УДК 004.732

Модель процесса идентификации в системах контроля и управления доступом

А. Ю. Исхаков

В статье рассматриваются вопросы идентификации посетителей как один из механизмов обеспечения безопасности в местах массового пребывания людей. Рассмотрены особенности функционирования подобных объектов и ограничения для применения в них систем контроля и управления доступом. Разработана модель процесса идентификации в системах контроля и управления доступом.

Ключевые слова: идентификация, контроль доступа, модель, процесс.

1. Введение

В современном мире одной из наиболее значимых угроз безопасности населения является международный терроризм. В условиях крайней степени актуальности данной угрозы спецслужбы всего мира предпринимают различные действия по усилению мер безопасности в местах массового пребывания людей (ММПЛ) [1]. В общем случае под ММПЛ понимаются общественные места с высокой плотностью человеческих потоков и вероятностью возникновения неуправляемой толпы. В некоторых случаях [2] такие объекты подлежат обязательной охране полицией, и усиление мер безопасности на объектах подобного рода достигается путем ужесточения действующего пропускного и внутриобьектового режимов.

В то же время существуют ММПЛ, особенности функционирования которых не позволяют внедрить полноценный пропускной режим. К подобным местам можно отнести крупные офисные центры (площади которых арендуются множеством различных компаний), выставочные комплексы (экспоцентры), кинозалы, театры и т.д.

Зачастую администрация таких объектов добросовестно относится к требованиям законодательства и реализует комплекс инженерных, технических и организационных мероприятий по обеспечению мер безопасности посетителей (выборочный контроль посетителей сотрудниками охраны, использование металлодетекторов на пунктах прохода, установка систем пультовой охраны, средств видеонаблюдения и т.д.). Однако постоянный поток «случайных» посетителей и отсутствие функциональных возможностей регистрации посетителей не позволяет проводить процедуру идентификации личности. Этот факт значительно повышает степень реализации угрозы несанкционированного доступа злоумышленников на объект. Кроме того, отсутствие идентифицирующих сведений о посетителях ММПЛ значительно затрудняет расследование преступлений и различных инцидентов органами безопасности.

Таким образом, актуальной научной задачей является исследование подходов и методик, которые бы позволяли организовать идентификацию посетителей ММПЛ без ущерба для протекающих в них бизнес-процессов.

В рамках данной работы проводится моделирование процесса идентификации и анализ возможности применения систем контроля и управления доступом (СКУД) как инструмента для решения поставленных задач в ММПЛ.

2. Модель процесса идентификации

Процедура идентификации предполагает опознавание пользователя по присущему или присвоенному ему идентификационному признаку [7]. При этом выполняется сравнение предъявляемого идентификатора с полным перечнем присвоенных идентификаторов.

Модель процесса идентификации может быть представлена следующим образом. Пусть в системе идентификации зарегистрировано *n* субъектов доступа. При этом в момент регистрации *i*-го субъекта доступа в системе идентификации создается его образ p_i – набор эталонных значений характеристик. Тогда база данных эталонных характеристик для всех зарегистрированных субъектов доступа описывается множеством $P = \{ p_1, p_2, \ldots, p_n \}$.

Будем полагать, что система идентификации позволяет анализировать (распознавать) *k* идентификационных характеристик субъекта доступа. Множество $Z = \{ z_1, z_2, \ldots, z_k \}$ определяет характеристики, по которым в данной системе осуществляется процесс идентификации. Элементами множества Z могут выступать серия или номер пропуска, рабочая частота используемой технологии передачи данных, параметры кодирования и т.д. В случае применения биометрии идентификационными характеристиками могут выступать, например, минуции – уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий (окончание, раздвоение, разрыв и т.д.).

Необходимо отметить, что множество Z формируется для каждой системы идентификации. Образу p_i при $i = \overline{1..n}$ соответствует набор диапазонов значений идентификационных характеристик z_j, $j = \overline{1..k}$, полученных на этапе регистрации *i*-го субъекта доступа. Данный набор диапазонов представляет собой вектор $D_i = (d_{i1}, d_{i2}, \ldots, d_{ik})$, определяющий интервалы, в которые должны попадать значения соответствующих характеристик для того, чтобы *i*-ый субъект был идентифицирован системой. Каждый элемент d_{ij} для *j*-ой идентификационной характеристики *i*-го субъекта доступа может быть представлен как интервал $[d_{ij_{\min}}; d_{ij_{\max}}]$. А набор всех диапазонов, известных системе, может быть представлен в виде матрицы *D* следующего вида:

$$D = \begin{pmatrix} d_{11} & d_{12} & \ldots & d_{1k} \\ d_{21} & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ d_{n1} & \ldots & \ldots & d_{nk} \end{pmatrix}.$$

Для формального описания процедуры идентификации введены следующие обозначения:

$\hat{p}$ – некий образ, который необходимо идентифицировать;

$\hat{z}$ – вектор зарегистрированных системой значений идентификационных характеристик множества Z, принадлежащих образу $\hat{p}$;

$\hat{z}_j$ – зарегистрированное системой значение характеристики $z_j \in Z$; $j = \overline{1..k}$;

$Q(\hat{p}, p_i)$ – мера близости между образами $\hat{p}$ и p_i, $p_i \in P$, $i = \overline{1..n}$;

$\Phi(\hat{z}, D_i)$ – аналитическое выражение для расчета числовой оценки критерия близости двух образов. Функция для вычисления $Q(\hat{p}, p_i)$;

$v(\hat{z}_j, d_{ij})$ – мера принадлежности зарегистрированного системой значения идентификационной характеристики $\hat{z}_j$ диапазону значений d_{ij} *i*-го образа.

Задача идентификации состоит в том, чтобы ответить на вопрос, соответствует ли предъявленный образ $\hat{p}$ строго одному элементу множества P или нет. Для определения такого соответствия в данной модели использовано понятие меры близости $Q(\hat{p}, p_i)$.

Выбор вида $\Phi(\hat{z}, D_i)$ зависит от особенностей выбранной системы идентификации: например, мера близости может быть рассчитана с использованием расстояния Хэмминга, коэффициента парной корреляции, вероятностных оценок метода Байеса и других метрик.

Обобщенная математическая модель распознавания $\hat{p}$ в общем случае имеет следующий вид:

$$Q(\hat{p}, p_i) = \Phi(\hat{z}, D_i), \; i = \overline{1..n}, \tag{1}$$

$$\hat{p} = p_i \; : \Phi(\hat{z}, D_i) \equiv \text{Max или } \min \Phi(\hat{z}, D_i), \text{ где } p_i \in P, \; D_i \in D, i = \overline{1..n}, \tag{2}$$

$$\hat{p} \notin P \; : \Phi(\hat{z}, D_i) < \text{или} > \text{Lim } \Phi(\hat{z}, D_i), \text{ где } p_i \in P, \; D_i \in D, i = \overline{1..n}. \tag{3}$$

Выражение (2) описывает правило, при котором отнесение $\hat{p}$ к конкретному образу p_i производится по мажоритарной оценке значения функции $\Phi(\hat{z}, D_i)$. При этом обязательным ограничивающим условием выступает выражение (3), согласно которому идентификация представленного образа в текущей системе невозможна в случае, если в зависимости от выбранной метрики оценки близости значение $\Phi(\hat{z}, D_i)$ превышает (или не достигает) некоторый заданный численным значением порог $\text{Lim}\,\Phi(\hat{z}, D_i)$, где $i = \overline{1..n}$.

3. Использование системы контроля и управления доступом в ММПЛ

Согласно [4] комплексное обеспечение безопасности объекта определяется как деятельность по созданию условий и обеспечению ресурсов для предотвращения и уменьшения последствий от угроз различного характера. Для формирования комплексной системы защиты объекта в первую очередь необходимо разработать концепцию безопасности. В [5] подробно рассмотрены вопросы разработки и реализации концепции безопасности и показано, что в общем случае система защиты объекта должна включать в себя следующие элементы:

– организационные мероприятия;

– физическую охрану;

– технические средства обеспечения безопасности (ТСОБ).

Среди множества ТСОБ одним из ключевых элементов являются системы контроля и управления доступом (СКУД). В соответствии с [3] СКУД – совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью. Основными задачами СКУД являются:

– предотвращение несанкционированного доступа в контролируемые зоны с ограниченным доступом;

– организация возможности беспрепятственного прохода (проезда) в зоны со свободным доступом;

– обеспечение условий для соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта.

Особенностью СКУД является тот факт, что их функционирование требует совмещения как ТСОБ, так и организационных мероприятий. Это связано с тем, что для эффективного применения СКУД на защищаемом объекте должен быть строго регламентирован контрольно-пропускной режим (КПР) [3], который представляет собой комплекс организационно-правовых ограничений и правил, инженерно-технических решений и действий подразделе-

ния безопасности, а также устанавливает порядок пропуска через контрольно-пропускные пункты в отдельные здания (помещения) людей, транспорта и материальных средств.

Для решения вышеперечисленных задач современные СКУД обладают следующим функционалом [4, 6]:

1. Защита от несанкционированного доступа на охраняемый объект в режиме снятия их с охраны:

– ограничение доступа посетителей в охраняемые помещения;

– временной контроль перемещений посетителей по объекту.

2. Контроль и учет доступа посетителей на охраняемый объект в режиме снятия их с охраны:

– контроль действий охраны во время дежурства;

– табельный учет рабочего времени персонала;

– фиксация времени прихода и ухода посетителей.

3. Регистрация и выдача информации о попытках несанкционированного проникновения в охраняемое помещение.

4. Совместная работа с системами охранной и пожарной сигнализации, системами видеонаблюдения и т.д. Например, при срабатывании пожарных извещателей разблокируются двери охраняемого помещения.

Функционирование СКУД реализуется следующими программно-техническими средствами:

– устройства идентификации (считыватели, кодонаборные устройства и т.д.);

– средства обнаружения различных материалов (металлодетекторы, обнаружители взрывчатых веществ и радиационных материалов и т.д.);

– устройства обработки информации (контроллеры, панели управлении, согласующие устройства и т.д.);

– исполнительные устройства (электромеханические, электромагнитные и механические кодовые замки, доводчики, турникеты, шлагбаумы и т.д.);

Пример реализации современной СКУД представлен на рис. 1 [4].

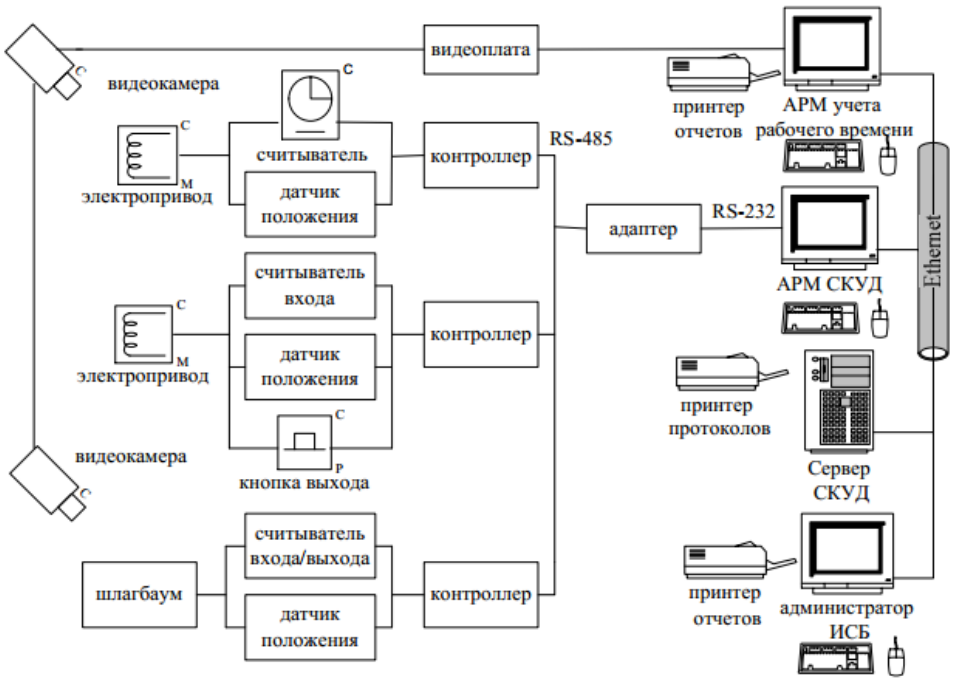

Рис. 1. Пример реализации современной СКУД

Решение вышеперечисленных задач аппаратно-программными и техническими средствами СКУД основано на организации процедуры идентификации личности.

Представленные ранее теоретические выкладки относятся к аспектам моделирования систем идентификации. Однако практическое применение СКУД в ММПЛ обуславливает необходимость не только решить задачу идентификации в общем виде, но и максимально эффективно распознавать предъявляемый образ $\hat{p}$.

В случаях использования биометрии с ростом числа зарегистрированных пользователей понижается вероятность достоверности процедуры идентификации и возрастает время ее проведения, что в свою очередь отражается на протекающих в ММПЛ бизнес-процессах. Другими словами, для решения задачи идентификации посетителей ММПЛ применение технологий биометрической идентификации представляется нецелесообразным. Эффективным представляется применение в ММПЛ таких методов и средств идентификации, в которых мера сходства шаблона и эталона определяется как строгое соответствие.

В настоящее время на практике существует большой спектр электронных идентификаторов для СКУД: штрихкодовые, магнитные карты доступа, смарт-карты, «электронные таблетки» (Touch Memory), «Виганд»-карты и т.д. Большой популярностью в сфере электронных пропусков пользуются RFID-технологии. Однако описанные выше особенности функционирования ММПЛ вносят значительные ограничения на применение подобных идентификаторов.

В то же время политика тотальной проверки и регистрации паспортных данных посетителей объектов в журналах контроля также не находит своего применения на практике ввиду значительного замедления бизнес-процессов ММПЛ.

4. Заключение

Использование современных СКУД позволяет автоматизировать процесс идентификации посетителей, однако порождает проблемы организации первичной инициализации (регистрации) и обслуживания персональных идентификаторов посетителей ММПЛ.

Таким образом, разработка подходов и методик, которые бы позволяли организовать идентификацию посетителей ММПЛ без ущерба для протекающих в них бизнес-процессов, является дальнейшим направлением развития проводимого автором исследования.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2015-2016 годы (проект № 3657).

Литература

1. Постановление Правительства РФ от 25 марта 2015 г. № 272 «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране полицией, и форм паспортов безопасности таких мест и объектов (территорий)».
2. Распоряжение Правительства РФ от 2 ноября 2009 года N 1629-р.
3. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом Классификация. Общие технические требования. Методы испытаний. М.: Госстандарт России, 1999.
4. *Рыжова В. А.* Проектирование и исследование комплексных систем безопасности. СПб.: НИУ ИТМО, 2012. 157 с.
5. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. М.: Стандартинформ, 2010.
6. *Синилов В. Г.* Системы охранной, пожарной и охранно-пожарной сигнализации: учебник. 5-е изд., перераб. и доп. М.: Академия, 2010. 512 с.
7. *Африн А. Г., Аралбаев. Т.З.* Повышение производительности устройства распознавания образов на основе метода ассоциативной организации памяти эталонов // Автоматизация в промышленности. 2007. № 9. С. 7–10.

8. *Мещеряков Р.В.* Технология усиленной аутентификации пользователей информационных процессов / Р.В. Мещеряков, М.В. Савчук, И.А. Ходашинский, И.В. Горбунов // Доклады ТУСУР, 2012. – № 2 (34). Ч.3. – С. 236–248.

Статья поступила в редакцию 15.02.2016

Исхаков Андрей Юнусович
инженер института систем интеграции и безопасности Томского государственного университета систем управления и радиоэлектроники (634045, Томск, ул. Красноармейская, 146) тел. (3822) 900-111, e-mail: iay@security.tomsk.ru

Identification process model in access control systems

Andrey Y. Iskhakov

In this article, the questions of procedures modeling of access control and inside-object modes in crowded places are considered. Features of functioning of such objects and restrictions for using access control and management system application are identified. Identification process model in access control and management systems is developed.

Keywords: identification, access control, model, process.