

## DigitalRing® Identer

Система контроля и управления доступом (СКУД).

Краткое описание системы.

Программно-аппаратный комплекс **DigitalRing Identer** – это недорогое и эффективное решение для создания интегрированной, полностью сетевой системы контроля и управления доступом (СКУД) на вашем предприятии. Простота монтажа системы, легкость настройки программного и аппаратного обеспечения позволяют в кратчайшие сроки оснастить удобной и современной системой контроля доступа ваш офис, предприятие, склад, гостиницу, учебное заведение, жилое помещение и т.д.



**Система контроля и управлением доступом (СКУД)** – совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также задача оперативного контроля за персоналом и временем его нахождения на территории объекта. Системы контроля и управления доступом прошли длительный эволюционный путь от простейших кодовых устройств, управляющих дверным замком, до сложных распределенных компьютерных систем, охватывающих целые комплексы зданий.

Использование в качестве пропускной системы предприятия СКУД позволяет:

- контролировать доступ людей в служебные помещения и на территорию предприятия;
- контролировать въезд и выезд автомобильного транспорта на(с) территорию(ии) объекта;
- поддерживать базу данных сотрудников и посетителей;
- отслеживать процесс прохождения сотрудниками и посетителями точек контроля;
- организовать учет рабочего времени персонала.

Всем сотрудникам компании, в которой установлена система контроля доступа, выдаются специальные электронные пропуска (бесконтактные идентификаторы), представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в систему контроля доступа, которая на основании анализа данных о владельце идентификатора, принимает решение о разрешении допуска или запрете прохода того или иного сотрудника на охраняемую территорию. База данных позволяет оперативно разыскать сотрудника на территории по последней точке прохода, где он предъявлял идентификатор.

В каждой точке прохода может быть несколько тайм зон (временных ограничений на доступ). Например, сотруднику может быть разрешен проход только в интервале времени с 10:00 до 17:00 часов.

В качестве исполнительных устройств СКУД могут использоваться электромеханические или электромагнитные замки и защелки различных типов, турникеты, автоматические двери и т.п. Объектом доступа может быть не только человек, но и автомобиль, с закрепленным на нем специальным устройством или груз (товар). Исполнительными механизмами доступа в этом случае являются шлагбаумы и автоматические привода ворот.

Среди основных функций которые выполняет СКУД можно выделить следующее:

- контроль и регистрация прохода сотрудников в разрешенное время или в соответствии с допуском в охраняемые помещения;
- ведение архива проходов;
- отображение состояния системы в режиме реального времени на дисплее компьютера;
- автоматический учет рабочего времени;
- сравнение фотографии сотрудника, хранящейся в базе данных, с реальным изображением с видеокамеры зоны прохода;
- воспроизведение звукового сообщения и информации на экране монитора с указанием названия, номера комнаты в следующих случаях:
  - несанкционированного доступа в помещение
  - попытки повреждения оборудования системы
  - пропадания напряжения в сети
  - пропадания связи с помещением
- составления отчетов по параметрам: вход/выход, тревоги, дежурств, рабочего времени и пр.
- фотографирование сотрудников и посетителей с сохранением фотографий в картотеке

**Для решения всех вышеописанных задач идеально подходит программно-аппаратный комплекс DigitalRing Identifier.**

## **Назначение системы**

Программное обеспечение **DigitalRing Identifier** предназначено для построения интегрированных сетевых систем контроля и управления доступом (СКУД) на объектах различного типа. Система позволяет контролировать вход и выход с объекта, перемещение сотрудников и посетителей внутри объекта, производить выдачу пропусков, печать отчетов и выполнять все прочие стандартные функции характерные для систем подобного рода.

## **Отличительные особенности нашей системы**

1. Низкая стоимость.
2. Рекордно малое время и легкость монтажа системы.
3. Простота настройки оборудования.
4. Легкость установки и настройки программного обеспечения.
5. Простота использования системы.
6. Нетребовательность к системным ресурсам.
7. Программное обеспечение не имеет никаких ограничений по количеству подключаемых единиц оборудования.
8. Хорошая масштабируемость системы.
9. Полностью сетевая, открытая, клиент-серверная архитектура.
10. Возможность интеграции как с другими продуктами компании DigitalRing, так и с решениями других производителей.

## Минимальные системные требования

- Операционная система: Windows 2000 или более новая.
- Процессор: Intel Celeron 1 ГГц.
- Оперативная память: 256 Мб.
- Дисковое пространство: 10 Мб + дисковое пространство под базу данных.
- 100 Мбит сетевая плата.

Следует иметь в виду, что приведенные выше системные требования – минимальны и при построении больших систем контроля и управления доступом, требования могут быть серьезно повышены.

## Состав системы

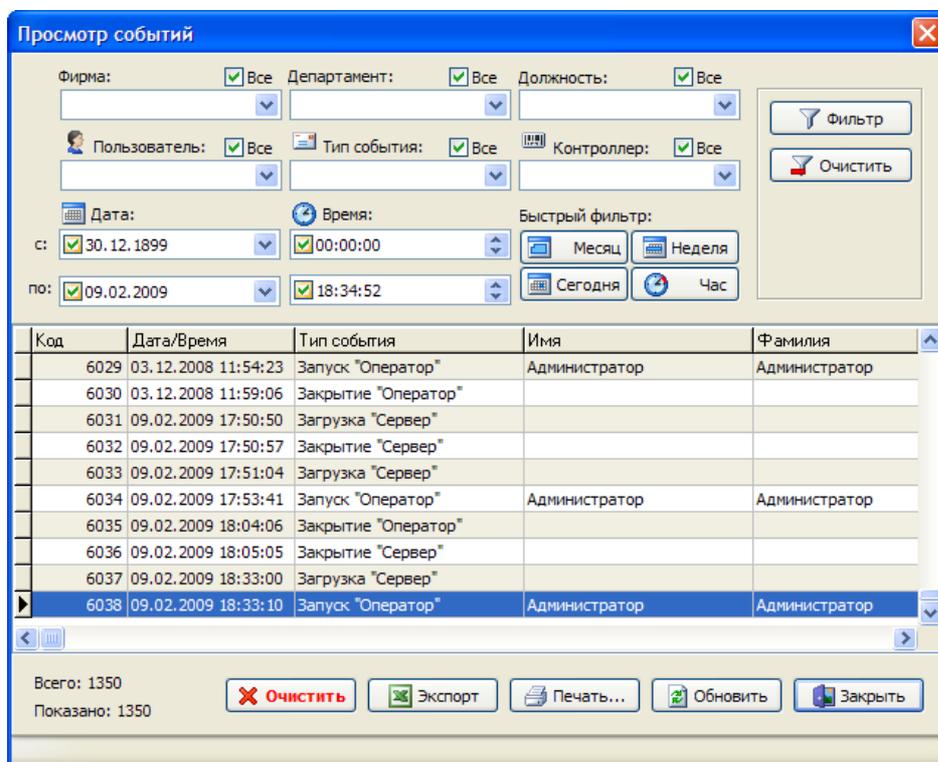
Система контроля и управления доступом DigitalRing Identifier представляет собой программно-аппаратный комплекс, включающий в себя:

- 1. Специализированные сетевые контроллеры.** Каждый такой контроллер представляет собой микрокомпьютер, работающий под управлением Linux-подобной операционной системы. Имеет собственную память, для хранения настроек, порты RS232 и RS485 для подключения считывателей бесконтактных идентификаторов (карт), выходы для управления исполнительными устройствами (замок, турникет). Кроме того, каждый такой контроллер снабжен одним портом Ethernet с поддержкой технологии PoE (питание по сети) и имеет собственный уникальный IP адрес. Встроенное программное обеспечение контроллера позволяет управлять контроллером по сети Ethernet и считывать с него необходимую информацию. При необходимости, встроенное программное обеспечение контроллера может быть модифицировано для выполнения им дополнительных функций. В задачу контроллера входит получение идентификационных номеров со считывателей, декодирование номеров, передача их серверу авторизации, а также управление исполнительными устройствами (замками, турникетами) по командам с сервера.
- 2. Считыватели бесконтактных идентификаторов (карт).** Считыватель представляет собой устройство, которое позволяет считывать информацию, записанную на идентификаторе. Эту информацию он передает на контроллер, который передает ее серверу авторизации и принимает решение о допуске человека в помещение. Устройства контроля доступа позволяют распознавать персональный код доступа при поднесении идентификатора к считывателю. В системе могут использоваться считыватели различных производителей для разных типов карт.
- 3. Идентификаторы.** Наиболее распространенными идентификаторами являются: бесконтактная карточка, пластиковая карточка с магнитным носителем кода или таблетка типа TouchMemory. Один и тот же идентификатор может открывать как одну дверь, так и служить «ключом» для нескольких дверей. Для временных сотрудников и посетителей оформляются временные или разовые «пропуска» – карточки с ограниченным сроком действия.

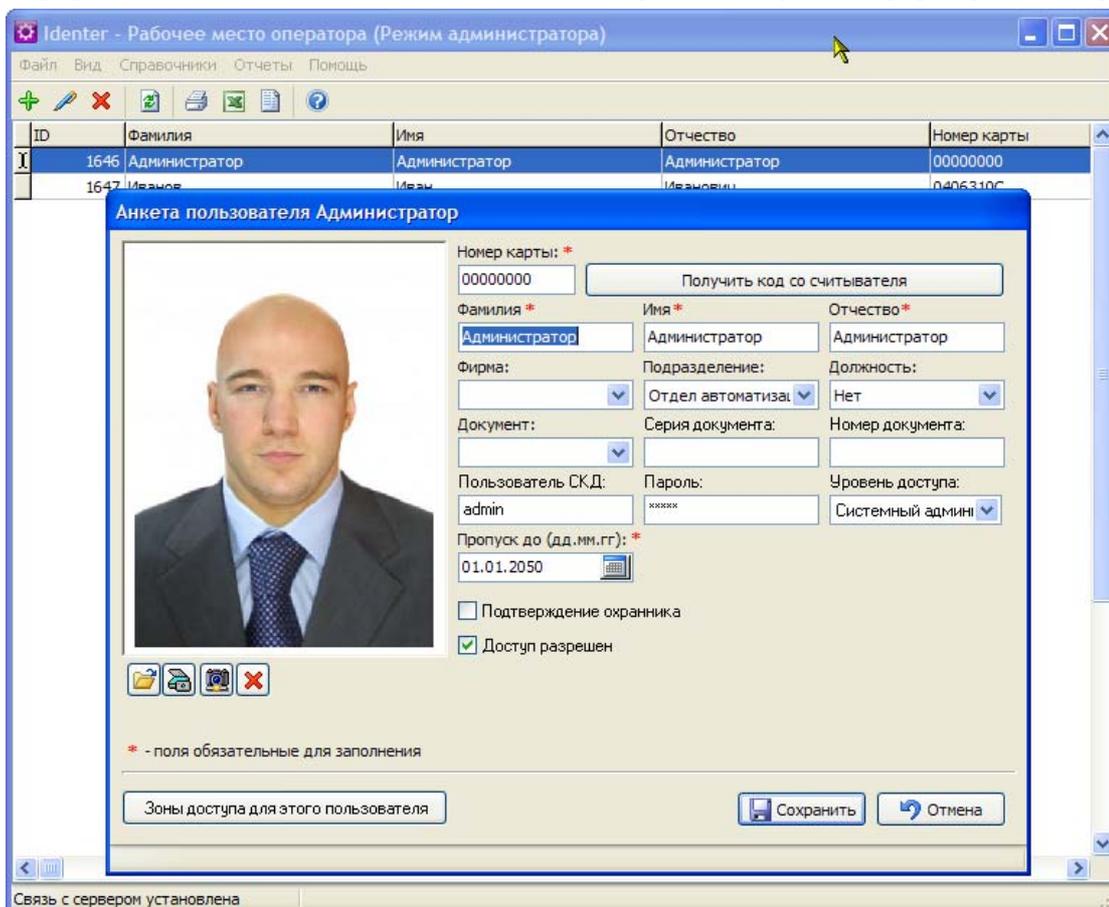


4. **Исполнительные устройства:** электромагнитные и электромеханические замки, турникеты и т.д. Современные СКУД комплектуются в основном электромагнитными замками. Их основное преимущество в отсутствии движущихся частей и исключительной износоустойчивости. Удержание двери осуществляется создаваемым замком магнитным полем с силой до 500 кг. При этом потребление энергии минимальное, а эффективность выше всяких ожиданий. Электромеханические турникеты предназначены для использования в системах контроля доступа в тех случаях, когда необходимо обеспечить контроль однократных проходов при высокой пропускной способности турникета.
5. **Сервер авторизации, сервер контроля доступа.** Основной элемент системы контроля и управления доступом. В задачу сервера авторизации входит поддержание связи с имеющимися сетевыми контроллерами, прием и обработка информации присылаемой контроллерами, а также управление контроллерами и состоянием подключенных к ним исполнительных устройств. Именно сервер авторизации, на основании информации имеющейся в базе данных системы принимает решение о разрешении или запрете на доступ тому или иному идентификатору. В системе может одновременно присутствовать несколько серверов контроля доступа работающих совместно или резервирующих друг друга.
6. **База данных системы контроля доступа.** Может располагаться как на отдельном сервере (для достижения максимальной производительности системы), так и на том же компьютере, где располагается сервер авторизации. База данных содержит в себе следующую информацию:
  - Список пользователей системы контроля доступа с указанием их персональных данных, номера бесконтактного идентификатора, прав и расписаний доступа.
  - Список контроллеров системы с указанием параметров подключения (адрес, порт, логин, пароль и т.д.)
  - Список объектов, к которым предоставляется доступ (зоны, помещения, двери и т.д.)
  - Список расписаний доступа, с возможностью задания индивидуальных расписаний для каждого пользователя и объекта доступа, плавающих расписаний, расписаний с учетом выходных и праздничных дней.
  - Журнал событий системы. В журнале фиксируются все происходящие в системе контроля доступа события: запуск и останов системы, ошибки в работе системы, факты отказа и разрешения доступа к тем или иным объектам и т.д.
  - Прочая служебная информация.

7. **Рабочее место «Начальник службы безопасности».** С помощью данной программы производится настройка и обслуживание системы контроля и управления доступом. Так же из данной программы возможен просмотр журнала событий работы программы и вывод различного рода отчетов.

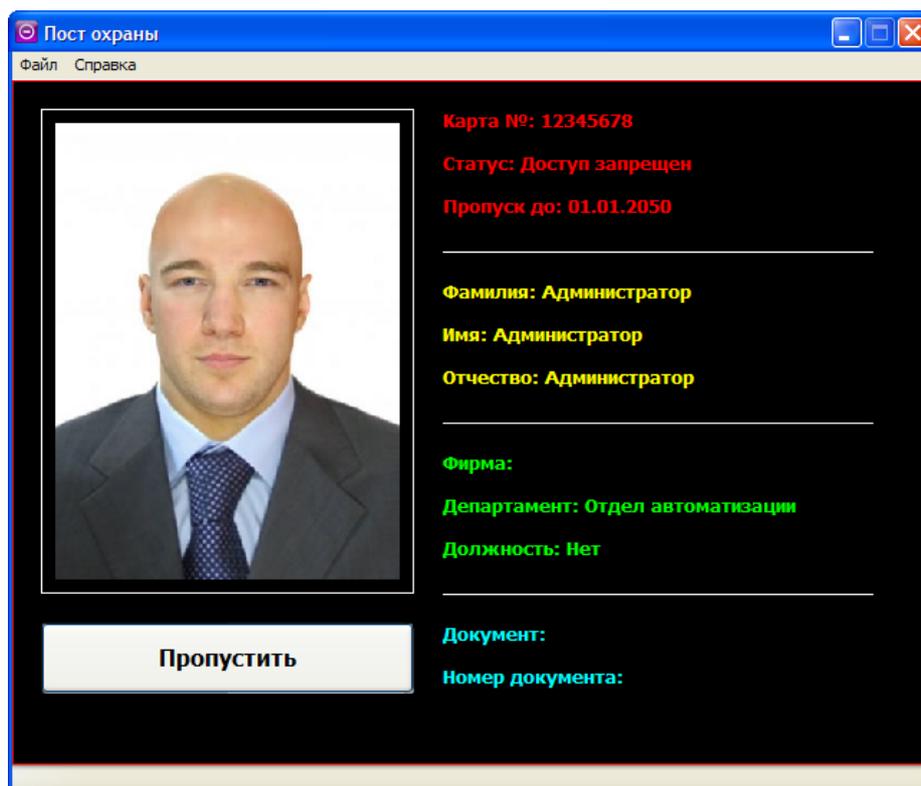


8. **Рабочее место «Бюро пропусков».** Служит для внесения и редактирования информации о пользователях системы контроля доступа и формирования режима



прохода. Для удобства внесения информации данное рабочее место может быть оборудовано персональным контроллером со считывателем бесконтактных идентификаторов (карт), сканером, USB или IP камерой для внесения в базу фотографий пользователей.

9. **Рабочее место «Пост охраны».** Специальная программа, устанавливаемая на компьютер охранника. Позволяет производить визуальный контроль посетителей на предмет соответствия внешности предъявителя бесконтактного идентификатора (карты) и информации содержащейся в базе данных (фотография владельца карты). Кроме этого, с данного рабочего места возможно осуществлять ручное управление выбранной точкой прохода (пропуск посетителя с подтверждением охраны).



Следующий рисунок иллюстрирует работу системы контроля и управления доступом DigitalRing Identifier.

