В.А.ВИШНЯКОВ[1], С.М.ГОНДАГ САЗ[2]

ИНТЕЛЛЕКУАЛЬНЫЙ ВЫБОР ВИДА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

[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].

Рассмотрим подход к поддержке принятия решения по выбору МА и МИ. В работе [2] предложена классификация системы аутентификации по признакам выполнения целей и задач обеспечения ИБ. Процесс аутентификации состоит из последовательно выполняемых процедур двух классов: к первому относятся процедуры регистрации нового пользователя ИС и хранения аутентификационной информации (АИ), ко второму – процедуры предъявления АИ, протоколы обмена «претендент–проверяющая сторона», валидация и принятия решения о результате прохождения претендентом процесса аутентификации. Модель классификации аутентификации − *MCA* представим тройкой:

MCF = {*A, W, C*},

где *A* − доступность (accessibility), *T* − целостность (wholeness), *C* − конфиденциальность (confidelity). Детализацию модели классификации выразим таким образом:

A = {GA, *DA, CA, PA*}: *W* = {*WS, WRR,WAP, WPC*}; *C* = {*CPP, CAP, CPC* },

где *GA* − гарантия обработки запросов пользователей на аутентификацию, *DA* − разделе-ние доступа пользователей, *CA* − контроль доступа , *PA* − персонификация доступа; *WS* − целостность ПО, *WRR* − целостность учетных записей , *WAP* − целостность АИ пользователя, *WPC* − целостность АИ пользователя в облачной среде; *CPP* − конфиденциальность учетных записей , *CAP* − конфиденциальность АИ пользователя, *CPC* − конфиденциальность АИ пользователя в облачной среде.

Интеллектуальный подход для выбора вариантов СИА базируется на составлении базы правил выбора, в качестве интеллектуального инструмента используются основанные на правилах, экспертные системы (ЭС). ЭС в базе знаний содержит описание классификационных правил СИА, соответствующих профилям легальных пользователей. Эксперт с инженером по знаниям формирует базу правил для выбора варианта СИА. Работа такой ЭС может базироваться как на экспертном подходе, так и в автоматическом режиме сервера. Для первого варианта организуется диалог, в ходе которого выявляются пожелания или требования пользователя или администратора КИС. На основании результатов опроса формируется вариант СИА. В автоматическом режиме сервера вариант СИА формируется по профилям легальных пользователей. Разработана программная поддержка выбора аутентификации.

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. Сабанов, А. Г. Принципы классификации систем идентификации и аутентификации по признакам соответствия требованиям информационной безопасности / А. Г. Сабанов // «Электросвязь», № 2, 2014. – С. 6-9.