СРАВНЕНИЕ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО СОВОКУПНОСТИ ПОКАЗАТЕЛЕЙ КАЧЕСТВА

Безрук В.М., Кобцева В.М., Скорик Ю.В.
Кафедра Информационно-сетевая инженерия, ХНУРЕ, г. Харьков, Украина,valerii.bezruk@nure.ua

Аннотация - Рассматриваются методы биометрической аутентификации, используемые для защиты информации в компьютерных сетях. Проводится сравнительный анализ основных методов с учетом совокупности показателей качества.

Ключевые слова – безопасность, биометрическая система, идентификация, биометрические методы.

I. Введение

Быстрое развитие информационных технологий требует постоянного совершенствования систем защиты информации. Обеспечение безопасности в компьютерных сетях - это условие защиты конфиденциальных данных от различного рода угроз.

Существует большое разнообразие методов идентификации. В основе наиболее распространенных технологий верификации и идентификации лежит использование паролей и персональных идентификаторов (личный идентификационный номер-PIN) или документов типа паспорта, водительских прав. Однако такие системы слишком уязвимы и могут легко пострадать от подделки, воровства и других факторов. Поэтому все больший интерес вызывают методы биометрической идентификации, позволяющие определить личность человека по его физиологическим характеристикам путем распознания по заранее сохраненным образцам [1-6].

Биометрические системы доступа являются весьма удобными для пользователей и надежными для защиты информации. Основными преимуществами биометрических технологий являются следующие факторы:

- избавление пользователей от проблем, связанных с потерей ключей и удостоверений личности, а также от необходимости запоминать идентификационный код и пароли;
- уникальность биометрических характеристик каждого человека делает невозможным их использование третьими лицами;
- процесс общения пользователя с биометрическим сканером происходит легко и требует минимальных временных затрат;
- процесс распознавания, благодаря интуитивности программного и аппаратного интерфейса, понятен и доступен людям любого возраста и не знает языковых барьеров;
- в случае каждого обращения к системе можно доказать авторство того или иного действия, например, сохранить биометрические данные злоумышленника.
- предотвратить проникновение злоумышленников на охраняемые территории и в помещения за счет подделки, кражи документов, карт, паролей;
- ограничить доступ к информации и обеспечить персональную ответственность за ее сохранность;
- обеспечить допуск к ответственным объектам только сертифицированных специалистов;

Поэтому существует необходимость сравнительного анализа различных биометрических методов и соответствующих систем аутентификации с учетом совокупности показателей качества.

II. Сравнительный анализ биометрических систем методом анализа иерархий

Проанализированы сравнительные характеристики разных статических биометрических методов, которые приведены в работах [1-9]. Для оценки качества работы биометрических систем выбраны характеристики, по которым можно получить количественные показатели создаваемых биометрических систем.

При сравнении систем выбраны следующие показателя качества: коэффициент ложного пропуска (FAR), т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе и коэффициент ложного отказа (FRR), т.е. процент отказа в доступе настоящему пользователю системы. Оба параметры рассчитываются методами математической статистики. Чем меньше значения этих показателей, тем выше качество аутентификации пользователей. Рассмотрены также и другие показатели качества систем, в частности, вероятность того, что система ошибается в определении совпадений между входным образцом и соответствующим шаблоном из базы данных (FNMR); относительная рабочая характеристика (график ROC) - это визуализация компромисса между характеристиками FAR и FRR; коэффициент отказа в регистрации (FTE или FER) – коэффициент безуспешных попыток создать шаблон из входных данных; коэффициент ошибочного удержания (FTC) - вероятность того, что автоматизированная система не способна определить биометрические входные данные, когда они представлены корректно; ёмкость шаблона - максимальное количество наборов данных, которые могут храниться в системе; устойчивость к подделке - эмпирическая характеристика, обобщающая то, насколько легко обмануть биометрический идентификатор, устойчивость к окружающей среде - характеристика, эмпирически оценивающая устойчивость работы системы при различных внешних условиях.

В частности, с использованием метода анализа иерархий проведено многокритериальное сравнение и выбор предпочтительного варианта для самых популярных систем биометрической идентификации на основе анализа отпечаток пальца, распознавания лица 2D, радужной оболочки глаза, сетчатки глаза, рисунка вен, клавиатурного почерка, голоса. При этом рассмотрен случай сравнительного анализа и выбора предпочтительного типа системы биометрической идентификации с учетом показателей качества в виде средних значений FAR и FRR.

Метод анализа иерархий (МАИ) состоит в декомпозиции проблемы выбора предпочтительного проектного варианта некоторой системы на простые составляющие части и получении суждений экспертов по парным сравнениям различных элементов проблемы выбора - показателей качества и вариантов системы [10]. Принцип сравнительных суждений экспертов в МАИ состоит в том, что объекты проблемы выбора сравниваются экспертами попарно по важности. Попарно сравниваются важности разных показателей качества и важности разных вариантов системы. В результате обработки полученных от экспертов матриц парных сравнений согласно определенной математической процедуры получают компоненты вектора глобальных приоритетов, значения которых характеризуют приоритетность выбора предпочтительного варианта системы из заданного множества вариантов.

Для вычисления вектора глобальных приоритетов сравниваемых вариантов системы выполняется обработка матриц парных сравнений альтернатив. Вычисляются компоненты главного собственного вектора V_j матрицы и вектора

приоритетов P_j на каждом уровне иерархии согласно соотношениям

$$P_j = \frac{V_j}{S}, \quad V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}}, \quad S = \sum_{j=1}^{n} V_j, \quad j = \overline{1,n}. \qquad (1)$$

где n – число сравниваемых элементов на каждом уровне иерархии.

С использованием этих данных вычисляются значения компонентов вектора глобальных приоритетов

$$C_j = \sum_{i=1}^{n} P_i Q_{ij} \qquad (2)$$

где Q_{ij} - векторы приоритетов систем, вычисленные согласно (1) по отношению к каждому показателю качества.

По максимальному значения компонентов вектора глобальных приоритетов (2) выбирается единственный предпочтительный вариант системы.

В табл. 1 представлены значения показателей качества для разных биометрических систем [2,4].

ТАБЛИЦА 1

Показатели качества ложного пропуска и ложного отказа для различных типов биометрической системы

№	Система на основе анализа:	FAR	FRR
N1	отпечатка пальца	0,001%	0,6%
N2	распознавания лица 2D	0,1%	2,5%
N3	распознавания лица 3D	0,0005%	0,1%
N4	радужной оболочки глаза	0,00001%	0,016%
N5	сетчатки глаза	0,0001%	0,4%
N6	рисунка вен	0,0008%	0,01%
N7	клавиатурного почерка	0,01%	3,0%
N8	голоса	1%	3%

В табл. 2 приведены вычисленные значения компонент вектора приоритетов вариантовсистем по отношению к каждому показателю качества, а также компоненты вектора глобальных приоритетов.

ТАБЛИЦА 2

Вычисление компонент вектора глобальных приоритетов

Тип системы	Q_{i1}	Q_{i2}	C_j
N1	0,071	0,075	0,077
N2	0,025	0,037	0,031
N3	0,153	0,157	0,165
N4	0,35	0,349	0,373
N5	0,108	0,112	0,117
N6	0,235	0,239	0,252
N7	0,044	0,018	0,036
N8	0,012	0,015	0,014
P_j	0,667	0,399	

Как следует из табл. 2 максимальному значению компонент вектора глобальных приоритетов соответствует предпочтительный тип биометрической системы N4 на основе анализа радужной оболочки глаза,

III. Выводы

1. Рассмотрен многокритериальный поход к сравнительному анализу разных биометрических методов идентификации с учетом совокупности показателей качества.

2. Приведены результаты многокритериального анализа и выбора предпочтительного варианта биометрической системы контроля доступа с использованием метода анализа иерархий.

3. Получено, что с учетом показателей качества ложного пропуска и ложного отказа предпочтительной является биометрическая система на основе анализа радужной оболочки глаза.

IV. Список литературы

1 Сайт ИТНУИТ [Электронный ресурс] Режим доступа: www/ URL https://www.intuit.ru/studies/courses/10620/1104/lecture/24041 -28.03.2019г

2 Вихман В.В. Биометрические системы контроля и управления доступом в задачах защиты информации : учебно-метод. пособие / В.В. Вихман, А.А. Якименко. – Новосибирск: Изд-во НГТУ, 2016. – 54 с.

3 Сайт Techportal.ru [Электронный ресурс] Режим доступа: www/ URL http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html -28.03.2019г.

4 Лебеденко Ю. И.Биометрические системы безопасности. - Тула: Изд-во ТулГУ, 2012. - 160 с.

5 Сайт Современные биометрические методы идентификации [Электронный ресурс] Режим доступа: www/ URLhttp://masters.donntu.org/2013/fknt/fomenko/library/article4.htm - 28.03.2019г

6. Яндиев И. Б. Исследование временных характеристик клавиатурного почерка для быстрой аутентификации личности // Молодой ученый. - 2017. - №14. - С. 154-158.

7. Сайт Биометрия [Электронный ресурс] Режим доступа: www/URL https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%8F - 28.03.2019г.

8. Матвеев Ю.Н. Технологии биометрической идентификации личности по голосу и другим модальностям / Вестник МГТУ им. Н.Э. Баумана. 2012. с. 46-61

9. Юсупов О. Р. Сравнительный анализ возможности использования технологий биометрической идентификации // Молодой ученый. 2016. №19. С. 118-121.

10. Безрук В.М., Чеботарьова Д.В., Скорик Ю.В. Многокритериальный анализ и выбор средств телекоммуникаций: Монография. – Харьков: ФОП Коряк С.Ф., 2017. – 268с.