УДК 612.087.1:57.087.1

И.Ш. Невлюдов, С.В. Пшеничных, О.Н. Пастушенко

Харьковский национальный университет радиоэлектроники, Харьков

АНАЛИЗ ТЕНДЕНЦИЙ В РАЗВИТИИ СИСТЕМ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ И СЕТЕЙ

Анализируются современные системы аутентификации. На основании критерия эффективность/стоимость предпочтение отдается голосовым системам аутентификации. Рассмотрены их преимущества и недостатки. В отличие от известных решений, предложено регистрацию голосового сигнала осуществлять с помощью двух разнесенных в пространстве микрофонов. Указанное решение позволит не только реализовать пространственно-временную обработку, схема которой представлена, но и более тонко восстановить структуру регистрируемого сигнала в условиях наличия помеховых и шумовых сигналов.

Ключевые слова: *анализ, аутентификация, биометрия, голос, защита, идентификация, сигнал*

Введение

Постановка задачи в общем виде. В последние десятилетия значительный рост производительности вычислительных средств, развитие телекоммуникационных систем и технологий передачи, обработки и хранения данных стимулировали активный перенос все большего числа экономических, социальных и межличностных процессов в электронную сферу. При этом значительное число предприятий и организаций по всему миру используют компьютерные системы для управления производственными процессами и персоналом, распределения ресурсов, подключения удаленных пользователей, стратегического и тактического планирования действий и т.д. Современные организации все чаще сталкиваются с такими реалиями, как повышение мобильности рабочей силы, ужесточение законодательства и появление новых угроз, затрагивающих конфиденциальную информацию и интеллектуальную собственность, которая храниться в электронном виде.

Безусловно, использование информационных технологий имеет ряд очевидных преимуществ – это снижение накладных расходов, ускорение производственных процессов, повышение мобильности и оперативности доступа к информации и услугам, а также, возможно, создание определенного имиджа организации. Кроме того, в последние годы сформировался рынок таких услуг, которые ранее просто не существовали, например, удаленное управление банковскими счетами, заказ и оплата товаров и услуг, получение специальной информации и новостей и т.д. Как следствие данных процессов весьма значительно выросла стоимость информации циркулирующей в корпоративных и глобальных компьютерных сетях. В качестве подтверждения данного утверждения можно привести среднегодовые результаты котировок индекса NASDAQ Computer Index, отражающего суммарную стоимость акций ряда компаний занятых в сфере информационных технологий, который за десять лет растет более чем в 10 раз [1, 2].

Одновременно следует иметь в виду, что слабая защита вычислительных систем и сетей на основе только паролей уже не способна остановить умелых кибер-преступников и больше не является эффективным способом предотвращения несанкционированного доступа к ресурсам компаний. Особенно если компании имеют свои информационные ресурсы в сети Интернет и предоставляют удаленный доступ к данным через веб-приложения и подключения к виртуальным частным сетям с соответствующим криптографическим протоколом.

Подтверждением сказанного является следующее. По результатам ряда отчетов по состоянию дел в информационной безопасности средних и крупных предприятий можно сделать вывод, что значительно увеличились потери предприятий от несанкционированного доступа, повреждения или уничтожения их ресурсов. Приведем пример из ежегодного отчета Института Компьютерной безопасности (Computer Security Institute, CSI) в Сан-Франциско и подразделения по борьбе с компьютерными преступлениями (Computer Intrusion Squad) Федерального Бюро Расследований США под названием «Компьютерные преступления и анализ системы защиты» (Computer Crime and Security Survey) [3]. В этом отчете приводятся результаты опроса сотрудников более чем пятисот различных государственных учреждений и организаций о состоянии дел с информационной безопасностью в их фирмах. В разделе «Цена компьютерных преступлений» (Cost of Computer Crime), сообщается о том, что общие зафиксированные потери этих компаний (только 44% респондентов смогли корректно оценить свои финансовые потери) от компьютерных преступлений, например, за 2002 год выросли с 377,8 млн. долларов до 455,8 млн.

Для предотвращения вторжений и обеспечения безопасности критических ресурсов и, следовательно, снижения возможных финансовых потерь используются многофакторные системы безопасности, осуществляющие взаимосвязанное управление рядом технологий защиты информации [4, 5]. В этих условиях задачи совершенствования технологий защиты информации в вычислительных системах и сетях явля-

ются очень актуальными. Кроме этого, научные результаты, получаемые в области защиты компьютерной информации, могут с успехом использоваться для идентификации граждан (электронный паспорт, пограничный контроль, системы голосования и т.д.), а также в системах контроля физического доступа (учет и управление рабочим временем, корпоративная безопасность, биометрические терминалы и т.д.). К сожалению, большинство исследований в данной области носит закрытый характер, здесь можем обратить внимание на работы [4 – 7].

Цель статьи – кратко проанализировать существующие биометрические системы аутентификации и определить основное направление совершенствования голосовой аутентификации.

Основной раздел

Анализ систем биометрической аутентификации в вычислительных системах и сетях

В настоящее время существует достаточно большое количество технологий, позволяющих обеспечить безопасность некоторых аспектов разных видов ресурсов. Однако, необходимо отметить, что при реализации большинства технологий безопасности применяются аналогичные элементы, а именно, управление доступом посредством криптографической аутентификации/ идентификации, шифрование данных и управление электронно-цифровыми подписями. Ниже основное внимание уделим процедурам идентификации и аутентификации (ИдиА).

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется идентификацией. Идентификация обеспечивает выполнение следующих основных функций:

– установление подлинности и определение полномочий субъекта при его допуске в систему;

– контроль установленных полномочий в процессе сеанса работы;

– регистрация действий пользователя ресурсов и др.

Аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Таким образом, идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации. Однако, как свидетельствуют ряд информационных сообщений, эта линия обороны является ненадежной [4 – 6]. Поэтому активно ведутся работы по совершенствованию ИдиА и, в первую очередь, большие надежды возлагают на биометрические методы аутентификации пользователей, анализ которых выполним ниже.

Как известно, биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации пользователей на основе их физиологических и поведенческих характеристик [6]. К числу физиологических характеристик принадлежат особенности: отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь, в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев. К сожалению, с внедрением электронных паспортов, созданием их баз хранения, надежность этого метода ставиться под сомнение [6, 7].

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных.

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных. Обычно биометрию применяют вместе с другими аутентификаторами, такими, например, как интеллектуальные карты. Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты; в таком случае биометрический шаблон хранится на той же карте. При рассмотрении систем биометрической аутентификации особое внимание должно быть уделено точностным характеристикам:

– вероятности ошибочного пропуска злоумышленника (False Acceptance Rate);

– вероятности ошибочного отказа сотруднику (False Reject Rate, FRR);

– ординате точки пересечения кривых FRR и FAR (Equal Error Rate).

В математической статистике характеристики FAR и FRR имеют названия ошибки первого и второго рода, а в радиолокации соответственно – «ложная тревога» и «пропуск цели».

Наиболее разработанные и распространенные устройства идентификации (примерно 59 % рынка продуктов) используют дактилоскопию (распознавание отпечатков пальцев). Катализатором развития метода послужило его широкое использование в криминалистике 20 века. На втором месте (примерно 18% рынка) находятся устройства, которые анализируют геометрию лица. Все другие устройства, базирующиеся на анализе радужной оболочки, геометрии руки и голоса, занимают от 5 до 7 процентов рынка. Указанные процентное соотношение представлено в [7].

Однако большинство методов биометрической идентификации требуют специальных устройств – сканеров, которые, как правило, имеют большую сложность и стоимость. При этом, как правило, формируется пространственное изображение, которое требует значительных вычислительных затрат в процессе аутентификации. Некоторые характеристики биометрических систем представлены в табл. 1.

Таблица 1

Характеристика современных биометрических систем

№ п/п	Анализируемая характеристика	Название устройства	Уровень FRR, %	Уровень FAR, %	Значение EER, %	Цена, долл.
1	Радужная оболочка	System 2000EAC	0,00066	0,00078	0,00076	6500
2	Сосуды сетчатки глаза	Icam 2001	0,4	0,001	–	2650
3	Папиллярные узоры	TouchLock II	< 1	0,0001	–	2950
4	Папиллярные узоры	FIC-2000I	1,0	0,0001	–	1600
5	Папиллярные узоры	Puppy Logon System	< 1	< 0,1	–	650
6	Форма кисти	Digi-2	0,01	0,01	0,01	–
7	Форма кисти	HandKey ID3D	0,1 (0,03)	0,1	0,1	2150
8	Особенности голоса	Voice Guardian	5	2	1	200
9	Особенности голоса	SpeakerKey	4,3	0,66	2	200
10	Особенности голоса	«Кристалл»	2-4	0,7	–	200
11	Особенности почерка	IBM	0,2	0,4	–	300
12	Геометрия лица	Vocord	2,5	0,1	–	2500

Анализ данных представленных в таблице подтверждает тенденцию последнего времени: все большее внимание уделяется голосовой аутентификации, которая с точки зрения эффективность/стоимость является предпочтительной. Устройства голосовой аутентификации обладают следующими характеристиками:

– простота, компактность, дешевизна устройств ввода информации;

– ввод информации осуществляется дистанционно без участия рук;

– реализация процедур аутентификации осуществляется алгоритмически с приемлемыми вычислительными затратами, поскольку обработке подвергается временной ряд.

Повышение надежности систем аутентификации личности по голосу является актуальной научно-технической задачей. Точность идентификации (установление) и верификации (подтверждение) личности по голосу в существенной мере определяется рядом факторов:

– качеством введения голосового сообщения на фоне пространственно-разнесенных помеховых сигналов и изотропных шумов;

– распознаванием введенного голосового сообщения;

– идентификации и аутентификации пользователя;

– снижение уровня ошибок систем аутентификации по голосу за счет исключения влияния трансформации голоса вследствие болезней, особых эмоциональных состояний, возрастных изменении и т.д.

Решение ряда из перечисленных задач может быть достигнуто за счет совершенствования системы ввода голосового сигнала. Заметим, что известные решения голосовой аутентификации ориентированы на регистрацию голоса с помощью одного микрофона [7, 8]. В тоже время, стандартные системные устройства записи звука имеют два канала, которые способны регистрировать голосовой сигнал в широком диапазоне (квантования по уровню и времени). Применение двух микрофонов, разнесенных в пространстве, позволяет не только увеличить отношение сигнал/шум у анализируемой временной последовательности, но и в последующем даст возможность реализовать схему пространственно-временной обработки [9], которая является предпочтительной при наличии пространственно-сосредоточенных помех (работа кондиционера, вентилятора либо мощных сетевых источников питания).

Возможная структурная схема пространственно-временной обработки представлена на рис. 1, где используются следующие обозначения.

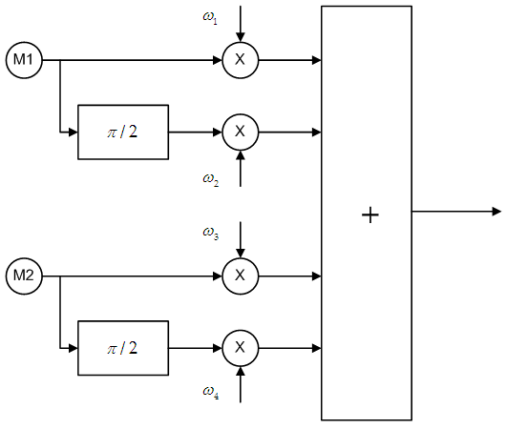

Рис. 1. Структурная схема процедур обработки голосового сигнала

M1 и M2 – микрофоны, разнесенные в пространстве на некоторое расстояние; $\pi/2$ – программные формирователи квадратурной составляющей голосового сигнала; X – умножители, реализующие весовую обработку; + – сумматор. Качественное формирование квадратурной составляющей зарегистрированного сигнала, даст возможность более тонко восстановить его структуру, что является очень важным в процессе аутентификации пользователя.

Выводы и направления дальнейших исследований

Одним из возможных путей защиты информации в вычислительных системах и сетях является использование биометрических систем аутентификации пользователей. Проанализированы характеристики современных систем биометрической аутентификации и обоснована целесообразность использования голосовой аутентификации пользователей. Для устранения недостатков голосовой аутентификации предложено использовать два микрофона. Реализация записи голосового сигнала на два микрофона не только позволит реализовать процедуры пространственно-временной обработки, но и даст возможность более тонко восстановить структуру голосового сигнала пользователя. Предложена структурная схема процедур пространственно-временной обработки регистрируемого голосового сигнала с двух микрофонов.

Дальнейшие исследования будут направлены на выбор оптимального расстояния между микрофонами, а также синтез процедур выделения голосового сигнала пользователя и оценку их характеристик на фоне пространственно-сосредоточенных помех и изотропных шумов.

Список литературы

1. *Nasdaq Index descriptions, Nasdaq Computer Index. Режим доступа: http://www.2.com/reference/ IndexDescriptions.stm.*

2. *Nasdaq Computer Index Dynamics. Режим доступа: http://www.dynamic.2.com/dynamic/com_0.stm.*

3. *Cost of Computer Crime. Режим доступа: http:// www.citadel-information.com/library2/4/2004-fbi-csi-surveys.pdf.*

4. *Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин – М.: ДМК Пресс, 2010. – 544 с.*

5. *Хамидуллин Р.Р. Методы и средства защиты компьютерной информации / Р.Р. Хамидуллин, И.А. Бригаднов, А.В. Мороз – СПб.: СЗТУ, 2005. – 178 с.*

6. *Болл Руд М. Руководство по биометрии / Болл Руд М., Ратха Налини К., Сеньор Эндрю У. – М.: Техносфера, 2007. – 368 с.*

7. *Традиционные методы биометрической аутентификации и идентификации / В.М. Колешко, Е.А. Воробей, П.М. Азизов, А.А. Худницкий, С.А. Снигерев. – Минск: БНТУ, 2009. – 107 с.*

8. *Макаревич О.Б. Методы биометрической аутентификации / О.Б. Макаревич, Л.К. Бабенко, Е.П. Тумоян – Таганрог: ТРТУ, 2004. – 56 с.*

9. *Адаптивная компенсация помех в каналах связи / под ред. Ю.И. Лосева. – М.: Радио и связь, 1988. – 208 с.*

Надійшла до редколегії 18.07.2012

Рецензент: д-р техн. наук, доцент Д.В. Агеев, Харьковский национальный университет радиоэлектроники, Харьков.

АНАЛІЗ ТЕНДЕНЦІЙ У РОЗВИТКУ СИСТЕМ АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ І МЕРЕЖ

І.Ш. Невлюдов, С.В. Пшеничних, О.М. Пастушенко

Аналізуються сучасні системи автентифікації. На підставі критерію ефективність/вартість перевага віддається голосовим системам автентифікації. Розглянуто їхні переваги й недоліки. На відміну від відомих рішень, запропоновано реєстрацію голосового сигналу здійснювати за допомогою двох рознесених у просторі мікрофонів. Зазначене рішення дозволить не тільки реалізувати просторово-часову обробку, схема якої представлена, але й більш тонко відновити структуру сигналу, які реєструється, в умовах наявності завадових і шумових сигналів.

Ключові слова: *аналіз, автентифікація, біометрія, голос, захист, ідентифікація, сигнал.*

ANALYSIS OF TRENDS IN THE DEVELOPMENT OF SYSTEMS FOR AUTHENTICATING USERS COMPUTER SYSTEMS AND NETWORKS

I.S. Nevlyudov, S.V. Pshenichnih, O.N. Pastushenko

The modern authentication systems are analyzed. Based on the criterion of the efficiency/cost the preference is given to authentication systems. Their advantages and disadvantages have been considered. In contrast to the known solutions, was suggested the registration of voice signal by using two spaced microphones. This decision will not only realize the space-time processing, which circuit is shown, but will restore the structure of the signal which is detected with disturbance and noise signals.

Keywords: *analysis, authentication, biometrics, voice, protection, identification, signal.*