СПИСОК ЛИТЕРАТУРЫ:

1. http://gtmarket.ru/news/2012/06/19/4439 (дата обращения: 13.12.2012).
2. http://hdrstats.undp.org/en/indicators/103706.html (дата обращения: 13.12.2012).
3. http://espanol.doingbusiness.org/~/media/fpdkm/doing%20business/documents/profiles/country/YEM.pdf (дата обращения: 13.12.2012).
4. http://thewebindex.org/data/index/ (дата обращения: 13.12.2012).
5. http://ru.wikipedia.org/wiki/Кат (дата обращения: 13.12.2012).

А. П. Никитин

МОДЕЛЬ СИСТЕМЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПО ЕГО «КЛАВИАТУРНОМУ ПОЧЕРКУ»

Целью работы является построение теоретической модели системы идентификации пользователей, основанной на применении динамических биометрических параметров.

Данной теме посвящено значительное количество работ, однако ряд их носит сугубо теоретический характер, задачей других является аутентификация пользователя. Также в некоторых работах отмечаются ошибки как первого, так и второго рода, затрудняющие практическое использование предложенных схем. Причиной этого является рост объемов текстов и/или длительности обучения.

Необходимость системы идентификации пользователя возникает в целом ряде случаев, например, когда стоит задача идентификации «анонимных» пользователей в сети Интернет. Вторым применением данной системы может быть мониторинг пользователей в процессе их работы за компьютером с целью предотвращения НСД в систему через АРМ, на которых уже выполнена аутентификация пользователей другими методами.

Наиболее перспективным методом решения данной задачи представляется использование «клавиатурного» почерка, т. е. характерных особенностей работы пользователя с клавиатурой, которые позволяют однозначно идентифицировать пользователя.

Система идентификации, предложенная в данной работе, имеет клиент-серверную архитектуру и состоит из двух компонентов — клиентской части, предназначенной для сбора статистики по клавиатурному «почерку», и серверной части, предназначенной для выполнения следующих функций:

- построение на основе собранных статистических данных образов «почерка»,
- хранение образов,
- сопоставление полученного образа с имеющимися в базе,
- принятие решения об идентификации пользователя на основании сравнения полученного образа его «почерка» с уже имеющимися в базе данных.

Клиентская часть комплекса реализуется с использованием приложений уровня ядра, перехватывающих сообщения драйвера клавиатуры.

Серверная часть производит первичную обработку полученных от клиента данных. Затем происходит построение образа пользователя. Далее полученный образ последовательно сопоставляется со всеми имеющимися в базе образами.

Также предлагается метод идентификации пользователей по «клавиатурному почерку», основанный на применении статистических критериев. Данный метод обладает рядом положительных особенностей:

- высокая надежность идентификации,
- простота реализации,
- независимость от языка, на котором осуществляется ввод текста,
- нечувствительность к аппаратной составляющей системы,
- возможность идентификации пользователя по произвольному тексту,
- отсутствие необходимости в предварительном обучении системы, достаточно создания только одного контрольного образа для каждого пользователя.

СПИСОК ЛИТЕРАТУРЫ:

1. *Трушина Е. А.* Идентификация пользователя ЭВМ по клавиатурному почерку как метод защиты от несанкционированного доступа. 1997. //Электронный источник, опубликовано на сайте http://www.securityclub.ru/
2. *Иванов А. И.* Нейросетевые алгоритмы биометрической идентификации личности / Научная серия «Нейрокомпьютеры и их применение». Кн. 15. Ред. А. И. Галушкин. М.: Радиотехника, 2004. — 143 с.
3. ГОСТ Р 52633-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».

А. Н. Ручай

ПРОТОТИП ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА НА ОСНОВЕ ИЗБИРАТЕЛЬНОЙ МНОГОФАКТОРНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Разработчики и исследователи биометрических систем предлагают программные реализации на основе, как правило, только одной биометрической характеристики без дополнительных инструментов и модулей, что создает проблемы при их использовании и эксплуатации [1].

В зависимости от разных условий и факторов, в частности от доступности электронных средств, удобства, стойкости к атакам и уязвимостям, болезней или увечий пользователей, может быть выбрана биометрическая аутентификация на основе любых таких биометрических характеристик, как ритм ввода пароля, голос, динамика подписи и графическое распознавание. Например, если необходимо разграничить права доступа в изолированном помещении без посторонних, то может быть использована аутентификация по голосу, по ритму ввода пароля или графическому распознаванию. Если помещение, наоборот, не обладает такими условиями, то аутентификация может быть осуществлена на основе ритма ввода пароля или по динамике подписи. Для осуществления аутентификации в мобильных или сенсорных устройствах может быть выбрана аутентификация по ритму ввода пароля, по динамике подписи или графическому распознаванию. На пропускных пунктах возможна аутентификация по динамике подписи.

В настоящее время актуальной является задача разработки универсальных модулей, реализующих разграничение прав доступа на основе биометрической аутентификации [2]. Данная