Защита объектов от несанкционированного проникновения — залог их безопасности

Защиту различных объектов от несанкционированного проникновения на них могут обеспечить биометрические системы.

Промышленные объекты являются ключевым звеном всей инфраструктуры промышленных узлов, городов и страны в целом. Их защита от несанкционированного на них проникновения остается важнейшей задачей, даже если большинство из них уже оборудованы системами видеонаблюдения. Кроме того, особый интерес представляет реальная возможность проанализировать, кто и в течение какого времени находится на объекте.

В связи с этим наибольшее применение в мире находят биометрические системы, которые идентифицируют людей по их уникальным физиологическим и поведенческим параметрам. Рассмотрим некоторые из них.

В настоящее время доминируют системы, основанные на идентификации по отпечаткам пальцев. Они занимают до двух третей от общего объема биометрического рынка. На основе анализа, проведенного компанией «Research and Markets» (США), такое положение дел сохранится и в перспективе. Оставшуюся часть рынка делят решения, распознающие пользователей по их лицам и радужной оболочке глаз: первые востребованы в паспортных и визовых системах, а вторые — в банках и других финансовых структурах.

Популярность технологий идентификации по отпечаткам пальцев объясняется целым рядом факторов. Во-первых, они представляют достаточно высокую степень защиты, так как у обычного человека на руках 10 пальцев. Во-вторых, рассматриваемые технологии развиваются уже давно и в своей эволюции достигли такой стадии зрелости, что способны предоставить оптимальное соотношение цены и качества распознавания. В-третьих, это распознавание может эффективно осуществляться в двух режимах: собственно идентификации и верификации.

При идентификации сравнение осуществляется по модели «один-комногим»: пользователь просто предъявляет отпечаток, а биометрическая система сама находит соответствие в базе данных о ранее зарегистрированных идентификаторах. При верификации сравнение идет «один-к-одному»: пользователь сообщает дополнительные сведения о себе — например, фамилию, и из базы данных извлекаются сведения, относящиеся к конкретному человеку.

Режим идентификации гораздо удобнее, но в нем пока не умеют действовать системы, распознающие пользователей по рисунку вен на ладони или пальце, трехмерной модели черепа и прочей экзотике: им нужны дополнительные данные (карта или PIN-код). Поэтому неудивительно, что доля этих систем составляет в лучшем случае лишь несколько процентов от общего объема биометрического рынка.

На промышленных предприятиях особое значение приобретает главное преимущество биометрических технологий, способных идентифицировать именно человека, а не карточку или PIN-код, которые легко похитить, потерять или добровольно передать другому человеку. Конечно, мало приятного, когда по украденной карте вор проникает в гостиничный номер, но если по чужой карте злоумышленник получает доступ на территорию предприятия или логистического центра, возможные последствия и риски значительно выше.

Турникетами, шлюзами, электромагнитными и электромеханическими замками управляют биометрические терминалы. В их состав входят сканеры отпечатков пальцев, сетевые модули, компоненты для взаимодействия с упомянутыми исполнительными механизмами, внутренняя память для хранения сведений о биометрических идентификаторах. Предусмотрены также и средства информирования пользователя о результатах распознавания: цветовые индикаторы, динамики для вывода звуковых оповещений и дисплеи для трансляции текста (например, ФИО пользователя, проходящего на объект или покидающего его).

Реализуются и другие важные функции.

Запрет повторного прохода.

Не отметив приход на работу, сотрудник не получит права на уход, и

наоборот. Эта функция актуальна для борьбы с любителями скрывать опоздания, проходя «паровозиком» через турникет вместе с коллегой.

Разграничение доступа по времени.

К примеру, с 9.00 до 18.00 для рядовых сотрудников; для руководителей, сотрудников службы безопасности и ИТ-специалистов — круглосуточно.

Многофакторная идентификация.

Доступ в важные помещения (кабинеты руководителей, серверные, переговорные) разрешается по предъявлении не одного, а нескольких идентификаторов (карта + отпечаток пальца, PIN-код + отпечаток пальца и т. д.); биометрические терминалы, как правило, поддерживают возможность идентификации по бесконтактной карте и PIN-коду.

Наряду с контролем доступа биометрические системы реализуют задачу учета рабочего времени. Благодаря исключению ошибок, неизменно возникающих при ведении учета вручную, они обеспечивают повышение трудовой дисциплины, существенное уменьшение числа опозданий и ранних уходов, исключают выплаты за якобы переработанное (а на самом деле приписанное) время.

«Карточные» системы учета выглядят более привычными. Практика показывает, что персонал научился легко обманывать и обходить их. В иностранной литературе по управлению персоналом даже появился специальный термин «buddy punching», описывающий ситуацию, когда один сотрудник отмечает приход/уход карточками остальных коллег, что, естественно, сводит к нулю смысл учета рабочего времени. В противоположность карточке отпечаток пальца при всем желании невозможно передать другому человеку, а биометрия реализует главное требование к учету — его достоверность.

На самом деле функционал биометрических систем учета рабочего времени гораздо шире: они позволяют не только учитывать, но и планировать нагрузку персонала. Для этого в наиболее продвинутых системах предусмотрены модули календарного планирования, сменные, скользящие и другие нестандартные графики работы.

Не меньшее значение имеет и способность биометрических систем взаимодействовать с внешним окружением — например, платформой 1С, кадровыми и управленческими системами (скажем, Microsoft Dynamics). Так, из 1С в биометрическую систему можно импортировать сведения о сотрудниках (ФИО, подразделение, табельный номер и т. д.), а из биометрической системы — точные и достоверные сведения об отработанном времени для справедливого начисления зарплаты.

Это превращает биометрические системы в универсальное средство для управления производством. При этом возникает вопрос выбора системы и ее поставщика.

На рынке Союзного государства России и Беларуси представлено немалое число компаний, предлагающих биометрические системы учета рабочего времени и контроля доступа. В качестве критериев отбора можно предложить следующие:

– технологическая состоятельность предлагаемого решения, оценивать которую рационально по наличию упомянутых выше функций. Здесь же следует упомянуть адаптированность системы к отечественному рынку (понятно, что переведенный с китайского софт, несмотря на его дешевизну, вряд ли устроит требовательного заказчика);

– масштабируемость решения, его готовность обслуживать не десятки или сотни, а тысячи и десятки тысяч сотрудников;

– способность компонентов системы функционировать в самостоятельном режиме. Это относится и к работе терминалов (при сбоях в сети они должны переходить в автономный режим, а по восстановлении связи с сервером — автоматически передавать ему накопленную информацию о событиях приходов/уходов), и к функционированию подсистем в территориально удаленных филиалах;

– зрелость системы, то есть число ее внедрений (особенно крупных), время ее присутствия на рынке (в идеале — не менее десяти лет), отзывы других заказчиков;

– компетентность разработчика, о которой свидетельствуют партнерские отношения с грандами ИТ-рынка (например, статус сертифицированного партнера Microsoft);

– открытость разработчика/поставщика, его готовность предоставлять систему на предварительное тестирование, организовывать референс-визиты к другим заказчикам, осуществлять пилотные проекты, проводить мероприятия для имеющихся и потенциальных заказчиков;

– широкая номенклатура аппаратных средств биометрической идентификации, включающая не только несколько типов сканеров отпечатков пальцев, но и различные Ethernet-терминалы, реализующие функции учета рабочего времени и/или контроля доступа.

Сеть подобных предприятий на территории России разрослась довольно густо.

В качестве примеров внедрения системы учета рабочего времени можно привести следующие предприятия промышленного, энерго- и нефте-газового комплекса Российской Федерации:

– Наро-Фоминская теплоэнергетическая компания, Московская область;

– «Сургутнефтегаз», г. Сургут;

– «Нефтегазпоставка», г. Москва;

– «Нефтьгазкомплект», г. Москва;

– «Межрегионэнергогаз», Московская область;

– «СНГ-Нефтегаз», г. Саратов;

– Машиностроительный завод «Тяжмаш», г. Сызрань;

– «Татнефть-Транс», г. Альметьевск.

Таким образом, внедрение биометрических систем позволяет не только защитить промышленные объекты от несанкционированного проникновения на них, но и лучше организовывать производственно-хозяйственную деятельность, повышать уровень безопасности труда персонала, обслуживающего предприятия.

Инна МЕЖЕНИНА,
директор частного торгового унитарного предприятия