НАДЕЖНОСТЬ И БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ НА ОБЪЕКТАХ СИСТЕМ ИДЕНТИФИКАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ПРИЗНАКОВ

Современный подход к выбору и построению систем безопасности уже невозможен без учета современных IT-технологий. Рассматривая в этом выпуске вопрос надежности применения биометрических систем идентификации для различных систем контроля доступа на объекты, к данным или системам управления, мы не смогли обойти этот аспект. Компания Cisco – признанный мировой лидер в области сетевых технологий – имеет значительный опыт в применении различных систем идентификации.

Алексей Викторович Лукацкий – *бизнес-консультант Cisco по информационной безопасности, ответил на вопросы редакции. Надеемся, нашим читателям будет интересно узнать его мнение о реалиях и перспективах использования биометрии для различных задач.*

1. На каких типах объектов и при достижении каких целей компания Cisco уже сталкивалась с задачей внедрения биометрических систем идентификации?

Если отбросить встроенные во многие модели ноутбуков и смартфонов сенсоры, позволяющие входить в компьютер по отпечатку пальца, то в большинстве случаев применение биометрии касается сферы государственных секретов. Например, доступ в помещения, в которых ведется обработка сведений, составляющих государственную тайну, или иных не менее важных данных, используемых спецслужбами. Следующий важный сектор – финансовые сервисы, для которых важна идентификация человека, получающего денежные средства. На эти два сегмента приходится львиная доля всех внедрений. В последнее время активно обсуждается удаленная идентификация с помощью биометрии в рамках различных государственных услуг.

2. Обязывает ли применение биометрической идентификации изменить подход к построению сетей, защите каналов передачи данных, защите баз данных на предприятиях и в организациях?

Никаких серьезных отличий от иных методов идентификации внедрение биометрии не имеет – защита идентификационной информации, независимо от ее типа, должна обеспечиваться на высшем уровне. Единственное отличие и местами существенное, это поддержка соответствующих методов в применяемой IT-инфраструктуре. Тут и внедрение соответствующих сенсоров/считывателей, и наличие соответствующих API в приложениях, без которых внедрить биометрию будет невозможно.

3. Можно ли считать биометрические данные человека абсолютно надежными как идентификационный признак. Какие специфические виды угроз безопасности могут быть связаны с применением биометрических систем на предприятиях и в организациях?

Об абсолютной надежности речи быть не может. Более того, в ряде случаев биометрическая идентификация имеет ряд проблем. Представьте себе, что в системе украли ваш логин. Его можно заменить очень быстро, тем самым приведя систему вновь в защищенное состояние. А если украдут ваш отпечаток, образец голоса или фотографию? Изменить их – значит изменить сам объект идентификации. Это невозможно, если не рассматривать варианты пластической хирургии. Однако вокруг биометрии уже сформировался миф о ее непогрешимости и надежности. Поэтому внедрение биометрии требует гораздо более грамотной и тщательной проработки, чем обычно. Например, вместо одного варианта биометрической идентификации можно использовать два – так называемую бимодальную идентификацию, когда применяется в качестве идентификатора, например, изображение лица и голос человека.

4. Можно ли сравнивать биометрию с уже привычными системами идентификации и доступа на базе персональных паролей, карт доступа, идентификации через персональные мобильные устройства и т. д.?

Упомянутые системы идентификации являются статическими, используемыми обычно один раз или реже через заданные интервалы времени. У биометрии есть неоспоримый плюс – она может быть динамической и прозрачной. Например, через камеру ноутбука мы можем отслеживать мимику лица. Это исключает целый класс атак с подменой фотографии человека. Или можно отслеживать голос человека, задавая ему разные вопросы и анализируя его ответы. В этом случае защищенность идентификации повышается многократно. В случае применения иных методов биометрии (например, клавиатурный почерк или поведенческие характеристики) идентификация может стать прозрачней и многократно надежней.

5. Какие из идентификационных признаков имеют большие перспективы развития в ближайшее время и почему?

Из всех методов биометрической идентификации наиболее популярными сегодня считаются 3: отпечатки пальцев, голос и геометрия лица. Они с большим отрывом лидируют в разных приложениях, что связано с простотой и дешевизной их реализации. Все остальное требует гораздо больших вложений. Например, считыватели радужки глаза или рисунка вен. Есть методы с пониженной эффективностью, например, поведенческие методы – и это приводит к снижению соотношения цена/качество.

6. Готовы ли существующие на объектах системы безопасности и системы обмена данными к более-менее массовому внедрению биометрических систем? Имеет ли смысл сейчас тратить на это усилия, не лучше ли остановиться пока на классических системах идентификации?

Внедрение любой системы требует обоснования. Либо новая технология должна быть дешевле существующей, либо более безопасной, либо давать какие-то новые качества. В каждой конкретной организации необходимо изучение текущей ситуации, после чего можно судить о том, стоит ли переходить на нечто новое. Применительно к биометрии я бы задал простой вопрос: почему не устраивает текущая технологии идентификации? Увеличилось ли за последнее время число инцидентов, связанных с обходом системы идентификации? Довольны ли пользователи текущей системой идентификации? Не теряет ли компания деньги из-за слишком длительного процесса идентификации? От ответов на эти вопросы и зависит переход на биометрию.

7. Каково Ваше мнение: готовы ли в целом современные биометрические системы к требованиям безопасности предприятия или организации? Каких шагов Вы ждете от производителей таких систем?

Проблема сегодня не в производителях, а в потребителях. Они должны «дозреть» до данной технологии. С точки зрения производителей сегодня сделано уже много. Дело за малым – начать внедрять. А вот в этом нет такой уж большой необходимости, исключая некоторые ситуации. И они, по большей части, касаются специальных задач, описанных мною в начале.