ВЫБОР ПОЛЬЗОВАТЕЛЕМ БИОМЕТРИЧЕСКИХ СРЕДСТВ КОНТРОЛЯ ДОСТУПА

А.А. Гивойно, Ю.Ю. Григорьева, И.А. Сеглюк, М.Ю. Ситник, Е.Ю. Нарижный

В настоящее время защита данных проводится в основном с помощью разрешения на доступ к ним, в том числе и по биометрическим параметрам. Общепринято считать, что разрешение доступа к данным по биометрическим параметрам может осуществляться на основе распознавания а) отпечатков пальцев; б) радужной оболочки глаза (РОГ); в) лица; г) геометрии руки; д) голоса; е) сетчатки глаза; ж) ряда дополнительных биометрических параметров (по ДНК, по термограммам, по запаху тела и т. д.) [1]. Из-за множества вариантов средств доступа перед собственником данных возникает задача их выбора.

Для решения этой задачи в докладе предлагается следующая последовательность шагов.

1. Определить несколько вариантов предпочтительных средств доступа (авторизационных систем, АС).
2. Выбрать набор технико-экономических показателей сравниваемых друг с другом АС.
3. Каждый выбранный показатель представить в виде балльной шкалы (чем предпочтительнее АС, тем выше балл), например, для показателя «цена АС»: 25 000 $ – 7 баллов, 26 000 $ – 5 баллов, 27 000 $ – 3 балла.
4. Выбрать весовые коэффициенты каждого показателя так, чтобы сумма их равнялась единице.
5. Рассчитать критерий выбора АС как скалярное произведение вектора выбранных показателей и вектора весовых коэффициентов (чем предпочтительнее АС, тем выше критерий).

Предлагаемая последовательность шагов иллюстрируется двумя примерами: сравнением друг с другом и последующим выбором двух средств контроля доступа по РОГ и двух средств контроля доступа по отпечатку пальца.

Литература

1. Прудник, А.М. Биометрические методы защиты информации / А.М. Прудник, Г.А. Власова, Я.В. Рощупкин. Минск: БГУИР, 2014. – 150 с.

СИСТЕМА АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ДЛЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ

И.В. Голубович

На сегодняшний день, благодаря бурному развитию технологий электронной обработки данных, биометрические технологии находят применение не только в криминалистике, но и в иных областях. К таким областям можно отнести информационную безопасность, защиту в банковских технологиях, системы управления доступом, системы учета рабочего времени и регистрации посетителей и др.

Основной целью удостоверения личности с целью аутентификации пользователя для учета рабочего времени является уникальная идентификация личности. Биометрические системы, базирующиеся на физиологических параметрах, значительно надежнее систем, основывающихся на характерных чертах поведения. В биометрии используются признаки присущие каждому человеку, такие как: папиллярный узор пальца, форма кисти руки, узор радужной оболочки глаза, параметры голоса, черты лица, термограмма лица, схема кровеносных сосудов, форма и способ подписи, фрагменты генетического кода и др.

Биометрическая идентификация это также и дополнительный уровень защиты, так как биометрические данные сложно подделать. Одним из достоинств подобных данных является то, что биометрические данные неизменны и уникальны для каждого человека. Основным преимуществом биометрической аутентификации является то, что подобные данные невозможно забыть, потерять, передать другому человеку, украсть или воспроизвести в полном объеме.

Для реализации подобных биометрических систем часто используется такая биометрическая характеристика как отпечаток пальца, так как она обладает наиболее высокими экспертными оценками свойств среди биометрических характеристик человека. Самым