В.А.ВИШНЯКОВ[1], С.М.ГОНДАГ САЗ[2]

АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В РАСПРЕДЕЛЕННОЙ КИС

[1]*Учреждение образования «Белорусская государственная академия связи», г. Минск, Республика Беларусь*

[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

Информационная безопасность облачных вычислений (ОВ) имеет специфику: защита периметра и разграничение сети; динамичность ВМ; уязвимости и атаки внутри виртуальной среды; защищенность данных и приложений; доступ системных администраторов к серверам и приложениям; защита бездействующих ВМ. Усложняется аутентификации в среде ОВ [1].

Проанализированы способы и протоколы аутентификации в мобильных системах для сред ОВ. Предложена концепция интегрированной КИС, базирующаяся на использовании в составе классической КИС предприятия технологий облачных вычислений и мобильных приложений, что дает новое качество информационного управления и модификации средств аутентификации [1].

Получена математическая модель модифицированной аутентификации, которая позволяет по заданному числу неудовлетворительных оценок вычислить вероятность успешной аутентификации, позволяющая восстанавливать пароль как при его утере, так и при смене злоумышленником. Приведены модели для безопасной работы пользователей в среде облачных вычислений [2].

Разработаны модели аутентификации пользователей мобильных приложений по паролю с сервером приложений, по сертификатам, по одноразовым паролям, по ключам доступа, по токенам. Рассмотрен подход к поддержке принятия решения по моделей аутентификации и идентификации. Предложен интеллектуальный подход для выбора вариантов СИА, базирующийся на составлении базы правил выбора для ЭС [2].

Для аутентификации пользователей в облачной среде предложено использовать технологию единого входа (Single Sign-On). Рассмотрены ее преимущества для пользователей и предприятия. Приведены также выгоды, такие как: увеличение безопасности, повышение производительности, сокращение расходов, уменьшая количество паролей в системе. Рассмотрены три основных типа единого входа: веб-SSO, Legacy SSO и Federated SSO. Приведена архитектура WebAuth, которая включает в себя два основных компонента: сервера регистрации и приложений [2].

Получены алгоритмы трех вариантов аутентификации с использованием метода 2FA. В первом варианте проверяется необходимость метода 2FA. Во втором варианте код активации для токена (APP) отправляется по электронной почте после регистрации пользователя на сайте. В третьем варианте пользователь (с маркером) либо получает доступ, либо после проверок получает код активации для токена (APP), который отправляется по электронной почте после регистрации пользователя на сайте [2].

Выбрана конструкция функция безопасности для MVC 5, которая основана на средствах Owin − промежуточного программного обеспечения аутентификации. Преимущество этого средства является то, что функция безопасности может совместно использоваться другими компонентами, которые могут быть размещены на Owin. Представлена структура программной системы аутентификации в ИКИС для работы сотрудников с мобильными приложениями [2].

ЛИТЕРАТУРА

1. Вишняков, В.А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения. Монография. / В.А. Вишняков. – Минск: Бестпринт, 2016. – 276 с.

2. Вишняков, В.А. Модели аутентификации в облачных вычислениях для мобильных приложений с интеллектуальной поддержкой выбора / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР, № 1, 2017. – С. 82-86.