В.А.ВИШНЯКОВ[1], С.М.ГОНДАГ САЗ[2]

АЛГОРИТМЫ И МЕТОДИКА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ В ОБЛАЧНОЙ СРЕДЕ

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

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

В докладе представлена концепция интнегрированной КИС с использованнием облачных вычислений (ОВ). Проанализированы основные проблемы информационной безопасности (ИБ) при использовании ОВ, механизмы аутетификации пользователей [1]. Политика доступа может быть усилена использованием более сильного метода аутентификации. Таким является метод Two-Factor Authentication (2FA), использующий одноразовые пароли (OTP), он является одним из самых надежных решений аутентификации, в то же время его не сложно реализовать, и он имеет низкую стоимость [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.

Архитектура WebAuth включает в себя два основных компонента: сервера регистрации и приложений. Роль сервера регистрации в том, что он предоставляет доверенный, централизованный сервис аутентификации для непосредственного взаимодействия с пользователями. Сервер приложений выступает в качестве регулятора аутентификации. Он перенаправляет не аутентифицированных пользователей на сервер авторизации и проверяет информацию об аутентификации, возвращаемую с сервера авторизации.

До начала процесса аутентификации пользователя рассмотрена дополнительная фаза между сервером авторизации и каждым из серверов приложений, предназначенная для генерации общего симметричного ключа для защиты куков. Приведено управление доступом по схеме однократного входа с авторизацией Single Sign-On. Рассмотрена простая система однократного входа Single Sign-On.

Показана структура облака безопасности, для которой предложен алгоритм аутентификации пользователей через мобильное приложение. В сервере аутентификации для аутентификации пользователя и облачного веб-сервера выполяется 5 шагов. Приведены 12 этапов алгоритма аутентификации пользователей для регистрации в облачой среде через мобильное приложение.

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.

ЛИТЕРАТУРА

1. Intelligence Community Information Technology Enterprise (ICITE) [Электронный ресурс], режим доступа: http://www.insaonline.org/i/d/a/Resources/ ICITE_Doing.aspx (дата доступа 22.09.2017.

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