ВЫБОР СРЕДСТВ КОНТРОЛЯ ДОСТУПА К ОБЪЕКТУ СРЕДИ СРЕДСТВ, ОСНОВАННЫХ НА РАЗЛИЧНЫХ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЯХ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Сеглюк И.

Охрименко А. А. – канд. техн. наук., доцент

Рассматриваются вопросы достаточности работ по тестированию информационной безопасности программного обеспечения веб-сервера vCenter Server 5.5. Показывается, что качество и объём таких работ недостаточны для полного устранения дефектов программного обеспечения сервера.

Средства контроля доступа (СКД) к объекту на основе отпечатков пальцев (СКД ОП) являются одним из дешёвых и в силу этого наиболее распространённых средств [1]. По поводу отпечатков пальцев ещё в Библии две тысячи лет назад было сказано: «Он (*имеется в виду всевышний*) полагает печать на руку каждого человека, чтобы все люди знали дело Его» (Ветхий Завет, Книга Иова, гл. 37, ст. 7). Эти средства в массовом порядке впервые начали применяться в дактилоскопии и криминалистике. Вариантов реализации СКД ОП и принципов их действия очень много, и они хорошо описаны в [1]. СКД ОП сейчас находят различные применения [1]. Их устанавливают на ноутбуки, в мыши, клавиатуры, флешки, а также применяют в виде отдельных внешних устройств и терминалов, продающихся в комплекте с системами AFIS (системами идентификации личности по отпечаткам пальцев).

Однако биометрические СКД не обязательно могут быть реализованы с помощью технологии распознавания отпечатков пальцев, в которых биометрический параметр – это отпечаток пальца (Рисунок 1).. В [2], например, кратко перечислены другие биометрические технологии идентификации личности, а сравнение СКД проводится на примере программно-аппаратных комплексов для распознавания личности по радужной оболочке глаза (РОГ) (биометрический параметр – РОГ, Рисунок 2).

Рисунок 1 – Отпечаток пальца как биометрический параметр СКД

Рисунок 2 – РОГ как биометрический параметр СКД

В этих условиях актуальной для будущего пользователя СКД является задача выбора среди средств доступа к объекту, основанных на различных биометрических технологиях, наиболее оптимального для него СКД. Похожая задача поставлена в отдельной главе монографии [1], но там задача решается очень сложным способом.

Для решения поставленной задачи более простым способом воспользуемся методикой, предложенной в [2], т. е. критерий выбора СКД будем рассчитывать, как скалярное произведение вектора выбранных показателей и вектора весовых коэффициентов (чем предпочтительнее СКД, тем выше критерий). Набор технико-экономических показателей, сравниваемых друг с другом СКД выберем в следующем виде: 1) цена БСКДкИО, 2) общая стоимость ущерба для пользователя в случае несанкционированного доступа к объекту; 3) суммарная вероятность ошибок идентификации в процентах (вероятность пропуска «чужого» плюс вероятность ложного отказа в доступе; 4) размер шаблона. Шаблон – это машинная репрезентация биометрического образца. Шаблон определенным образом описывает полученный биометрический образец для того, чтобы можно было провести как можно более точное автоматизированное сопоставление. Размер этой репрезентации в байтах или килобайтах является важным фактором, который может повлиять на выбор биометрического параметра. Маленькие шаблоны дают возможность использовать небольшие устройства их хранения, такие, как магнитные карты, и позволяют создавать распределенные базы данных [1].

Для иллюстрации пригодности предложенной методики в докладе приводится пример выбора пользователем одного из СКД, реализованного на двух биометрических технологиях распознавания – технологии идентификации личности с помощью отпечатков пальцев и технологии распознавания личности по радужной оболочке глаза.

Список использованных источников:

1. Прудник А. М. Биометрические методы защиты информации: учебно-методическое пособие для специальности 1-98 01 02 «Защита информации в телекоммуникациях»./ А. М. Прудник, Г. А Власова., Я.В. Рощупкин – Минск: БГУИР, 2014. .

2. Гивойно А.А. Методика выбора биометрических средств контроля доступа к информационному объекту/ Гивойно А.А., Ситник М.Ю., Нарижный Е.Ю. // В настоящем сборнике.