплекса модулей для разграничения прав доступа в ОС Windows XP на основе биометрической аутентификации // Информационные технологии и системы: материалы Первой Междунар. конф., Банное, Россия. 28 февраля — 4 марта 2012 г. Челябинск: ЧелГУ, 2012. С. 75—76.
4. *Ручай А. Н.* Формантный метод текстозависимой верификации диктора // Вестник Челяб. гос. университета. Математика. Механика. Информатика. 2010. № 23 (204). Вып. 12. С. 121—131.
5. *Ручай А. Н.* Улучшение надежности формантного метода текстозависимой верификации диктора с помощью нового метода сегментации сигнала // Доклады ТУСУР. 2011. № 2 (24). С. 241—246.
6. *Ручай А. Н.* Модель атак и защиты биометрических систем распознавания диктора // Доклады ТУСУР. 2011. № 1 (23). С. 96—100.