ВЫБОР ПОЛЬЗОВАТЕЛЕМ БИОМЕТРИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ ДОСТУПА

А.А. Гивойно, Ю.Ю. Григорьева, И.А. Сеглюк, М.Ю. Ситник, Е.Ю. Нарижный

В настоящее время защита данных проводится в основном с помощью разрешения на доступ к ним, в том числе и по биометрическим параметрам. Общепринято считать, что разрешение доступа к данным по биометрическим параметрам может осуществляться на основе распознавания а) отпечатков пальцев; б) радужной оболочки глаза (РОГ); в) лица; г) геометрии руки; д) голоса; е) сетчатки глаза; ж) ряда дополнительных биометрических параметров (по ДНК, по термограммам, по запаху тела и т. д.) [1]. Из-за множества вариантов средств доступа перед собственником данных возникает задача их выбора.

Для решения этой задачи в докладе предлагается следующая последовательность шагов.

1. Определить несколько вариантов предпочтительных средств доступа (авторизационных систем, АС).
2. Выбрать набор технико-экономических показателей сравниваемых друг с другом АС.
3. Каждый выбранный показатель представить в виде балльной шкалы (чем предпочтительнее АС, тем выше балл), например, для показателя «цена АС»: 25 000 $ – 7 баллов, 26 000 $ – 5 баллов, 27 000 $ – 3 балла.
4. Выбрать весовые коэффициенты каждого показателя так, чтобы сумма их равнялась единице.
5. Рассчитать критерий выбора АС как скалярное произведение вектора выбранных показателей и вектора весовых коэффициентов (чем предпочтительнее АС, тем выше критерий).

Предлагаемая последовательность шагов иллюстрируется двумя примерами: сравнением друг с другом и последующим выбором двух средств контроля доступа по РОГ и двух средств контроля доступа по отпечатку пальца.

Литература

1. Прудник, А.М. Биометрические методы защиты информации / А.М. Прудник, Г.А. Власова, Я.В. Рощупкин. Минск: БГУИР, 2014. – 150 с.

СИСТЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ДЛЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ

И.В. Голубович

На сегодняшний день, благодаря бурному развитию технологий электронной обработки данных, биометрические технологии находят применение не только в криминалистике, но и в иных областях. К таким областям можно отнести информационную безопасность, защиту в банковских технологиях, системы управления доступом, системы учета рабочего времени и регистрации посетителей и др.

Основной целью удостоверения личности с целью аутентификации пользователя для учета рабочего времени является уникальная идентификация личности. Биометрические системы, базирующиеся на физиологических параметрах, значительно надежнее систем, основывающихся на характерных чертах поведения. В биометрии используются признаки присущие каждому человеку, такие как: папиллярный узор пальца, форма кисти руки, узор радужной оболочки глаза, параметры голоса, черты лица, термограмма лица, схема кровеносных сосудов, форма и способ подписи, фрагменты генетического кода и др.

Биометрическая идентификация это также и дополнительный уровень защиты, так как биометрические данные сложно подделать. Одним из достоинств подобных данных является то, что биометрические данные неизменны и уникальны для каждого человека. Основным преимуществом биометрической аутентификации является то, что подобные данные невозможно забыть, потерять, передать другому человеку, украсть или воспроизвести в полном объеме.

Для реализации подобных биометрических систем часто используется такая биометрическая характеристика как отпечаток пальца, так как она обладает наиболее высокими экспертными оценками свойств среди биометрических характеристик человека. Самым

быстродейственным и простым в реализации методом аутентификации по отпечатку пальца является сравнение по особым точкам. Существуют проверенные временем алгоритмы, реализующие данную процедуру аутентификации, однако, необходимость в разработке и реализации новых алгоритмов с лучшими характеристиками не отпадает и на сегодняшний день.

Литература

1. Stan Z. Li Anil K. Jain, Encyclopedia of Biometrics. Second edition, Springer, 2009.
2. Maltoni D., Maio D., Jain A.K., Prabhakar S., Handbook of Fingerprint Recognition, Springer, 2003.

ИССЛЕДОВАНИЕ И ПРИМЕНЕНИЕ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Выбрана конструкция функция безопасности для MVC 5, которая основана на средствах Owin − промежуточного программного обеспечения аутентификации. В процессе исследований аутентификации использовалась система мобильных приложений для банка Последовательность для входа в систему приложений следующая: 1. Пользователь регистрировался в системе ibank24.ir. 2. После регистрации по электронной почте он получает экаунт активизации, в котором содержался ключ активизации мобильных приложений. 3. Пользователь загружает сайт Android app. 4. Для работы используется: имя, пароль и ключ активизации. 5. Ключ запрашивается системой для входа в облачную среду. 6. Меню и ключ вводится пользователем.

Представлена структура программной системы аутентификации в ИКИС для работы сотрудников с мобильными приложениями в реальной системе защиты информации банка. Проведены исследования модели и алгоритмов аутентификации пользователей мобильных приложений в облачной среде, результаты которых показали их эффективность при работе в системе защиты информации банка.

Разработанные модели и средства аутентификации пользователей мобильных приложений использованы в учебном процессе кафедры ИТ Минского инновационного университета для улучшения изучения дисциплины «Основы защиты информации» студентами специальности ПОИТ, а также при выполнении НИР «Модели и средства информационного управления и электронного маркетинга предприятия».

КОМПОНЕНТЫ СИСТЕМЫ АУТЕНТИФИКАЦИИ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ИНТЕГРИРОВАННОЙ КИС

М.М. Гондаг Саз, В.А. Вишняков

Активное развитие мобильных технологий ставит перед организациями вопрос аутентификации в корпоративной сети с облачными вычислениями. Простой и достаточно надежный метод аутентификации – это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться специальными программами, дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).

Усиленная аутентификация, в том числе с использованием дополнительных факторов, должна происходить на компьютере и мобильном устройстве, иначе мобильность будет слабым звеном в контуре безопасности организации. При этом меры обеспечения ИБ не должны создавать неудобства для пользователей. Одной из современных тенденций в области аутентификации является использование SSO (Single Sign-On). Идея этой технологии