КАФЕДРА ПРОЕКТИРОВАНИЯ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ СИСТЕМ

Тема 5. Технические решения и проектирование подсистем автоматического управления в ЭСБ различного функционального назначения (Часть 6)

Дисциплина:
«АВТОМАТИКА В ЭЛЕКТРОННЫХ СИСТЕМАХ БЕЗОПАСНОСТИ»

Идентификация но голосу и особенностям речи.
Биометрический подход, связанный с идентификацией голоса, удобен в применении. Однако основным и определяющим недостатком этого подхода является низкая точность идентификации.
При рассмотрении проблемы аутентификации по голосу важными вопросами с точки зрения безопасности являются следующие:

- как бороться против использования магнитофонных записей парольных фраз, перехваченных во время установления контакта законного пользователя с аутентификационным терминалом;
- как защитить систему от злоумышленников, обладающих способностью к имитации голоса, если им удастся узнать парольную фразу.

Работы по повышению эффективности систем идентификации по голосу ведутся постоянно. Существуют системы, где применяется метод совместного анализа голоса и мимики, так как мимика говорящего характерна только ему и будет отличаться от мимики другого человека, говорящего те же слова. Существуют комбинированные системы, состоящие из блоков идентификации и верификации голоса. При решении задачи идентификации находится ближайший голос (или несколько голосов) из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Задача повышения надежности распознавания может быть решена за счет привлечения грамматической и семантической информации в системах распознавания речи.

Идентификация по ритму работы на клавиатуре. Ритм работы на клавиатуре является достаточно индивидуальной характеристикой пользователя и вполне пригоден для его идентификации. Для измерения ритма оцениваются промежутки времени либо между ударами при печатании символов, расположенных в определенной последовательности, либо между моментом удара по клавише и моментом ее отпускания при печатании каждого символа в этой последовательности. Хотя второй способ считается более эффективным, наилучший результат достигается совместным использованием обоих способов.

В качестве исходных данных используют временные интервалы между нажатием клавиш на клавиатуре и время их удержания. При этом временные интервалы между нажатием клавиш характеризуют темп работы, а время удержания клавиш характеризует стиль работы с клавиатурой (резкий удар или плавное нажатие).

Идентификация пользователя по клавиатурному почерку возможна следующими способами: по набору ключевой фразы и по набору произвольного текста.

Принципиальное отличие этих двух способов заключается в том, что в **первом случае** используется ключевая фраза, задаваемая пользователем в момент регистрации его в системе, а **во втором случае** используются ключевые фразы, генерируемые системой каждый раз в момент идентификации пользователя.

Применяются два режима работы: обучение и идентификация.
В **режиме обучения** пользователь вводит некоторое число раз предлагаемые ему тестовые фразы. При этом рассчитываются и запоминаются эталонные характеристики данного пользователя.
В **режиме идентификации** рассчитанные оценки сравниваются с эталонными, на основании чего делается вывод о совпадении или несовпадении параметров клавиатурного почерка.
Применение способа идентификации по клавиатурному почерку целесообразно только по отношению к пользователям с достаточно длительным опытом работы с компьютером и сформировавшимся почерком работы на клавиатуре, то есть к программистам, секретарям и т.д.

Перспективные технологии биометрического контроля. Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. В настоящее время ряд биометрических технологий находится в стадии разработки. К ним относятся технологии на основе:

- термограммы лица в инфракрасном диапазоне излучения;
- характеристик ДНК;
- анализа структуры кожи и эпителия на пальцах;
- анализа отпечатков ладоней;
- анализа формы ушной раковины;
- анализа характеристик походки человека;
- анализа индивидуальных запахов человека;
- распознавания по уровню солености кожи;
- распознавания по расположению вен.

Технология на основе **анализа термограммы лица** является одним из последних достижений в области биометрии. Среди признаков лица, используемых для идентификации человека, наиболее устойчивыми и трудно изменяемыми является признаки изображения его кровеносных сосудов. Разные плотности кости, жира и кровеносных сосудов строго индивидуальны и определяют термографическую картину лица пользователя. Путем сканирования изображения лица в инфракрасном свете создается уникальная температурная карта лица – термограмма. Идентификация по термограмме обеспечивает показатели, сравнимые с показателями идентификации по отпечаткам пальцев.

Технология, построенная на **анализе характеристик ДНК** (метод геномной идентификации) является хотя и самой продолжительной, но и наиболее перспективной из систем идентификации. Метод основан на том, что в ДНК человека имеются полиморфные локусы (положение хромосомы в гене), часто имеющие 8-10 аллелей. Определение набора этих аллелей для нескольких полиморфных локусов у конкретного индивида позволяет получить своего рода геномную карту, характерную только для этого человека.

Для **идентификации человека по руке** используют несколько биометрических параметров – это геометрическая форма кисти руки или пальцев, расположение подкожных кровеносных сосудов ладони, узор линий на ладони. Причиной развития технологии **анализа отпечатков ладоней** послужил тот факт, что устройства для распознавания отпечатков пальцев имеют недостаток – им нужны только чистые руки, а отпечаток грязного пальца система может и не распознать. Поэтому ряд разработчиков сосредоточились на технологии, анализирующей не рисунок линий на коже, а очертания ладони, которые также имеет индивидуальный характер. Однако их анализ традиционными средствами достаточно трудоемок.

Технология **анализа формы ушной раковины** является одной из самых последних подходов в биометрической идентификации человека. С помощью даже недорогой Web-камеры можно получать довольно надежные образцы для сравнения и идентификации.

Также ведутся разработки систем «электронного носа», реализующих процесс распознавания **по запаху.** Наличие генетического влияния на запах тела позволяют считать эту характеристику перспективной для использования в целях биометрической аутентификации личностисистему, состоящую из трех функциональных узлов, работающих в режиме периодического восприятия пахучих веществ: системы отбора и подготовки проб, линейки или матрицы сенсоров с заданными свойствами и блока процессорной обработки сигналов матрицы сенсоров.

Электронная проходная для прохода посетителей по бумажным пропускам со штрих-кодом:

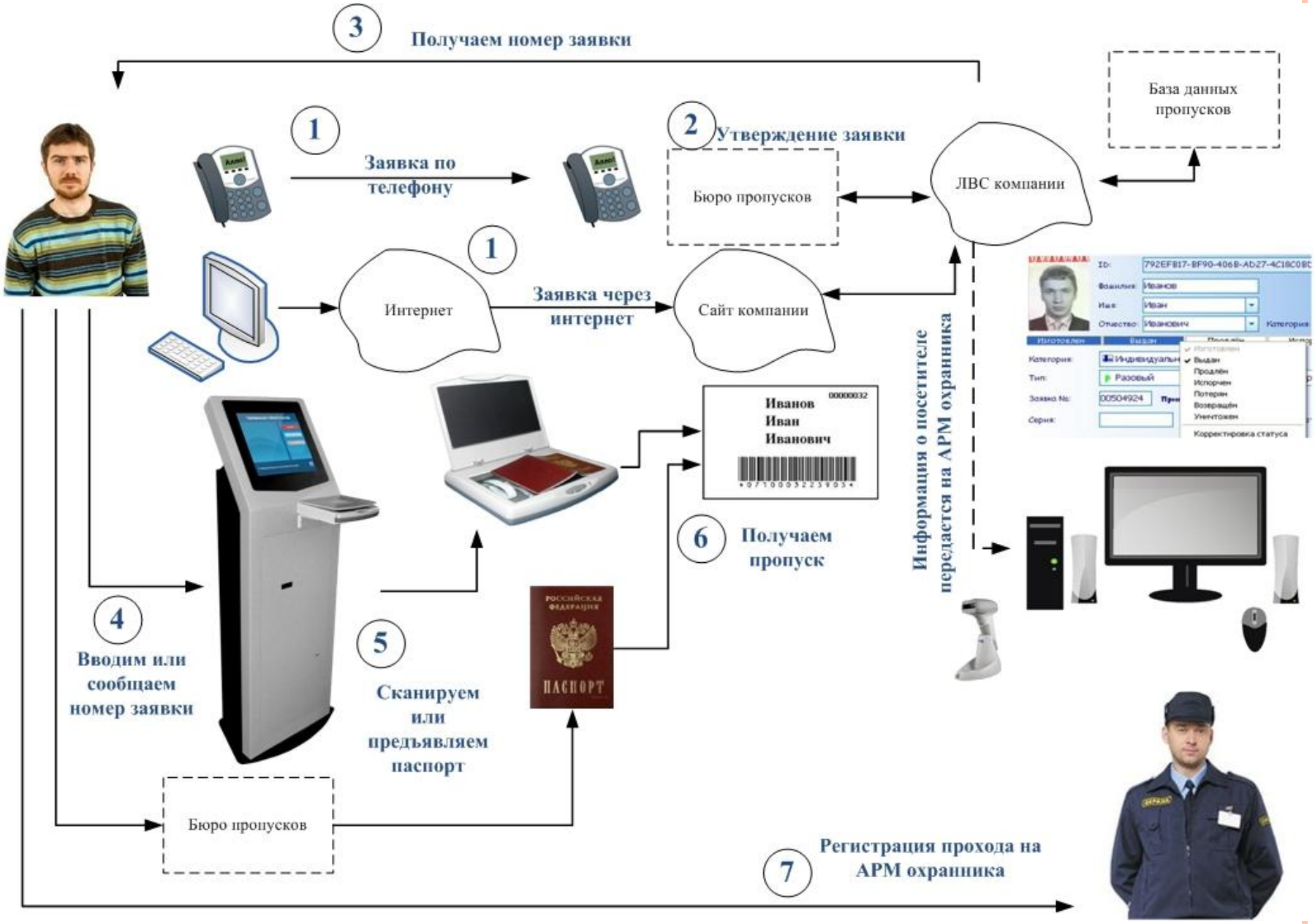
1) посетитель самостоятельно регистрируется (например, через Интернет);
2) данные о посетителе записываются в базу данных пропусков; посетитель получает номер заявки, с которой связывается будущий бумажный пропуск;
3) через бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T” посетитель получает пропуск, на котором нанесен штрих-код;
4) в точке прохода штрих-код с пропуска считывается специальным сканером;
5) информация о посетителе сохраняется в базе данных автономной проходной;
6) информация из базы данных проходной может быть перенесена на внешний носитель.

Особенности:

- процедура сканирования штрих-кода и занесение в базу данных занимает не более 7 секунд;
- охраннику не надо выполнять функции бюро пропусков: он занимается только контролем прохода;
- штрих-код не требователен к качеству печати.

Состав оборудования:

1) Оборудование бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T”
2) АРМ поста охраны (монитор, системный блок)
3) сканер штрих-кода – 1 шт. (контроль при входе на объект) или 2 шт. (контроль при входе и выходе с объекта)


3
Получаем номер заявки
1
Заявка по телефону
2
Утверждение заявки
Бюро пропусков
ЛВС компании
База данных пропусков
1
Интернет
Заявка через интернет
Сайт компании
Информация о посетителе передается на АРМ охранника
Иванов
Иван
Иванович
6
Получаем пропуск
4
Вводим или сообщаем номер заявки
5
Сканируем или предъявляем паспорт
ПАСПОРТ
Бюро пропусков
7
Регистрация прохода на АРМ охранника

Электронная проходная с использованием режима фотоидентификации

1) посетитель регистрируется и получает пропуск со штрих-кодом или радиокарту;
2) данные о пропуске передаются на АРМ охранника по сети;
3) в точке прохода посетитель прикладывает радиокарту к считывателю или считывает штрих-код с пропуска специальным сканером;
4) система выполняет поиск пропуска в базе данных проходной;
5) на мониторе АРМ охранника отображается информация о посетителе (ФИО, фото, время прохода и проч.);
6) охранник принимает решение о пропуске посетителя на объект;

7) информация о проходе посетителя сохраняется в базе данных АРМ охранника;
8) информация из локальной базы данных АРМ охранника может быть передана по сети в интегрированную систему безопасности объекта или перенесена на внешний носитель.

Состав оборудования:
1) Оборудование бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T”
2) АРМ поста охраны (монитор, системный блок)
3) считыватель штрих-кода – 2 шт.
или:
3.1) считыватель радиокарт – 2 шт.

Особенности:

- посетитель может оформить пропуск в бюро пропусков, зарегистрироваться с помощью электронного терминала “Fractal-T”, через Интернет или по телефону;
- при регистрации посетителей с помощью электронного терминала “Fractal-T” требуется только сам терминал и АРМ охранника, бюро пропусков не нужно (полуавтономное решение и экономия средств);
- пропуск со штрих-кодом может быть распечатан на любом принтере и сокращение затрат на создание пропусков;
- данное решение может легко интегрироваться с любыми системами безопасности (СКД, видеонаблюдение, бюро пропусков).

Проходная с турникетом:

1) посетитель регистрируется и получает пропуск со штрих-кодом или радиокарту;
2) данные о пропуске передаются по сети на контроллер проходной (АРМ поста охраны), оборудованной турникетом;
3) в точке прохода посетитель прикладывает радиокарту к считывателю или считывает штрих-код с пропуска специальным сканером;
4) система выполняет поиск пропуска в базе данных проходной;
5) в случае, если в базе данных контроллера проходной (АРМ поста охраны) найден действительный пропуск, турникет открывается;

6) информация о проходе посетителя сохраняется в базе данных контроллера проходной (АРМ поста охраны);
7) информация с контроллера проходной может быть передана по сети в интегрированную систему безопасности объекта или перенесена на внешний носитель.

Состав оборудования:
1) Оборудование бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T”
2) АРМ поста охраны (монитор, системный блок)
3) считыватель штрих-кода – 2 шт.
4) Турникет

Особенности:

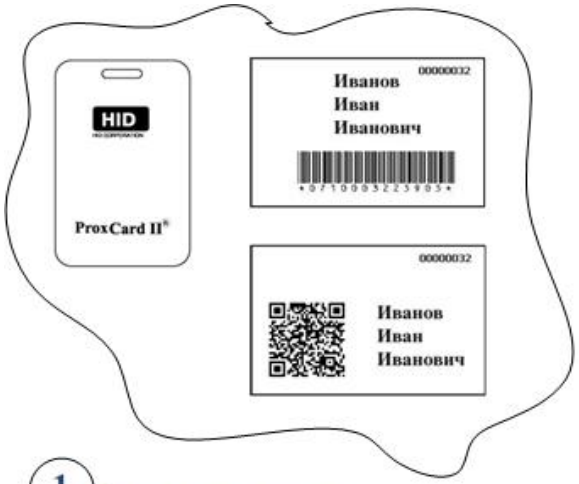
1) Возможно полностью автоматическая работа системы (турникет пропускает посетителя только в том случае, если в базе данных найден действительный пропуск);

2) Система может работать как в автоматическом (без охранника), так и в полуавтоматическом режиме – в последнем случае на АРМ поста охраны отображается информация о посетителе;

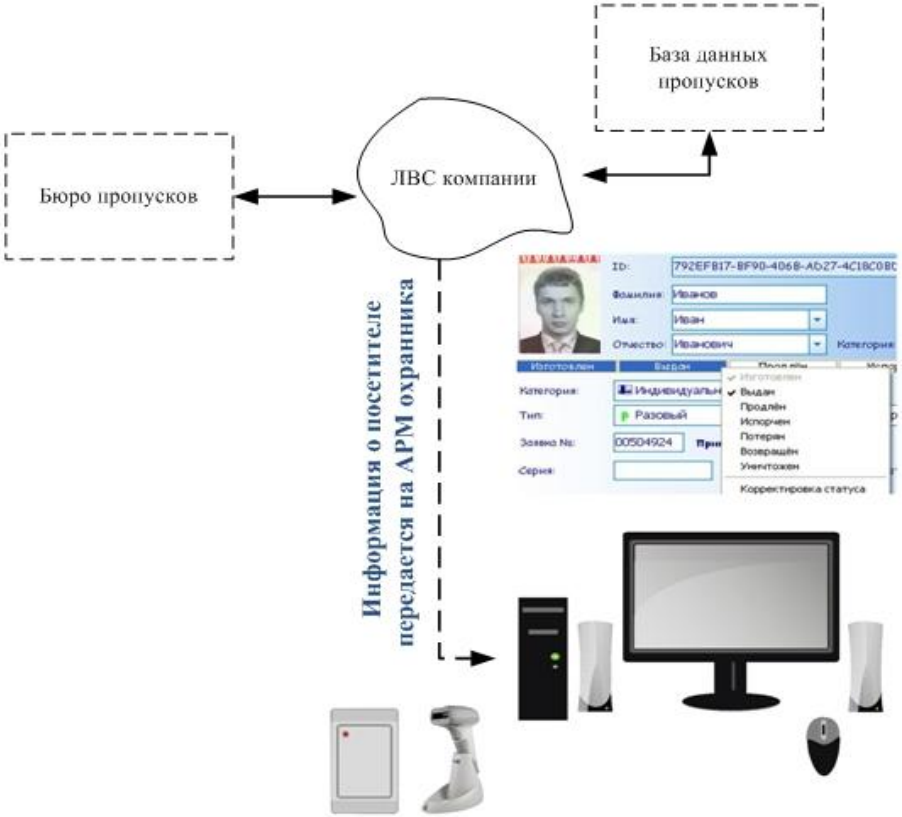
3) Посетитель может оформить пропуск в бюро пропусков, зарегистрироваться с помощью электронного терминала “Fractal-T”, через Интернет или по телефону;

4) При регистрации посетителей с помощью электронного терминала “Fractal-T” требуется только сам терминал и проходная, оборудованная турникетом и контроллером; бюро пропусков не нужно;

5) Информация обо всех посетителях сохраняется в базе данных системы, что актуально в условиях террористической угрозы;
6) Пропуск со штрих-кодом может быть распечатан на любом принтере à сокращение затрат на создание пропусков;
7) Данное решение может легко интегрироваться с любыми системами безопасности (СКД (СКУД), видеонаблюдение, бюро пропусков).



1 Получаем пропуск



2 Регистрация прохода на АРМ охранника при помощи считывателя радиокарт или штрих-кода с последующим проходом через турникет

Уличная проходная – полноростовой турникет для прохода по одному:

1) посетитель регистрируется и получает пропуск со штрих-кодом или радиокарту;
2) данные о пропуске передаются по сети на контроллер проходной, оборудованной турникетом;
3) в точке прохода посетитель прикладывает радиокарту к считывателю или считывает штрих-код с пропуска специальным сканером;
4) система выполняет поиск пропуска в базе данных проходной;
5) в случае, если в базе данных контроллера проходной найден действительный пропуск, турникет пропускает строго одного посетителя;

6) информация о проходе посетителя сохраняется в базе данных контроллера проходной;
7) информация с контроллера проходной может быть передана по сети в интегрированную систему безопасности объекта или перенесена на внешний носитель.

Состав оборудования:
1) Оборудование бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T”
2) Контроллер проходной
3) АРМ поста охраны (монитор, системный блок)- опционально
4) Турникет полноростовой
5) считыватель штрих-кода – 2 шт.

Особенности:

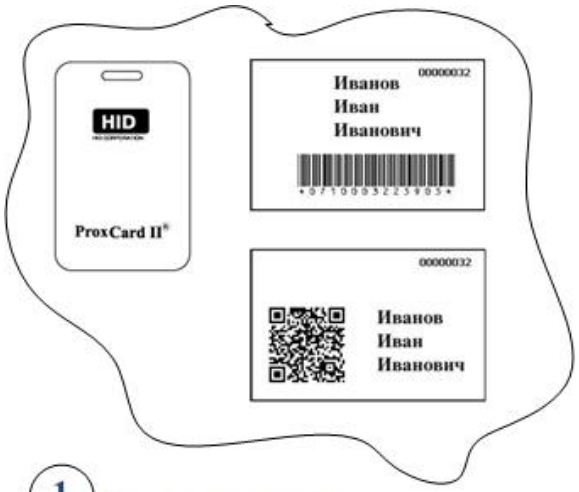
1) Возможно полностью автоматическая работа системы (турникет пропускает посетителя только в том случае, если в базе данных найден действительный пропуск);

2) Система может работать как в автоматическом (без охранника), так и в полуавтоматическом режиме (на АРМ поста охраны может отображаться информация о посетителе);

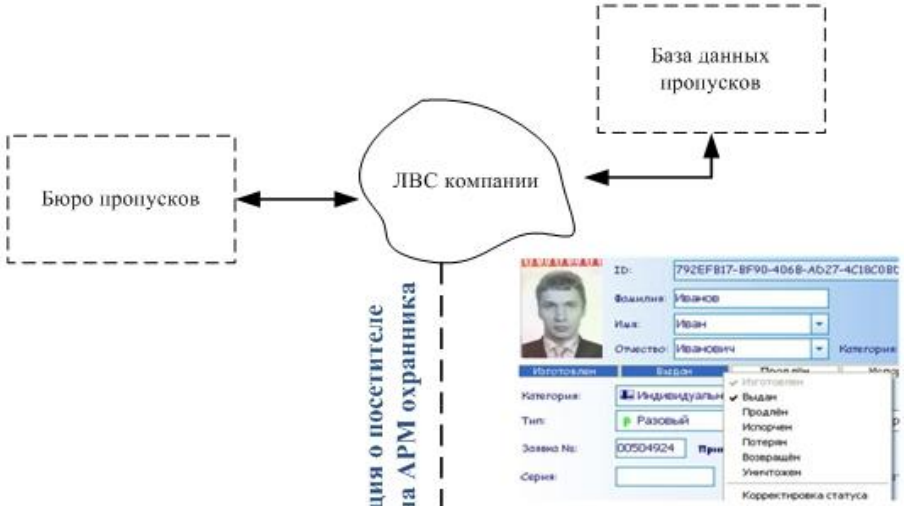
3) Посетитель может оформить пропуск в бюро пропусков, зарегистрироваться с помощью электронного терминала “Fractal-T”, через Интернет или по телефону;

4) При регистрации посетителей с помощью электронного терминала “Fractal-T” требуется только сам терминал и проходная, оборудованная полноростовым турникетом и контроллером;

5) Пропуск со штрих-кодом может быть распечатан на любом принтере и сокращение затрат на создание пропусков;
6) Данное решение может легко интегрироваться с любыми системами безопасности (СКД (СКУД), видеонаблюдение, бюро пропусков).



1 Получаем пропуск



2 Регистрация прохода на АРМ охранника при помощи считывателя радиокарт или штрих-кода с последующим проходом через турникет

Электронная проходная со шлюзом:

1) посетитель регистрируется и получает пропуск со штрих-кодом или радиокарту;
2) данные о пропуске передаются по сети на контроллер проходной, оборудованной шлюзом;
3) посетитель входит в шлюз;
4) после закрытия входной двери шлюза посетитель прикладывает радиокарту к считывателю или считывает штрих-код с пропуска специальным сканером;
5) система выполняет поиск пропуска в базе данных проходной;
6) в случае, если в базе данных контроллера проходной найден действительный пропуск, выходная шлюзовая дверь открывается, посетитель проходит на объект;

Состав оборудования:

1) Оборудование бюро пропусков или электронный терминал регистрации и выдачи пропусков “Fractal-T”

2) АРМ поста охраны (монитор, системный блок)

3) считыватель штрих-кода – 2 шт.

Или считыватель радиокарт – 2 шт.

4) Шлюз с контроллером и пультом управления

Особенности:

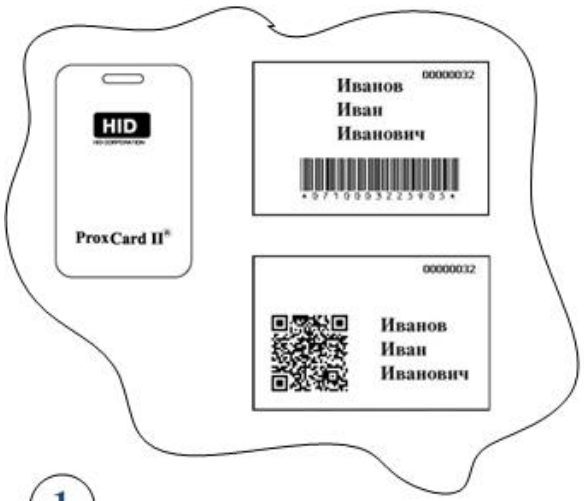
1) Возможно полностью автоматическая работа системы (шлюз пропускает посетителя только в том случае, если в базе данных найден действительный пропуск);

2) Система может работать как в автоматическом (без охранника), так и в полуавтоматическом режиме (на АРМ охранника может отображаться информация о посетителе);

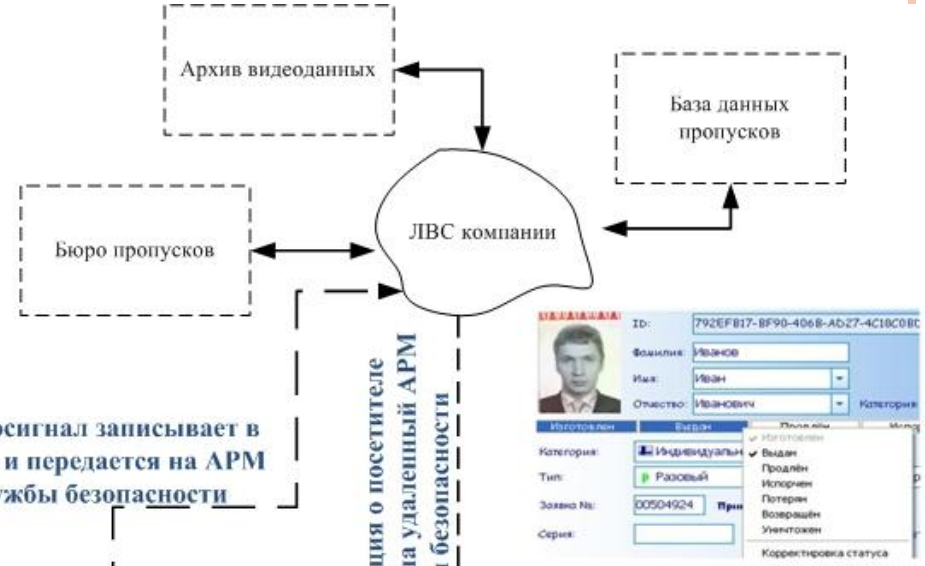
3) Возможен контроль прохода посетителей по второму признаку: кодовая панель или же биометрическая система;

4) Посетитель может оформить пропуск в бюро пропусков, зарегистрироваться с помощью электронного терминала “Fractal-T”, через Интернет или по телефону;

5) При регистрации посетителей с помощью электронного терминала “Fractal-T” требуется только сам терминал и проходная, оборудованная турникетом и контроллером; бюро пропусков не нужно (полуавтономное решение и экономия средств);
6) Информация обо всех посетителях сохраняется в базе данных системы, что актуально в условиях террористической угрозы;
7) Пропуск со штрих-кодом может быть распечатан на любом принтере à сокращение затрат на создание пропусков;
8) Данное решение может легко интегрироваться с любыми системами безопасности (СКД (СКУД), видеонаблюдение, бюро пропусков, система учета рабочего времени).

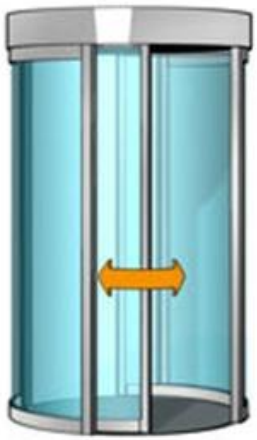


1 Получаем пропуск



Регистрация прохода на АРМ охранника при помощи считывателя радиокарт или штрих-кода с последующим проходом через шлюз

2



Электронная проходная + бюро пропусков:

1) посетитель обращается в бюро пропусков и получает пропуск со штрих-кодом или радиокарту;
2) данные о пропуске передаются в базу данных электронной проходной по сети;
3) в точке прохода посетитель прикладывает радиокарту к считывателю или считывает штрих-код с пропуска специальным сканером;
4) система выполняет поиск пропуска в базе данных проходной;
5) на мониторе АРМ охранника отображается информация о посетителе (ФИО, фото, время прохода и проч.);
6) охранник принимает решение о пропуске посетителя на объект;

7) информация о проходе посетителя сохраняется в базе данных электронной проходной;
8) информация из локальной базы данных электронной проходной может быть передана по сети в интегрированную систему безопасности объекта или перенесена на внешний носитель.

Особенности:
1) Строгий учет всех выданных пропусков;
2) Информация обо всех посетителях сохраняется в базе данных системы, что актуально в условиях террористической угрозы;
3) Данное решение может легко интегрироваться с любыми системами безопасности (СКД (СКУД), видеонаблюдение).

Состав оборудования:

1) Оборудование бюро пропусков IDmatic
2) АРМ поста охраны (монитор, системный блок)
3) считыватель штрих-кода – 2 шт.

Или считыватель радиокарт – 2 шт.