УДК 796.5:681.3.01

Е.В. Пахомов

ТЕХНОЛОГИИ КОНТРОЛЯ ДОСТУПА НА ПРЕДПРИЯТИИ ИНДУСТРИИ ГОСТЕПРИИМСТВА

Цель данной работы заключается в определении системы контроля доступа как необходимого элемента комплексной автоматизации гостиничного предприятия. Задачей исследования является анализ видов и вариантов развертывания систем. В результате исследования выявлена типовая структура системы контроля доступа на предприятии индустрии гостеприимства.

Система контроля доступа; электронный замок; электронный ключ; смарт-карта; технология RFI; стандарт ближней радиосвязи NFC.

E.V. Pakhomov

ACCESS CONTROL TECHNOLOGY FOR HOSPITALITY ENTERPRISE

The basic purpose of the paper is to define an access control system as the necessary element of all-round automation of hospitality enterprise. The main task of the research is to analyze different kinds and variants of development of such systems. As a result it is given a typical structure of an access control system for hospitality enterprise.

Access control system, electronic lock; electronic key; smart-card; Radio Frequency Identification; Near Field Communication.

Предшественниками электронных замков были механические замки, появившиеся в начале 70-х годов и использующие ключи в виде перфокарт. С этого времени можно вести историю специализированных замков для гостиниц.

В результате всестороннего развития технологий в индустрию гостеприимства из банковской сферы пришли пластиковые карты с магнитной полосой. Электронный ключ стал многофункциональным – помимо выполнения основной функции выступал инструментом безналичных расчетов, хранил информацию об условиях обслуживания клиента. В настоящее время карты с магнитной полосой распространены наиболее широко [1].

В состав системы контроля доступа (СКД) входят следующие компоненты:

- электронный ключ;
- электронный замок;
- считыватель электронного ключа;
- комплекс управления электронными замками, включающий:
  - устройство для кодирования ключа (энкодер);
  - устройство для программирования электронного замка (программатор);
  - клиент-серверное ПО, которое функционирует на компьютере или на специальном терминале.

Одно из основных преимуществ электронных ключей состоит в их универсальности.

При поселении гостю выдается электронная карта-ключ, которая действует в течение срока его пребывания в отеле. В ключ с помощью специального устройства – энкодера, установленного на стойке портье, заносится необходимая информация. Новому гостю каждый раз генерируется новый ключ.

Ключ обеспечивает постояльцу доступ не только в номер, но и в различные зоны отеля, где он, в течение срока проживания, может воспользоваться дополнительными услугами, например бассейном, тренажерным залом, сауной. Сотрудник отеля может с помощью одного ключа открывать номера и другие помещения оте-

ля, в соответствии с выделенными правами доступа. Такой способ организации контролируемого доступа в помещения называется «Мастер-система».

Карта-ключ может быть средством осуществления безналичных расчетов в рамках единого платежного пространства на территории гостиничного комплекса. С ее помощью гость оплачивает заказ в ресторане, посещение SPA-салона, фитнес-центра, прокат спортивного инвентаря, услуги бизнес-центра, покупку сувениров и т.д.

Электронные карты предоставляются посетителям, т.е. клиентам, не проживающим в отеле, но пользующимся некоторыми его услугами в течение выделенного времени и на определенных условиях расчетов.

Если гостиница не требует от клиентов возврата электронного ключа при выписке, то карта может служить рекламой отеля или какого-либо другого предприятия сферы сервиса, тогда затраты на изготовление ключа частично покрываются из маркетингового бюджета или за счет спонсора.

Рассмотрим виды электронных ключей.

Пластиковая карта с магнитной полосой. К основным преимуществам карт с магнитной полосой относятся их невысокая стоимость и наличие общепризнанных стандартов на оборудование таких систем, что способствовало их широкому распространению в различных сферах бизнеса. Магнитная полоска выступает в качестве носителя информации, которая размещается на трёх дорожках. Первая – свободна для записи данных по учету рабочего времени сотрудников, параметров программы лояльности, клубной системы и др. Вторая дорожка, согласно стандартам, используется для осуществления безналичных расчетов. Третья содержит, собственно, информацию о правах доступа.

Смарт-карта – пластиковая карта со встроенной микросхемой. Функциональность карты обеспечивается наличием микропроцессора и небольшой операционной системы, что позволяет хранить зашифрованную информацию и осуществлять ее защиту при чтении, записи и передаче.

Популярно использование смарт-карт в банковском обслуживании в качестве кредитных карт, способных хранить информацию о счете клиента. В электронных платежных системах карта выполняет функцию электронного кошелька.

Можно выделить следующие преимущества смарт-карт перед картами с магнитной полосой:

- за счет наличия памяти микросхема обладает большей информационной емкостью, что расширяет функциональность карты;
- карта обладает надежной системой защиты от подделки благодаря внедренным в чип криптоустойчивым алгоритмам шифрования. Обмен информацией осуществляется в зашифрованном виде, что устраняет возможность перехвата информации;
- карта более устойчива к воздействию окружающей среды, в том числе к размагничиванию, что увеличивает срок ее службы.

Смарт-карты сложнее в техническом исполнении, поэтому имеют более высокую стоимость. Кроме того, производители соответствующих систем пока не пришли к единому стандарту, что несколько сдерживает применение данной технологии в гостиницах.

Проксимити-карты относятся к категории бесконтактных смарт-карт и называются RFID-картами. RFID (Radio Frequency Identification – радиочастотная идентификация) – технология идентификации, в которой обмен информацией между ключом и считывателем осуществляется посредством радиосигналов.

Технология RFID имеет широкое применение в других сферах человеческой деятельности, среди которых транспортная и складская логистика, платежи в общественном транспорте, электронные паспорта [2].

Карта содержит так называемую RFID-метку или транспондер, в памяти которой записан ее уникальный идентификационный код и пользовательская информация. Метка состоит из микросхемы, являющейся информационным носителем, и антенны, которая способна излучать за счет встроенного элемента питания (активная метка), либо функционирует за счет энергии излучения считывателя (пассивная метка). Дальность действия пассивной метки варьируется от 10 см до нескольких метров, радиус считывания активной метки – до 300 м.

В зависимости от вида, память метки позволяет:

- только чтение данных (RO – Read Only). Данные заносятся в память один раз при изготовлении, после этого их изменение или дальнейшая запись невозможны. Полученные ключи пригодны только для идентификации;
- однократную запись данных (WORM – Write Once Read Many). В памяти метки содержится уникальный код, и есть область, куда можно однократно поместить информацию для ее дальнейшего считывания;
- чтение и запись данных (RW – Read and Write). Данные в соответствующей области памяти могут быть перезаписаны.

Преимущества систем на проксимити-картах, по сравнению с системами на магнитных картах:

- использование ключа не требует физического контакта с замком, в котором, соответственно, отсутствует картоприемник, куда могла бы попасть вода, грязь или посторонние предметы. Замок дольше служит и обладает высокой вандалозащищенностью. То же касается энкодеров;
- ключи меньше изнашиваются, проще в использовании, не подвержены размагничиванию, лучше защищены от подделки.

Недостатки рассматриваемых систем:

- более высокая стоимость ключа и остального оборудования;
- данная технология пока не получила распространение в смежных областях, например в системах безналичных расчетов.

Метку можно встроить в брелок или браслет, которые будут выполнять функции ключа, это применимо в SPA-отелях, курортных комплексах.

Электронный ключ iButton (Touch Memory). Ключ представляет собой микросхему с источником питания, заключенную в капсулу в виде таблетки со стальным корпусом. Микросхема имеет уникальный серийный номер, присваиваемый при изготовлении, и область перезаписываемой памяти, куда заносится, например, информация о номере комнаты и времени проживания гостя. Обмен информацией происходит при контакте ключа со считывателем. Предусмотрена возможность парольной защиты и шифрования данных.

Основное преимущество ключей iButton перед электронными ключами других типов состоит в их высокой надежности. Электронная «таблетка» имеет прочный влагонепроницаемый корпус, широкий температурный диапазон эксплуатации, не чувствительна к магнитным и статическим полям, может быть прикреплена к любой поверхности, в том числе на пластиковую карту или браслет.

Сфера применения устройств очень широка и, помимо систем контроля доступа, включает системы электронных платежей на общественном транспорте, системы учета рабочего времени, продукции на складе, санатории и лечебные учреждения (электронная карта пациента в браслете) и др.

Отдельно следует отметить стандарт ближней радиосвязи NFC (Near Field Communication), который является развитием технологии RFID. NFC-устройства

содержат одновременно метку и считыватель и взаимодействуют между собой, находясь на расстоянии нескольких сантиметров. Малые размеры и низкое энергопотребление NFC-чипа позволяют встраивать его даже в пластиковую карту. Данная технология ориентирована на использование в мобильных устройствах, прежде всего в сотовых телефонах. Стандарт задумывался для реализации безопасных электронных платежей, учитывая, что обмен данными между устройствами происходит на малой дистанции и их невозможно перехватить. Однако диапазон применения технологии значительно шире и включает системы контроля доступа.

Клиент бронирует гостиничный номер, после подтверждения оплаты ему высылается SMS-сообщение с кодом ключа. При поселении гость, минуя стойку портье, проходит к своему номеру и, пользуясь телефоном как ключом, открывает его.

Стандарт получил поддержку ряда крупных компаний-производителей мобильных телефонов и имеет хорошие перспективы.

Электронный замок обладает энергонезависимой памятью, в которой хранится различная информация:

- номер комнаты;
- разрешения на доступ;
- действия, выполненные с замком, – «события»: открытие замка, попытка открытия замка, программирование замка, экстренное открытие замка с помощью программатора и др.;
- фамилии пользователей, выполнивших действия, и время;
- служебная информация например, состояние батарей замка.

Информация из памяти замка (права доступа, протокол событий и др.) может быть записана на карты гостей и персонала.

Наличие памяти позволяет расследовать случаи пропажи вещей из номера, защититься от необоснованных претензий со стороны гостя, поскольку замок хранит историю открываний. Современные замковые системы имеют функции «антипаника» – замок открывается изнутри одним поворотом дверной ручки; «не беспокоить» – при повороте ригеля загорается индикатор на внешней стороне замка, означающий, что гость в номере; поддерживают несколько режимов работы: режим гостевого номера, режим свободного прохода, автоматическое переключение между этими режимами. Замки содержат часы, что позволяет разграничивать доступ по времени и ограничивать срок действия ключа.

Питание электронного замка осуществляется от батареек, т.е. он функционирует автономно, не завися от системы энергоснабжения гостиницы. Длительность использования батареек – до 3 лет.

Считыватель входит в состав электронного замка и, в зависимости от вида ключа, содержит магнитную головку, контакт для соприкосновения с микросхемой смарт-карты или приемопередающую антенну. Существуют настенные считыватели, используемые для управления автоматическими устройствами (лифтами, турникетами, шлагбаумами и др.).

Устройство для кодирования ключа (энкодер) записывает в память ключа или считывает оттуда различные данные, например срок действия ключа, номер комнаты, номер счета клиента в системе, параметры клубной, бонусной систем. Различают энкодеры для магнитных карт, смарт-карт, RFID-карт.

Программатор зачастую представляет собой обычный карманный ПК и используется для первоначального программирования замка, считывания информации из его памяти, экстренного открывания, подпитки замка.

Следующим компонентом комплекса управления электронными замками является специализированное программное обеспечение, устанавливаемое на компьютер. В более простом варианте предлагается терминал, представляющий собой

моноблок, в составе которого находятся ПО, энкодер и программатор. К основным функциям специализированного ПО относятся: контроль за изготовлением ключей, отмена ключей, интеграция с АСУ гостиницы и гостиничными системами продаж (POS-системами), поддержка различного оборудования. Основу ПО составляет база данных. В зависимости от размера гостиницы, для управления данными могут быть использованы промышленные СУБД типа MS SQL Server или СУБД для рабочих групп типа MS Access.

Программное обеспечение комплекса управления электронными замками должно быть интегрировано с АСУ гостиницы, что позволяет, с одной стороны, автоматически генерировать ключ в момент регистрации гостя, с другой – делает невозможным выдачу ключа без поселения и наоборот. Благодаря протоколированию событий известно, какой сотрудник, когда и кому выдал ключ.

Обеспечение интеграции систем – задача разработчика АСУ гостиницы. Задача решается посредством разработки специализированной интерфейсной программы [3].

В небольшом отеле может быть установлена упрощенная система контроля доступа, без комплекса управления электронными замками. Вместо него для управления замками используются программирующие ключи.

Рассмотрим виды СКД.

Автономные электронные замки можно объединить в систему с централизованным управлением. Такие СКД называются он-лайн-системами. В них, в отличие от офф-лайн-систем, замки связаны с компьютером каналами передачи данных. Линии связи могут быть проводными и беспроводными, в этом случае оправдано применение технологии обмена данными через инфракрасный порт, Wi-Fi-технологии. Большое количество проводов усложняет монтаж и эксплуатацию системы, делает ее менее надежной из-за вероятности обрыва проводов.

Централизованная система функционирует в режиме реального времени и дает возможность:

- удаленно считывать и записывать информацию в память замка;
- отслеживать состояние замка в любой момент времени;
- отслеживать открывания замков и другие действия с ними в режиме реального времени;
- быстро отменять и продлевать ключи;
- определять присутствие гостя в номере. Система контроля доступа может быть дополнена системой энергосбережения, т.е. ключ необходимо вставлять в энергосберегающий контроллер в номере, иначе электроприборы не включатся. Информация о наличии карты в контроллере передается в АСУ гостиницы в реальном режиме.

Основной недостаток он-лайн-систем состоит в их дороговизне, поэтому они мало распространены.

Офф-лайн-системы проще в установке и обслуживании. Для обмена информацией между замками и компьютером используется программатор. Однако такой способ сильно уступает предыдущему в оперативности.

В целях получения функций он-лайн-систем и снижения стоимости СКД к компьютеру подключаются не все замки, а некоторые, расположенные в служебных помещениях, или настенные считыватели, находящиеся в основных зонах отеля. Замки считывают информацию с предъявляемых ключей и передают ее в базу данных. Обратным путем информация может быть записана в ключи, а пользователи «разносят» ее по замкам, открывая их.

Технологии контроля доступа применяются в различных сферах человеческой деятельности. Вместе с тем, гостиничная индустрия имеет свою специфику, поэтому существуют разработчики гостиничных СКД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябов А.* Электронная память замков // Пять звезд. – 2008. – № 4. – С. 47-49.
2. *Платов А.* RFID: спорная технология будущего // Компьютерная газета. – 2009. – № 10. URL: http://www.nestor.minsk.by/kg/2009/10/kg91018.html (дата обращения: 21.01.10).
3. *Алексеев В.И.* Информационные технологии в туризме и гостиничном менеджменте. – СПб.: Д.А.Р.К., 2008. – 224 с.

Пахомов Евгений Вячеславович
Технологический институт федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: pahomov@tti.sfedu.ru.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 88634311426.

Pakhomov Evgeny Vyacheslavovich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: pahomov@tti.sfedu.ru.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 88634311426.

УДК: 338-001.57

М.С. Ракитина

РАЗРАБОТКА МЕТОДИКИ РАСПРЕДЕЛЕНИЯ ФИНАНСОВОЙ ПОМОЩИ МУНИЦИПАЛЬНЫМ ОБРАЗОВАНИЯМ НА ТЕРРИТОРИИ СУБЪЕКТА РФ*

Предлагается методика распределения трансфертов между муниципальными образованиями на территории субъекта РФ, основанная на комплексном применении системного подхода, когнитивного моделирования и рефлексивных игр. Данная методика предназначена для своевременного проведения анализа и принятия решений в области управления межбюджетными отношениями с целью повышения уровня бюджетной обеспеченности муниципальных образований.

Система межбюджетных отношений; уровень бюджетной обеспеченности; интеллектуальный поиск решений; рефлексивное управление; рефлексивные игры.

M.S. Rakitina

DEVELOPMENT OF METHODOLOGY FOR DISTRIBUTION OF TRANSFERS AMONG MUNICIPALITIES IN THE TERRITORY OF THE RF SUBJECT

The paper proposes a method of distribution of transfers among municipalities in the territory of the RF subject, based on an integrated systematic approach, cognitive modeling and reflexive games. This method is intended for timely analysis and decision making in the management of interbudgetary relations in order to increase the budgetary provision of municipal entities.

The system of intergovernmental fiscal relations; the level of budgetary support; intelligent search solutions; reflexive control; reflexive games.

* Работа выполнена в рамках ФЦП «Научные и научно-педагогические кадры», грант № 02.740.11.0379 «Моделирование процессов социального взаимодействия и проблем национальной безопасности Юга России».