

Решетников Д.В.

*Научный руководитель: к.т.н, доцент каф. СГПД М.В. Макаров
Муромский институт (филиал) федерального государственного образовательного
учреждения высшего образования «Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: student.reshetnikov@mail.ru*

Обзор и анализ механизма распознавания радужной оболочки глаза для систем аутентификации пользователей с использованием технологии Windows Hello

Целью данной работы является обзор и анализ механизма распознавания радужной оболочки глаза для систем аутентификации пользователей с использованием технологии Windows Hello.

Основной параметр деятельности всех биометрических систем распознавания радужной оболочки состоит в том, что при сканировании области глаза захватывается район зрачка и самой радужной оболочки. При этом радужная оболочка настолько неповторимый параметр, что даже не самый удачный в плане шумов или чёткости снимок даст достоверный результат. Отсканированная область с помощью вшитого программного обеспечения очищается от шумов и бликов, которые исходят, например, от очков. Далее считанная информация охватывается в прямоугольный формат – Iris Code, который несёт всю информацию о персональных параметрах объекта в черно-белом виде, подобно штрих-коду. Далее Iris Code проверяет изображение по готовой базе с хранящимися в системе шаблонами. Скорость обрабатываемых данных при этом крайне высокая, что позволяет применять систему для работы с большими базами данных, в том числе выполняя задачи правоохранительных органов и различных государственных организаций.

Более подходящую под обычных пользователей технологию биометрической аутентификации разработали в компании Microsoft. Их система под названием Windows Hello, помимо основных методов аутентификации, например, по отпечатку пальца или по голосу, так же имеет в своём составе сканирование радужной оболочки глаза.

Для использования сканирования необходима только соответствующая камера, поддерживающая данную технологию. Кроме камеры нужен светодиод и датчик, которому будет поступать отраженная информация. Как правило, глаз освещается инфракрасными лучами таким образом, чтобы камера смогла отсканировать оболочку.

Windows Hello может использоваться не только для входа в свой профиль, но и при авторизации в приложениях, корпоративных сервисах и на сайтах, что существенно повышает защиту персональных данных. При этом разработчикам сторонних приложений вовсе не нужно разбираться в шифровании, биометрике или технологии работы с учетными записями Microsoft.

Для анализа системы был выбран ряд основных критериев:

1. Безопасность – позволяет оценить вероятность того насколько сложно обмануть систему и получить несанкционированный доступ. В результате эксперимента Windows Hello ни разу не допустил в систему ложного близнеца.

2. Возможность перехвата данных по сети. Все полученные данные хранятся в локальной базе данных Windows Hello на устройстве пользователя для безопасности от хакеров. Они не перемещаются и не передаются на внешние устройства или серверы.

3. Доступность. Технология Windows Hello может использоваться в обычных пользовательских ноутбуках, смартфонах и планшетах. Стоимость данных девайсов в разы ниже, чем специальных аппаратов на производственных или государственных службах.

4. Простота и удобство в использовании. Любой пользователь может настроить для себя данную технологию распознавания радужной оболочки глаза без любых проблем с помощью имеющихся в свободном доступе документаций.

В результате анализа были выявлены следующие достоинства данной технологии, приведенные в таблице 1.

Таблица 1. Результаты анализа технологии Windows Hello

Технология	Безопасность	Возможность перехвата данных по сети	Доступность	Простота и удобство в использовании
Система аутентификации пользователей с использованием технологии Windows Hello	Windows Hello допускает ошибку реже чем 1 раз в 100000	Все данные хранятся на локальном устройстве.	Доступен каждому обычному пользователю	Максимальная для пользователя

В результате проведенного исследования было выяснено, что выбранная технология распознавания радужной оболочки глаза для аутентификации пользователей с использованием системы Windows Hello отвечает всем необходимым требованиям пользователя. Она сочетает надёжную безопасность с доступностью и простотой, необходимую для обычного пользователя.

Литература

1. Аутентификация по радужной оболочке глаза [Электронный ресурс] // wikipedia.org: интернет портал URL: [https://ru.wikipedia.org/wiki/Аутентификация по радужной оболочке глаза](https://ru.wikipedia.org/wiki/Аутентификация_по_радужной_оболочке_глаза) (дата обращения: 7.04.2017).
2. Управление проверкой личности с помощью Windows Hello [Электронный ресурс] // habrahabr.ru. URL: <https://habrahabr.ru/company/microsoft/blog/314822/> (дата обращения: 7.04.2017).
3. Р. М. Болл, Дж. Х. Коннел, Ш. Панканти, Н. К. Ратха, Э. У. Сеньор. РУКОВОДСТВО ПО БИОМЕТРИИ. - Издательство: Техносфера, Серия: Мир цифровой обработки, Год издания: 2007.