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