

ИНФОФОРУМ-Евразия

10–11 июня 2010 г.

Новый Арбат, 36



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ЯДЕРНЫЙ УНИВЕРСИТЕТ (НИЯУ) «МИФИ»

***«Интегрированные системы
безопасности на основе
биометрических технологий.
Опыт применения».***

*Дураковский Анатолий Петрович, к.т.н., НИЯУ МИФИ
Крахмалёв Александр Кузьмич, к.т.н., ООО НПФ «Сигма-ИС»*

Интегрированные системы (ИСБ)

ИСБ – перспектива развития технических систем безопасности

ИСБ – объединение на единой аппаратно-программной платформе технических средств безопасности, предназначенных для защиты объекта от нескольких видов угроз

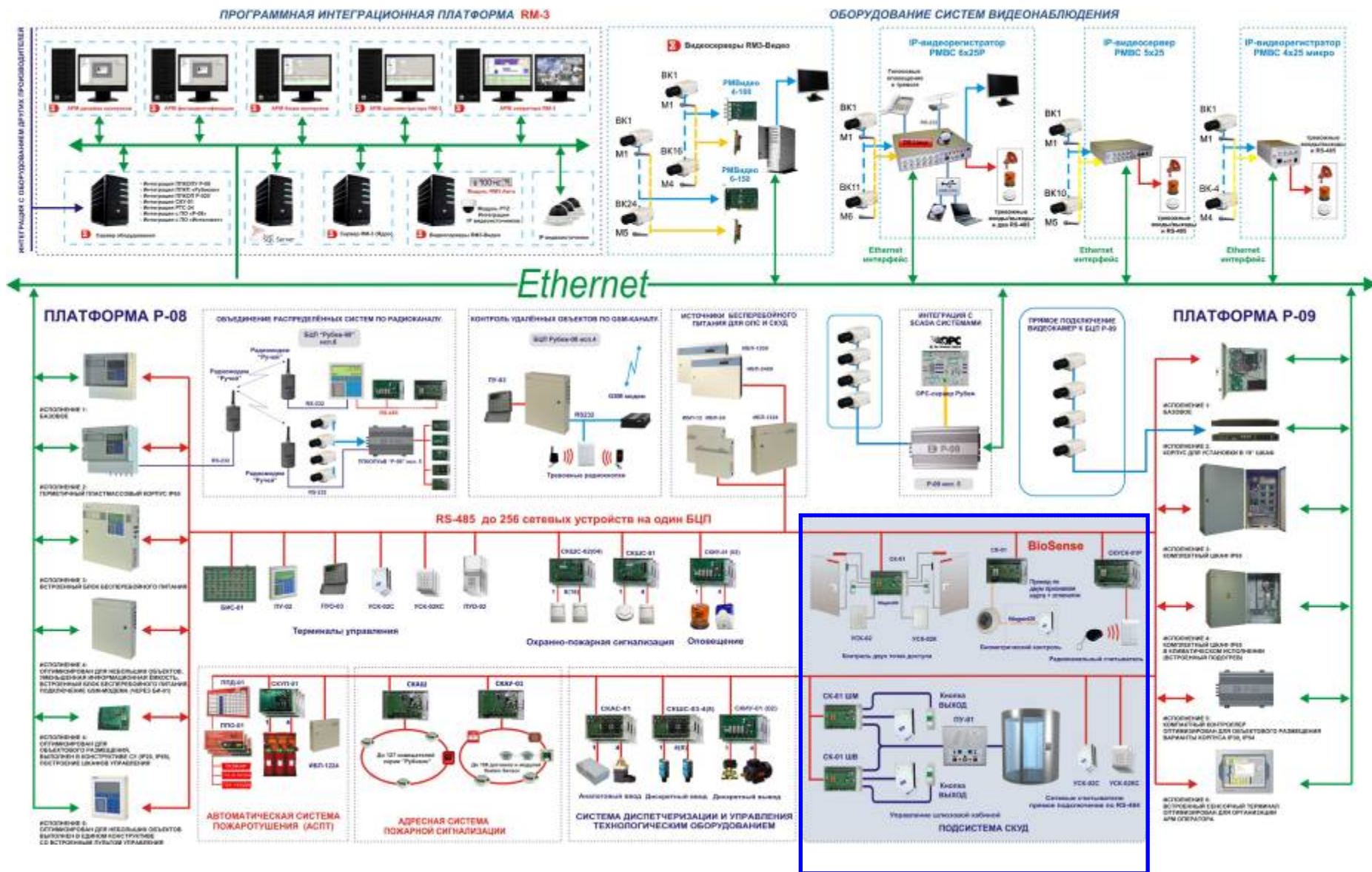
Состав ИСБ:

1. Охранная сигнализация
2. Пожарная сигнализация и противопожарная автоматика
3. Системы контроля доступа (СКУД)
4. Системы телевизионного наблюдения (охранного телевидения – СОТ)

Дальнейшие пути развития ИСБ

1. Объединение ИСБ с автоматизированием управления инженерными подсистемами здания, объекта – системы «интеллектуального здания» (для жилых, офисных зданий)
2. Автоматизированные системы управления функционированием, жизнеобеспечением, безопасностью - АСУ ФЖБ (для производственных зданий, объектов, сооружений)
3. Системы мониторинга безопасности территориально распределенных объектов с единым центром контроля (ситуационные центры, центры управления кризисными ситуациями ЦУКС)

Подсистема СКУД в общей структуре ИСБ «Рубеж»



Роль СКУД в обеспечении комплексной безопасности.

- ❑ Ограничение доступа в опасные помещения, контроль над перемещением персонала по объекту, позволяет повысить технику безопасности и снизить риск технологических аварий.
- ❑ Автоматизация учета рабочего времени, повышение дисциплины, охрана технологических и коммерческих секретов от промышленного шпионажа, предотвращение преступлений и краж на рабочем месте и т.д.
- ❑ Автоматизация процесса контроля доступа может снизить человеческий фактор и в общем случае привести к экономии средств на обеспечение безопасности
- ❑ Интеграция СКУД с системой телевизионного наблюдения и охранно-пожарной сигнализации позволяет повысить безопасность объекта в целом за счет оперативного взаимодействия подсистем в ИСБ.
- ❑ Управление оборудованием жизнеобеспечения объекта. (Управление освещением, обогревом, вентиляцией, кондиционированием воздуха и другим оборудованием. Экстренное автоматическое открывание дверей в критических ситуациях).

Участие в разработке нормативная базы на СКУД.

Работа в части создания нормативной базы и стандартов в области ИСБ (СКУД, СОТ, ОПС) ведется техническими комитетами (ТК) по стандартизации **Федерального агентства Российской Федерации** по техническому регулированию и метрологии:

- ❑ **ТК 234 «Технические средства противокриминальной безопасности»** (ведущая организация – **ФГУ «НИЦ «Охрана» МВД России**);
- ❑ **ТК 439 «Средства автоматизации и системы управления»** (ведущая организация – **Международная ассоциация МА «Системсервис»**);
- ❑ **ТК 22 / ПК 129 «Информационные технологии / Кодированное представление видео/аудио информации, мультимедийной и гипермедийной информации** (ведущая организация – **НПФ ООО «Сигма-ИС»**);

Международные организации по стандартизации:

- ❑ **МЭК / IEC** (Международная электротехническая комиссия – International Electrotechnical Commission) – международная организация по стандартизации в области электрических, электронных и смежных технологий.
- ❑ Комитет **IEC TC 79, Alarm and electronic security systems**
- ❑ **ИСО / ISO** (Международная организацией по стандартизации - International Organization for Standardization)
- ❑ **CENELEC** (European Committee for Electrotechnical Standardization) — Европейский комитет электротехнической стандартизации отвечающий за европейские стандарты в области электротехники

Система стандартов МЭК по противокриминальной безопасности (IEC TC 79, Alarm and electronic security systems)

В систему стандартов входит **26** стандартов, разработанных с 1998 по 2001 годы с последующими поправками. Во многих странах эти стандарты приняты в качестве национальных

Сейчас активно ведется работа по пересмотру этих документов и включению в их состав стандартов на **СКУД**, **СОТ** и отдельного стандарта на **ИСБ**.

| | |
|--|--|
| IEC 60839-1-1 | Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 1: Общие положения |
| IEC 60839-1-2 | Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 2: Источники электропитания, методы испытаний и критерии качества работы |
| IEC 60839-1-3 | Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 3: Испытания на воздействие внешних факторов |
| IEC 60839-1-4 | Системы тревожной сигнализации. Часть 1: Общие требования. Раздел 4: Правила по практическому применению |
| IEC 60839-2 (части 2,3,4,5,6,7) | Системы тревожной сигнализации. Часть 2: (6 стандартов - требования к охранам извещателям) |
| IEC 60839-5 (части 1,2,4,5,6,7) | Системы тревожной сигнализации. Часть 5: (6 стандартов - требования к системам передачи сигналов тревоги). |
| IEC 60839-7 (части 1,2,3,4,5,6,7,11,12,20) | Системы тревожной сигнализации. Часть 7 (10 стандартов - форматы сообщений и протоколы для интерфейсов последовательных данных в системах передачи) |
| IEC 60839-10-1 | Системы тревожной сигнализации. Часть 10: Системы охранной сигнализации для дорожного транспорта. Раздел 1: Легковые автомобили |

Европейские стандарты на СКУД

| | |
|-------------------------|--|
| EN 50133-1:1996/A1:2002 | Системы тревожной сигнализации. Системы контроля доступа, используемые в целях безопасности. Часть 1. Требования к системам |
| EN 50133-2-1:2000 | Системы аварийной сигнализации. Системы контроля доступа, используемые в целях безопасности. Часть 2-1. Общие требования к компонентам |
| EN 50133-7:1999 | Системы тревожной сигнализации. Системы контроля доступа, используемые в целях безопасности. Часть 7. Руководство по эксплуатации |

Эти европейские нормы, рассматриваются в ISO/IEC TC 79 в качестве проекта международного стандарта на СКУД.

Рассматривается также в качестве основы для международного стандарта на СКУД национальный стандарт Канады **CAN/ULC-S319-05 «ELECTRONIC ACCESS CONTROL SYSTEMS»**

Нормативная база СКУД. ГОСТ Р 51241-2008

ГОСТ Р 51241—2008

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

Содержание



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р
51241—
2008

СРЕДСТВА И СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Классификация. Общие технические требования. Методы испытаний

Издание официальное

| | |
|--|----|
| 1 Область применения | 1 |
| 2 Нормативные ссылки | 1 |
| 3 Термины и определения | 3 |
| 4 Классификация | 5 |
| 4.1 Классификация средств КУД | 5 |
| 4.2 Классификация СКУД | 6 |
| 4.3 Классификация средств и систем КУД по устойчивости к НСД | 6 |
| 4.4 Условные обозначения средств и систем КУД | 7 |
| 5 Технические требования | 9 |
| 5.1 Общие положения | 9 |
| 5.2 Требования к функциональным характеристикам средств КУД | 9 |
| 5.2.1 Требования к функциональным характеристикам УПУ и УИ | 9 |
| 5.2.2 Требования к функциональным характеристикам ИД и УС | 10 |
| 5.2.3 Требования к функциональным характеристикам СУ | 11 |
| 5.3 Требования к функциональным характеристикам СКУД | 12 |
| 5.4 Требования к электромагнитной совместимости | 15 |
| 5.5 Требования к устойчивости средств и систем КУД к НСД | 15 |
| 5.6 Требования к надежности | 16 |
| 5.7 Требования устойчивости к внешним воздействующим факторам | 16 |
| 5.8 Требования к электропитанию | 16 |
| 5.9 Требования безопасности | 17 |
| 5.10 Требования к конструкции | 18 |
| 5.11 Требования к маркировке | 18 |
| 6 Методы испытаний | 18 |
| 6.1 Общие положения | 18 |
| 6.2 Испытания на соответствие средств и систем КУД техническим требованиям | 18 |
| Приложение А (обязательное) Автоматизированные системы. Классификация автоматизированных систем и требований по защите информации | 20 |
| Приложение Б (обязательное) Средства вычислительной техники (СВТ). Показатели защищенности от НСД к информации по классам защищенности | 24 |
| Библиография | 28 |

БЗ 11—2008/380



Месяц
Стандартизации
2008

Биометрические стандарты (международные, принятые в России в качестве национальных)

| | |
|-----------------------------|--|
| ГОСТ Р ИСО/МЭК 19794-1-2008 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 1. Структура |
| ГОСТ Р ИСО/МЭК 19794-2-2005 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца - контрольные точки |
| ГОСТ Р ИСО/МЭК 19794-4-2006 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца |
| ГОСТ Р ИСО/МЭК 19794-5-2006 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица |
| ГОСТ Р ИСО/МЭК 19794-6-2006 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза |
| ГОСТ Р ИСО/МЭК 19794-7-2009 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи |
| ГОСТ Р ИСО/МЭК 19794-9-2009 | Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 9. Данные изображения |

Основные термины и определения (ГОСТ Р 51241-2008)

Контроль и управление доступом (КУД) - комплекс мероприятий, направленных на ограничение и санкционирование доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

Средства контроля и управления доступом (средства КУД) - механические, электромеханические, электрические, электронные устройства, конструкции и программные средства, обеспечивающие реализацию контроля и управления доступом.

Система контроля и управления доступом (СКУД) - совокупность средств контроля и управления, обладающих технической, информационной, программной и эксплуатационной совместимостью.

Идентификация - процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку. Под идентификацией понимается также присвоение субъектам и объектам доступа идентификатора и(или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

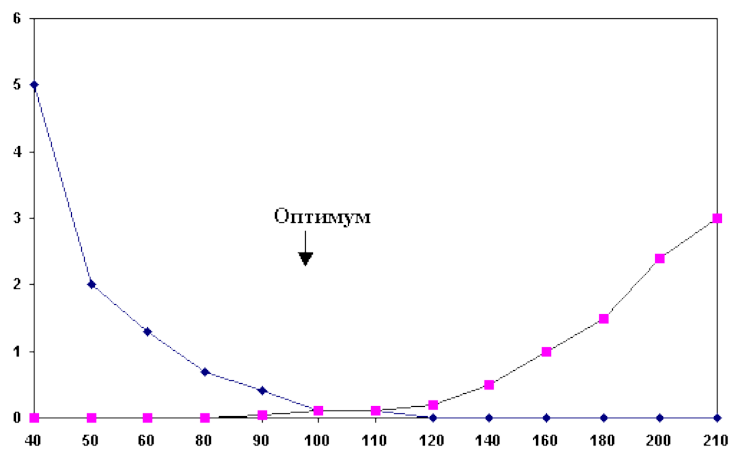
Аутентификация - процесс опознавания субъекта или объекта путем сравнения введенных идентификационных данных с эталоном (образом), хранящимся в памяти системы для данного субъекта или объекта.

Биометрическая идентификация - Идентификация, основанная на использовании индивидуальных физических признаков человека.

Точка доступа - место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные считывателем, исполнительным механизмом, электромеханическим замком и другими необходимыми средствами).

Биометрические технологии в СКУД

- ❑ отпечатки пальцев
- ❑ узор кровеносных сосудов сетчатки глаза,
- ❑ геометрия кисти,
- ❑ изображение лица,
- ❑ динамика подписи,
- ❑ голосовые характеристики
- ❑ другие технологии ...



Зависимость вероятности ошибки в процентах от уровня чувствительности анализатора

Вероятностный характер распознавания – наличие ошибок.

Современные системы обеспечивают:

Ошибка второго рода «ложный допуск»:

FAR (False Acceptable Rate):
 $10^{-6} - 10^{-9}$

Ошибка первого рода «ложный отказ»:

FRR (False Rejection Rate) :
0,5 - 4%.

Скорость распознавания – единицы секунд.

Преимущества биометрии в СКУД

❑ ПОВЫШЕНИЕ БЕЗОПАСНОСТИ

Биометрическая идентификация обеспечивает более высокий уровень безопасности, чем другие решения, такие как пароли, ПИН-коды, электронные карты, электронные ключи.

❑ ЭКОНОМИЯ СРЕДСТВ

Биометрические решения позволяют сократить человеческие и финансовые затраты (на 60-90%), связанные с поддержанием вещественных идентификаторов (карт, ключей), администрированием парольной системы.

❑ УДОБСТВО ИСПОЛЬЗОВАНИЯ

Пользователю не придется помнить пароли или носить с собой карты или электронные ключи.

Основные сферы применения биометрических технологий

СФЕРЫ ПРИМЕНЕНИЯ

Защита конфиденциальной информации

- Корпоративные сети
- Медицина
- Финансовый сектор
- Системы баз данных
- Интеллектуальная собственность
- Кассовые терминалы

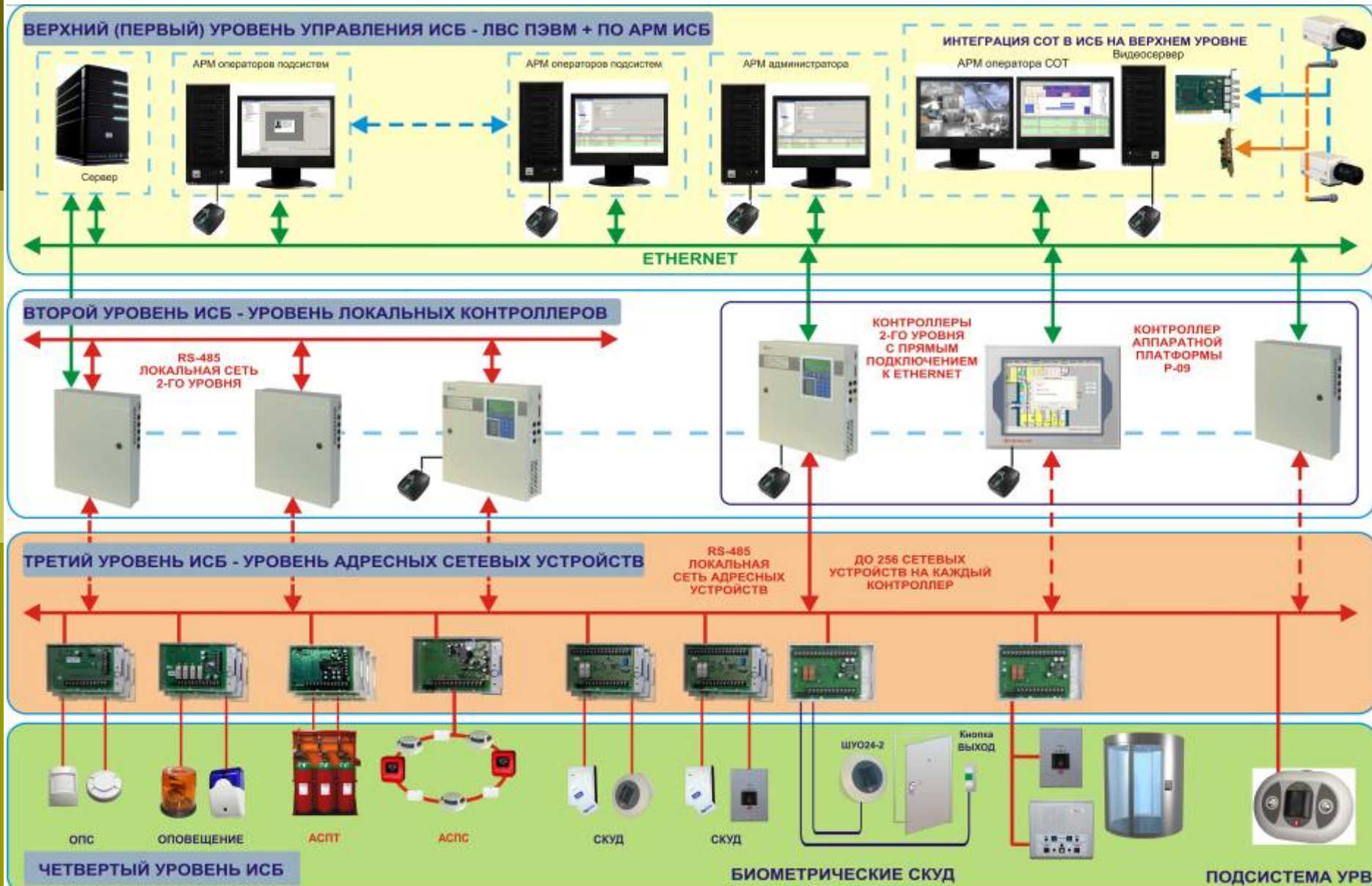
Физический контроль доступа

- Контроль доступа на периметрах объектов (проходные, КПП)
- Контроль доступа в помещения охраняемых объектов.
- СКУД в составе ИСБ и АСУ ФЖБ
- Учет и контроль рабочего времени
- Биометрические замки

Гражданская идентификация

- Системы голосования
- Водительские права
- Удостоверения личности
- Паспорт
- Пограничный контроль
- Таможенный контроль
- Полицейские системы
- Идентификация личности

Биометрические технологии в ИСБ «Рубеж»



Биометрические технологии в ИСБ «Рубеж»

- ❑ Биометрический контроль и разграничение доступа к информационным ресурсам верхнего уровня управления ИСБ (ЛВС ПО АРМ RM-3)
- ❑ Доступ к управлению на уровне аппаратных контроллеров (защита от НСД контроллеров второго уровня)
- ❑ Биометрический контроль управлением подсистемой охранной сигнализации
- ❑ Биометрические считыватели СКУД – возможность работы в качестве сетевых устройств ИСБ «Рубеж» и универсальный интерфейс Wigand26.
- ❑ Биометрическая подсистема учета рабочего времени (УРВ) – интеграция в ИСБ на верхнем уровне ПО АРМ и возможность автономной работы
- ❑ Автономная биометрическая система для управления электорозамком с возможностью интеграции с ПО RM-3 на уровне контроля работоспособности и ведения протокола событий.

Биометрический считыватель BioSense



- q Два типа сканера: **тепловой и емкостный**
- q Два режима работы: автономный контроллер доступа, считыватель с интерфейсом **Wiegand26**
- q Встроенная база данных на **9000** отпечатков пальцев
- q Задание до **10** отпечатков для каждого пользователя
- q Возможность подключения внешнего считывателя проксимити-карт для идентификации **по двум признакам**
- q Подключение по цифровой линии интеллектуального блока оборудования двери БОД-01 для работы в **автономном режиме**

Подключение биометрических считывателей BioSense

Работа в составе ИСБ "Рубеж"



Автономный режим работы

"Горячее" подключение компьютера для конфигурирования точки доступа

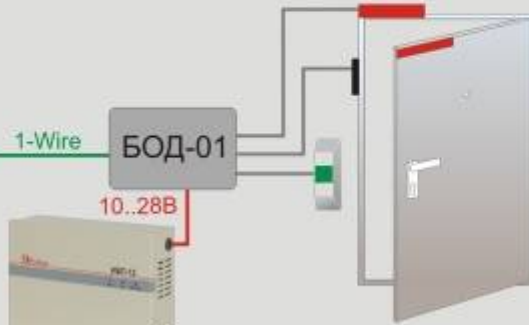


USB

Оptionальное подключение внешнего проксимитив-считывателя для прохода по двум признакам карта + отпечаток



Wiegand26



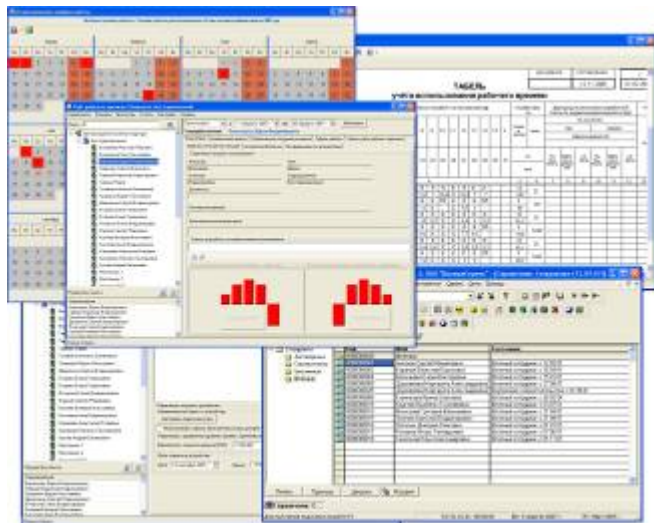
1-Wire

БОД-01

10..28В

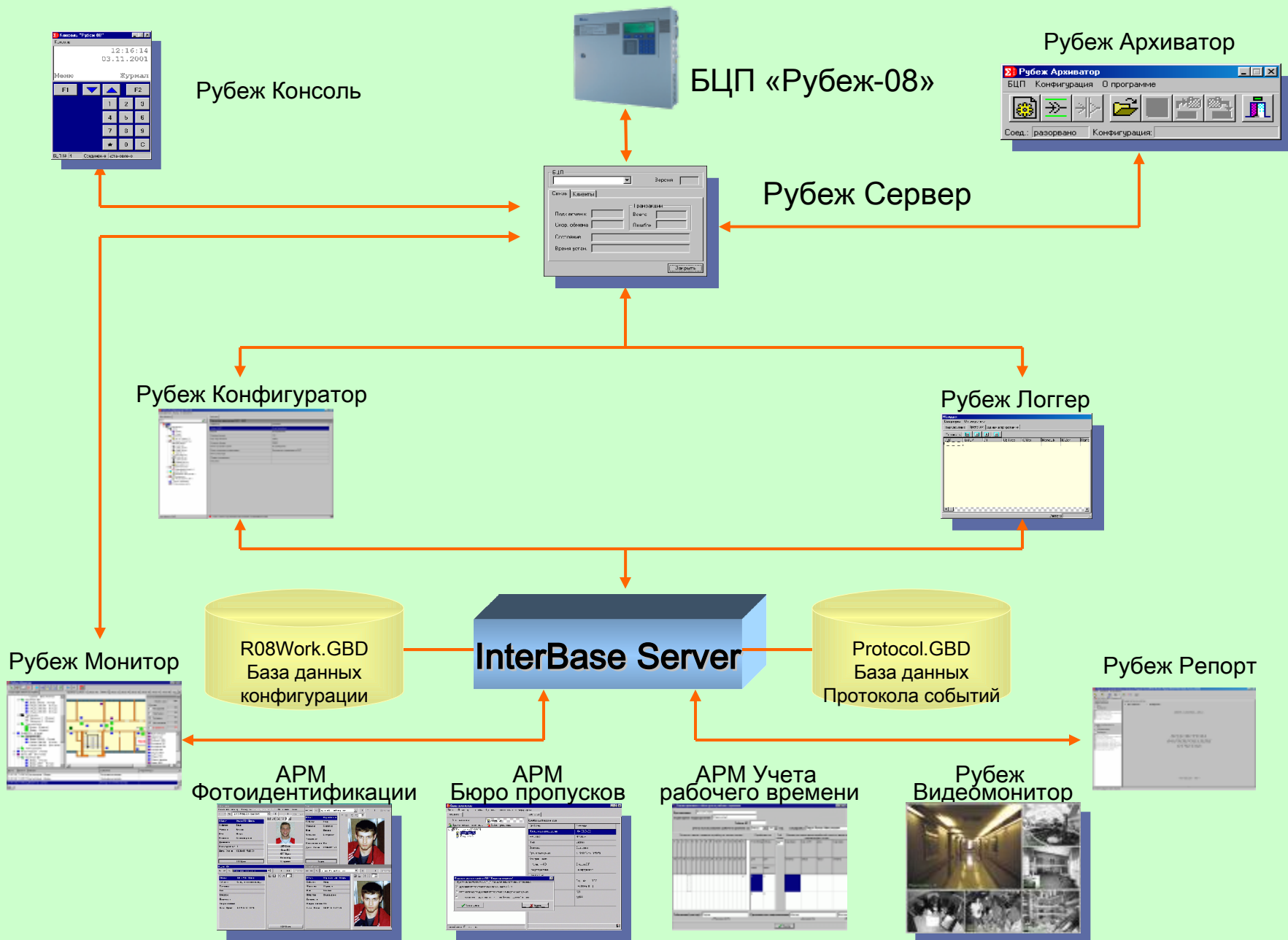
ИБП-12

Биометрическая система учета рабочего времени BioSense Time



- q Использование биометрического считывателя отпечатков пальцев в качестве устройства регистрации
- q Невозможность регистрации за другого человека
- q Формирование как типовых графиков работы (пятидневка, шестидневка), так и сменных, с возможными суточными переходами времени
- q Подсчет отработанного времени, опозданий, прогулов, болезней, досрочных уходов с работы
- q Учет командировок, отпусков, больничных
- q Табель отработанного сотрудниками времени по форме Т-13
- q Экспорт данных об отработанном времени в 1С Предприятие для расчета заработной платы
- q Подключение считывателя к компьютеру через RS-232, RS-485, Ethernet, USB

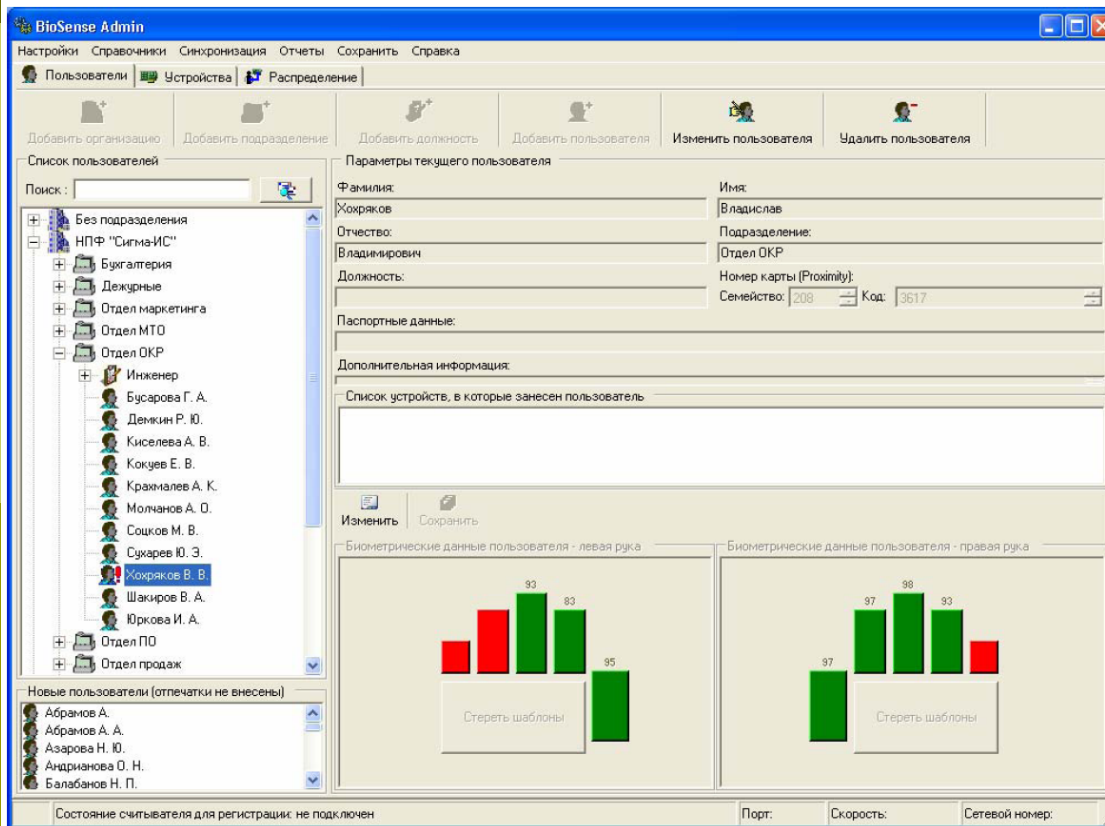
Программное обеспечение ИСБ «ПО Рубеж-08»



Программное обеспечение BioSense Admin

Назначение

Программа предназначена для организации СКУД на базе биометрических считывателей BioSense. Программа позволяет вести список устройств BioSense и пользователей СКУД, а также проводить распределение и загрузку учетных записей пользователей по устройствам. Дополнительно программа позволяет сформировать отчеты о конфигурации СКУД.



Позволяет:

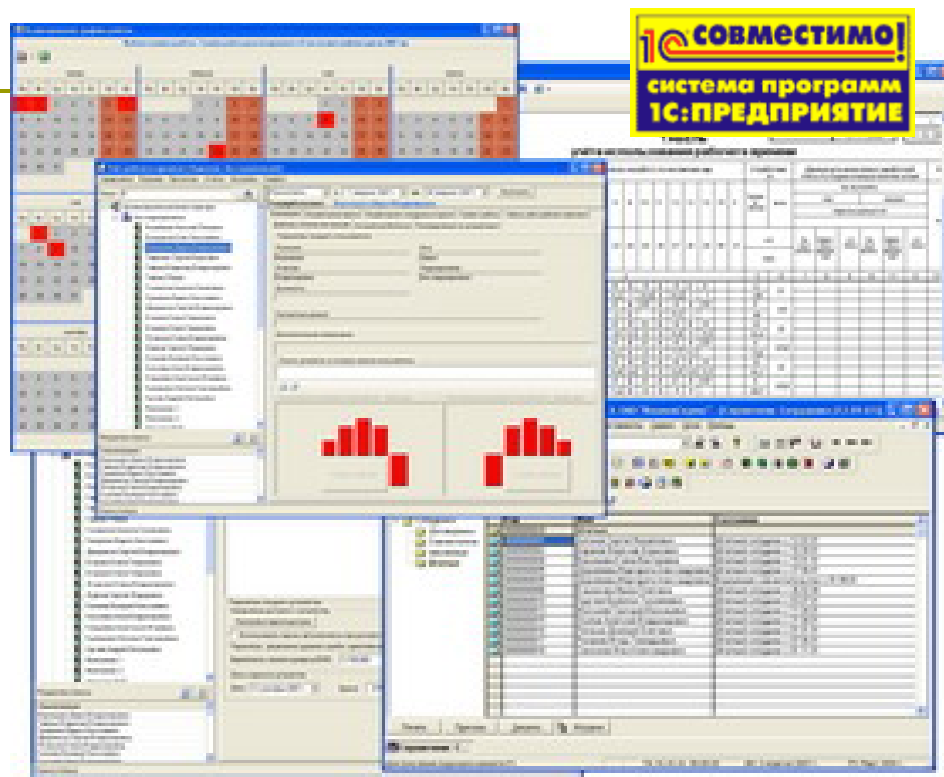
- Предоставление доступа к функциям BioSense программному обеспечению сторонних разработчиков.
- Составление организационноштатной структуры предприятия;
- Запись шаблонов отпечатков пальцев пользователей в базу;
- Создание / изменение / удаления устройств;
- Задание пароля на доступ к устройству;
- Распределение пользователей и их отпечатков пальцев по устройствам;
- Синхронизация с базой данных программного обеспечения Рубеж-08;
- Формирование отчетов по базе данных BioSense Admin

Программное обеспечение BioSense Time

Использование биометрического считывателя отпечатков пальцев в качестве устройства

регистрации.

- ❑· Невозможность регистрации за другого человека.
- ❑· Формирование как типовых графиков работы (пятидневка, шестидневка), так и сменных, с возможными суточными переходами времени.
- ❑· Подсчет отработанного времени, опозданий, прогулов, болезней, досрочных уходов с работы.
- ❑· Учет командировок, отпусков, больничных.
- Табель отработанного сотрудниками времени по форме Т-13.
- ❑· Импорт данных о пользователях из других программ.
- ❑· Экспорт данных об отработанном времени в 1С Предприятие для расчета заработной платы.
- ❑· Подключение считывателя к компьютеру через RS-232, RS-485, Ethernet, USB.



Работа с 1С:Предприятие

Взаимодействие программного обеспечения с платформой 1С:Предприятие осуществляется с помощью COM-объектов. В ходе взаимодействия осуществляется экспорт следующих данных в систему 1С:Предприятие:

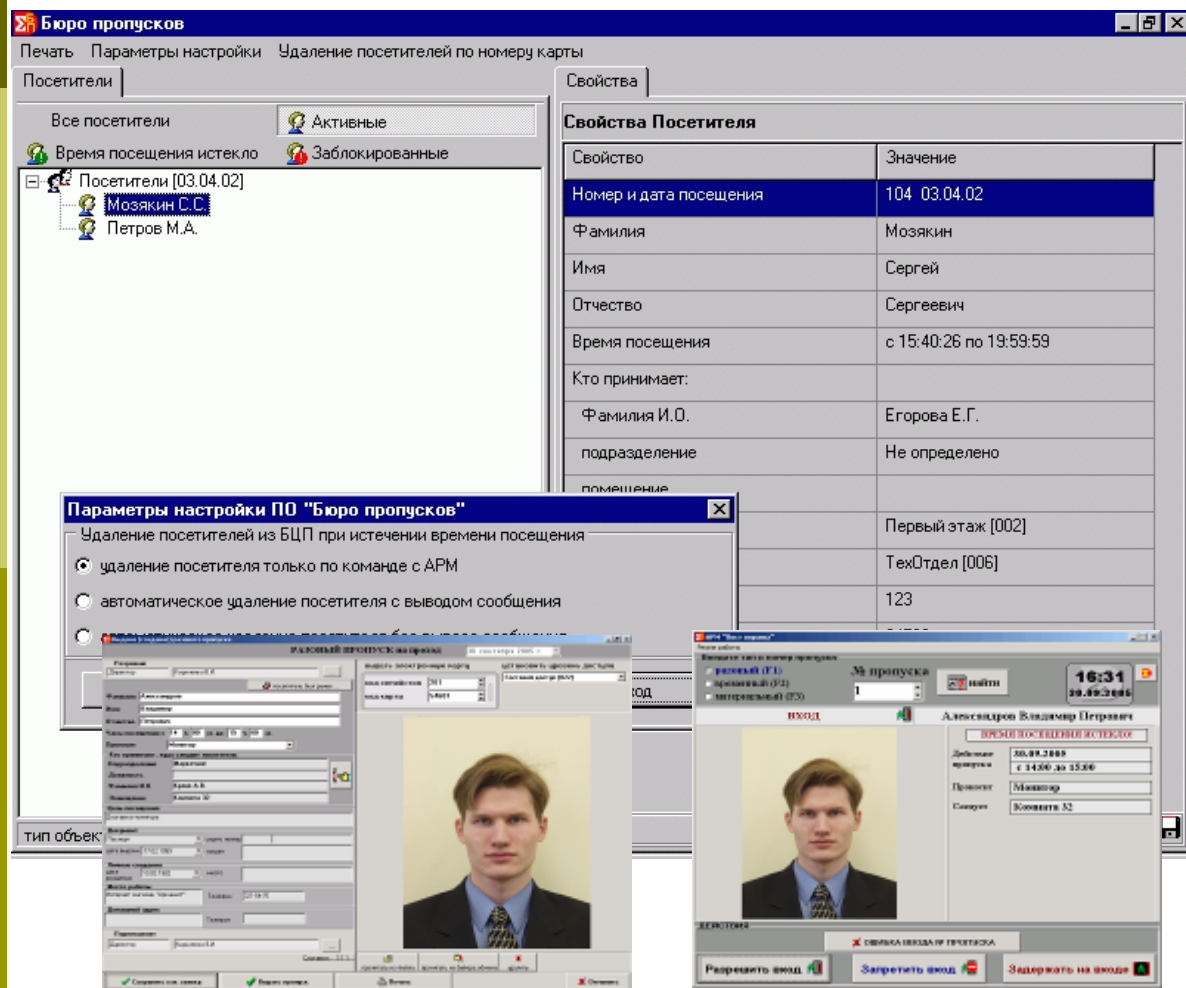
- отработанное сотрудниками время (табель учета рабочего времени, форма Т-13);
- данные о командировках сотрудников;
- данные о прогулах, больничных, отпусках и других отклонениях от графиков работы сотрудников.

В дальнейшем эти данные могут использоваться в 1С:Предприятие для проведения расчетов заработной платы сотрудников.

Модуль обмена данными с системой 1С: Предприятие имеет сертификат "Совместимо! Система программ 1С:Предприятие". Дополнительная информация

АРМ Бюро пропусков

АРМ «Бюро пропусков» – программный модуль, предназначенный для обеспечения работы сотрудников бюро пропусков по организации выдачи и сдаче разовых, временных, материальных пропусков формирования отчетов по базе данных событий в системе безопасности.



АРМ Бюро пропусков предназначен для организации выдачи пропусков посетителям.

Основные возможности:

- Ввод данных посетителей
- Выдача временных пропусков посетителям для прохода на объект
- Блокирование пропуска посетителя при превышении времени посещения
- Формирование отчетов по посещениям

АРМ Фотоидентификации

АРМ «Фотоидентификация» – программный модуль, предназначенный для проведения оператором визуальной идентификации пользователей системы безопасности, а также для пропуска их через точки доступа.

The screenshot displays two windows of the ARМ Photo Identification software. The top window, titled 'ПО и Офис', shows a photo of a man in a red jacket and a table with the following data:

| Объект | Отдел ПО : Дверь |
|---------------|-------------------|
| Событие | Вход |
| Фамилия | Князев |
| Имя | Игорь |
| Отчество | Александрович |
| Должность | |
| Подразделение | -1 |
| Дата - Время | 03.04.02 15:20:33 |

The bottom window, titled 'Отдел ОКР', shows the same photo and a table with the following data:

| Объект | Офис 205 : Дверь |
|---------------|------------------------|
| Событие | Выход по кнопке выхода |
| Фамилия | |
| Имя | |
| Отчество | |
| Должность | |
| Подразделение | |
| Дата - Время | 03.04.02 17:10:45 |

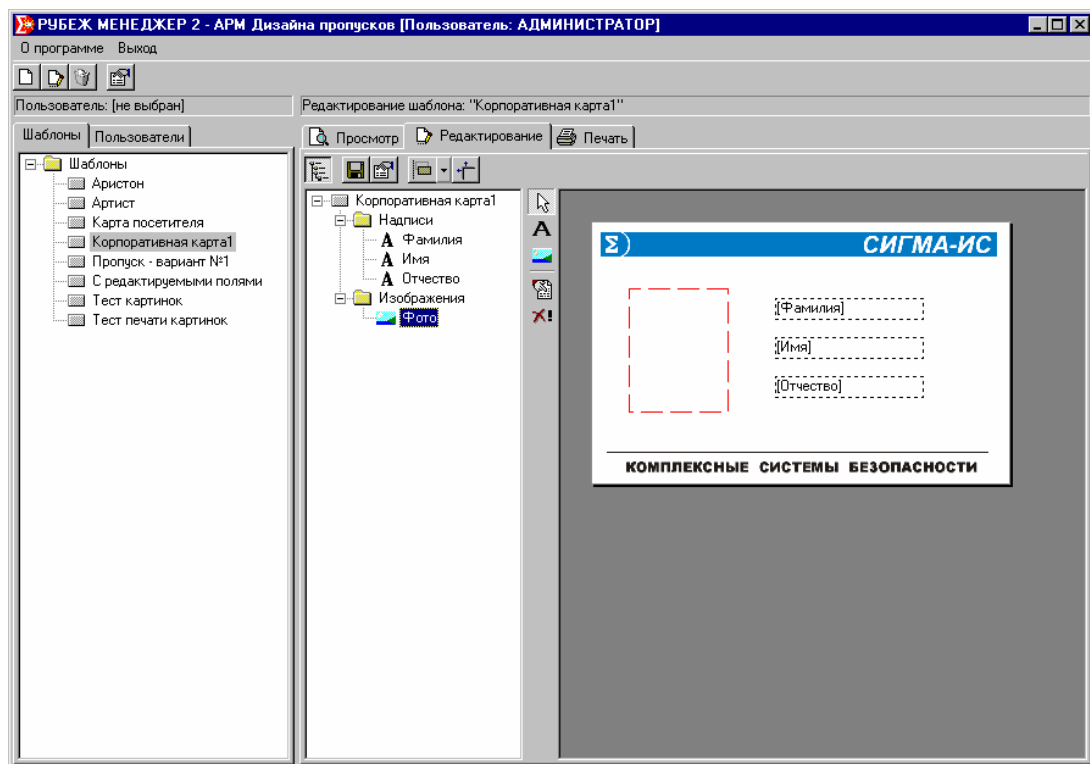
АРМ «Фотоидентификация» позволяет:

- проводить визуальную фотоидентификацию физических лиц, осуществляющих какие-либо действия в Системе Безопасности (вход, постановка на охрану и т.п.);
- управлять проходом физических лиц через точки доступа Системы Безопасности;
- хранить в буфере информацию о заданном количестве объектов идентификации.

АРМ Дизайн пропусков

Назначение

Создание и редактирование шаблонов пропусков и печати пропусков на пластиковых картах или наклейках (размера 54 x 86 мм) с использованием термопринтера или на обычных бумажных носителях с использованием стандартных средств печати. Основной задачей данного приложения является автоматическая подстановка значений полей БД в текстовые и графические поля пропуска. Разработка дизайна карты предполагается во внешнем графическом редакторе с дальнейшим размещением созданного образа карты на шаблоне пропуска в виде подложки.



Основные возможности

- ❑ Создание шаблонов пропусков с использованием в качестве подложки графических изображений формата jpeg и bmp
- ❑ Задание полей подложки (отступы от краев пластиковой карты)
- ❑ Размещение на шаблонах текстовых и графических компонентов с возможностью привязки их к полям БД
- ❑ Создание редактируемых непосредственно перед печатью текстовых полей
- ❑ Печать пропуска на основе выбранного шаблона и пользователя

АРМ «Учет рабочего времени PRO»

Назначение.

Предназначен для автоматизации пропускного режима предприятий (организаций) любого типа, как в части изготовления, выдачи и регистрации пропусков, так и в части автоматизации всего процесса доступа и контроля порядка посещения объекта.

В состав данного комплекса входят:

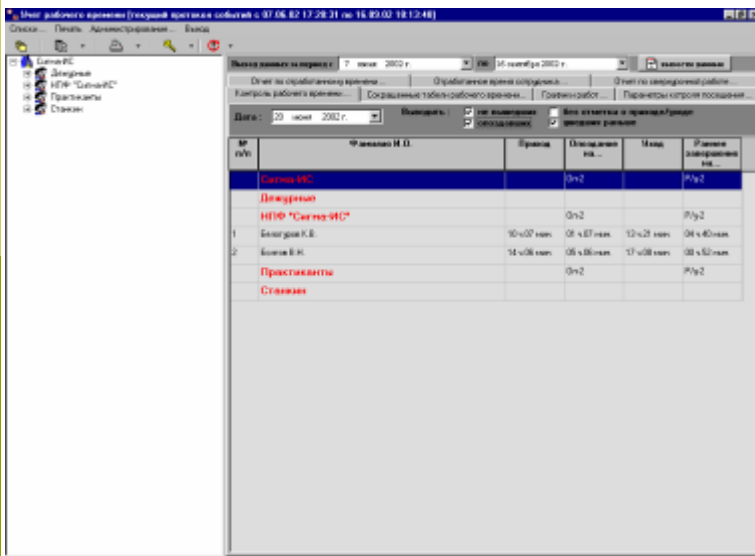
- Конфигуратор системы.
- АРМ ведения постоянных пропусков.
- АРМ Терминал заявок.
- АРМ Бюро пропусков.
- АРМ Пост охраны.
- Подсистема ведения отчетов.

Позволяет:

Осуществлять запросы к базе данных протокола событий по рабочему времени пользователей, в т.ч.:
рабочему (текущему) протоколу событий - при загрузке ПО

сохраненному протоколу событий - по запросу оператора
Формировать рабочие графики, в т.ч.:

- шаблоны рабочих графиков
- персональные рабочие графики сотрудников на весь рабочий год, с возможностью установки индивидуального режима работы каждого дня года
- рабочие графики сотрудников «недельного» режима работы
- рабочие графики сотрудников «сменного» режима работы
- производить перенос рабочих (выходных) дней с автоматической корректировкой графика работы
- копировать (изменять) рабочие графики группам сотрудников
- производить автоматический контроль соответствия изменений в графиках работ - произведенным расчетам рабочего времени сотрудников



Интеграционная программная платформа ИСБ «RM-3»

- ❑ **RM-3** – распределённая интеграционная программная среда, предназначенная для построения **единого верхнего уровня различных технологических систем** (пожарных, охранных, жизнеобеспечения, «интеллектуальных зданий» и т.д.).
- ❑ **RM-3** позволяет создавать **масштабируемые системы**, предоставляя средства для унифицированного **взаимодействия разнородного оборудования и программного обеспечения**, а также **единый пользовательский и программный интерфейс**.

