

Министерство образования и науки Российской Федерации
Национальный исследовательский ядерный университет «МИФИ»

А.В. Бадиков, П.В. Бондарев

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Лабораторный практикум

*Рекомендовано УМО «Ядерные физика и технологии»
в качестве учебного пособия
для студентов высших учебных заведений*

Москва 2010

УДК 654.923.1(076.5)

ББК 32.811.7я7

Б15

Бадиков А.В., Бондарев П.В. **Системы контроля и управления доступом.** Лабораторный практикум. – М.: НИЯУ МИФИ, 2010. – 128 с.

В лабораторном практикуме представлены четыре лабораторные работы. Две из них посвящены изучению контроллеров систем контроля и управления доступом и их сетей, одна лабораторная работа – по изучению устройств биометрической идентификации, и одна лабораторная работа – по созданию автоматизированной точки доступа (автоматизация работы турникета). В описаниях лабораторных работ определены цели лабораторных исследований, даны описания объектов лабораторных исследований, определён порядок выполнения лабораторных работ и сформулированы вопросы для контроля знаний.

Лабораторный практикум предназначен для студентов, специализирующихся в области физической защиты объектов, в рамках подготовки инженеров по специальностям 140309 «Безопасность и нераспространение ядерных материалов» и 090104 «Комплексное обеспечение информационной безопасности автоматизированных систем», а также магистров направления 553126 «Техническая физика».

Подготовлено в рамках Программы создания и развития НИЯУ МИФИ.

Рецензент канд. физ.-мат. наук, доцент *В.В. Болятко*

ISBN 978-5-7262-1261-6

© Национальный исследовательский ядерный университет «МИФИ», 2010

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ.....	5
ПРЕДИСЛОВИЕ	5
Лабораторная работа № 1. Изучение возможностей контроллера СКУД PXL-500W компании KERI SYSTEMS	8
1.1 Описание объекта лабораторного исследования	8
1.2 Порядок выполнения работы	13
1.3 Контрольные вопросы	15
Список литературы	15
Приложение А. Подключение контроллера PXL-500W.....	16
Приложение Б. Порядок работы с ПО «DOORS».....	19
Лабораторная работа № 2. Изучение возможностей построения распределённой СКУД на основе оборудования компании KERI SYSTEMS.....	45
2.1 Описание объекта лабораторного исследования	45
2.2 Порядок выполнения работы	48
2.3 Контрольные вопросы	49
Список литературы	49
Приложение В. Подключение контроллера PXL-250.....	49
Приложение Г. Подключение платы расширения SB-293	52
Лабораторная работа № 3. Устройства биометрической идентификации.....	56
Введение	56
3.1 Описание объекта лабораторного исследования	63
3.2 Порядок выполнения работы	76
3.3 Контрольные вопросы	77
Список литературы	78
Приложение Д. Описание работы с программным обеспечением администратора BM-ES300AE для IRIS CAMERA BM-ET 300 AE фирмы PANASONIC	79
Приложение Е. Описание работы с программным обеспечением HANDNET FOR WINDOWS VERSION 2.0.0.23 фирмы RECOGNITION SYSTEMS	89

Приложение Ж. Описание работы с программным обеспечением FINGERLAN 4.6 фирмы IDENTIX.....	100
Лабораторная работа № 4. Создание модели системы контроля и управления точкой доступа.....	106
4.1 Описание объекта лабораторного исследования	106
4.2 Порядок выполнения работы	121
4.3 Контрольные вопросы	121
Список литературы	121
Приложение 3. Основные возможности СКУД «ФОРПОСТ» с программным обеспечением «ФОРПОСТ-СТАНДАРТ»	122

СПИСОК СОКРАЩЕНИЙ

АРМ	– автоматизированное рабочее место
БД	– база данных
ЗПП	– запрет повторного прохода
КУД	– контроль и управление доступом
ЛВС	– локальная вычислительная сеть
НЗ	– нормально-замкнутый
НО	– нормально-открытый
ОС	– операционная система
ПК	– персональный компьютер
ПО	– программное обеспечение
РИП	– резервный источник питания
СКУД	– система контроля и управления доступом
СФЗ	– система физической защиты
УБИ	– устройство биометрической идентификации

ПРЕДИСЛОВИЕ

Данное издание является продолжением цикла лабораторных практикумов по системам физической защиты объектов.

Лабораторные работы посвящены изучению возможностей и методов применения систем контроля и управления доступом (СКУД). Представленные материалы не являются исчерпывающими по данной тематике, но позволяют студентам понять и изучить основополагающие функции элементов СКУД и особенности построения и использования таких систем.

Практикум состоит из четырёх лабораторных работ:

1. Изучение возможностей контроллера СКУД PXL-500W компании Keri Systems. (подготовил Бадиков А.В.)
2. Изучение возможностей построения распределённой СКУД на основе оборудования компании Keri Systems (Бадиков А.В.).
3. Устройства биометрической идентификации (Бондарев П.В.).
4. Создание модели системы контроля и управления точкой доступа (Бондарев П.В.).

Первые две лабораторные работы посвящены изучению контроллеров СКУД. Цель этих работ – показать студентам основные функции, выполняемые такими контроллерами, а также возможности построения распределённых систем КУД, то есть таких систем, где несколько контроллеров объединены в одну сеть и могут управляться с одного автоматизированного рабочего места (АРМ).

Третья работа направлена на изучение устройств биометрической идентификации (УБИ), работающих по различным признакам человека: по рисунку радужной оболочки глаза, по форме кисти руки, по отпечатку пальца. Цель данной работы – дать студентам практические навыки по настройке и использованию таких устройств.

Четвертая работа посвящена созданию автоматизированной точки доступа – автоматизация работы турникета.

Список необходимых для выполнения лабораторных работ программно-технических средств приводится в описании каждой лабораторной работы. Предполагается, что лабораторные стенды будут в основном собраны, а студенты, выполняющие лабораторную

работу, будут производить только некоторые подключения, наличие которых будет важным для выполнения данной работы.

Данный лабораторный практикум является развитием методологического обеспечения подготовки специалистов по специальностям «Безопасность и нераспространение ядерных материалов» и «Комплексное обеспечение информационной безопасности автоматизированных систем», а также магистерской образовательной программы «Учёт, контроль и физическая защита ядерных материалов».

Данному курсу лабораторных работ должно предшествовать изучение дисциплин, посвящённых системам физической защиты (СФЗ): «Инженерно-технические средства физической защиты» либо «Технические средства защиты объектов».

Основными документами для подготовки лабораторных работ являлись руководства по установке и программированию производителей оборудования.

Лабораторная работа № 1

ИЗУЧЕНИЕ ВОЗМОЖНОСТЕЙ КОНТРОЛЛЕРА СКУД PXL-500W КОМПАНИИ KERI SYSTEMS

Цель работы:

- 1) Изучение основных возможностей, предоставляемых современными контроллерами системы контроля и управления доступом.
- 2) Приобретение практических навыков работы с контроллерами на примере PXL-500W производства компании Keri Systems, США.

1.1 Описание объекта лабораторного исследования

В данном разделе описывается оборудование, используемое для выполнения лабораторной работы, и основные возможности этого оборудования.

1.1.1 Назначение СКУД

Система контроля и управления доступом – неотъемлемая часть системы физической защиты объекта. Основная задача системы контроля доступа – разрешить проход уполномоченным субъектам (сотрудникам, посетителям) и запретить проход всем остальным [1].

СКУД стали неотъемлемой частью комплекса безопасности современного предприятия, они успешно решают задачи по контролю, учету рабочего времени и управлению перемещением персонала.

Существующий ГОСТ Р 51241–98 «Средства и системы контроля и управления доступом» [2], который устанавливает классификацию, общие технические требования и методы испытаний, подразделяет СКУД по:

- способу управления;
- количеству контролируемых точек доступа;
- функциональным характеристикам;
- виду объектов контроля;

- уровню защищенности системы от несанкционированного доступа.

По способу управления СКУД могут быть автономными, сетевыми и универсальными. Автономные системы как класс не актуальны для крупных объектов. Централизованные (сетевые) СКУД обеспечивают возможность оперативного контроля и управления исполнительными устройствами СКУД со стороны оператора (операторов) и осуществляют обмен информацией с центральным пультом, в качестве которого обычно выступает персональный компьютер. Термин "универсальные" введен ГОСТом для сетевых систем, способных переходить в режим автономной работы при возникновении отказов управляющих компьютеров, сетевого оборудования или обрыве связи с контроллером СКУД. Большинство существующих сетевых систем выполняют эту функцию (которая фактически стала базовой), и их можно назвать универсальными. Тем не менее, данный термин «не прижился» и далее при рассмотрении сетевых систем будут подразумеваться универсальные.

Контроллер PXL-500W является сетевым (универсальным), но возможности и особенности его использования в сети контроллеров будут изучаться в лабораторной работе № 2 «Изучение возможностей построения распределённой СКУД на основе оборудования компании Keri Systems». В данной работе внимание будет уделено знакомству с контроллерами СКУД компании Keri Systems, изучению их возможностей при автономном функционировании, режимов работы, установки и программирования.

1.1.2 Состав лабораторного стенда

При выполнении лабораторной работы используется следующее оборудование:

- контроллер PXL –500W;
- 2 считывателя карт доступа с клавиатурой P-600H;
- персональный компьютер с установленной ОС Windows XP, имеющий COM-порт;
- монитор;
- программное обеспечение СКУД «Doors».

Также использовалось вспомогательное оборудование:

- бесконтактные карты доступа;
- блок бесперебойного питания 12 В постоянного тока;
- имитатор кнопки запроса на выход;
- имитатор датчика открытия двери;
- соединительные провода.

Схема соединения используемого в данной лабораторной работе оборудования показана на рис. 1.1.

Ниже приводится краткое описание используемого оборудования.

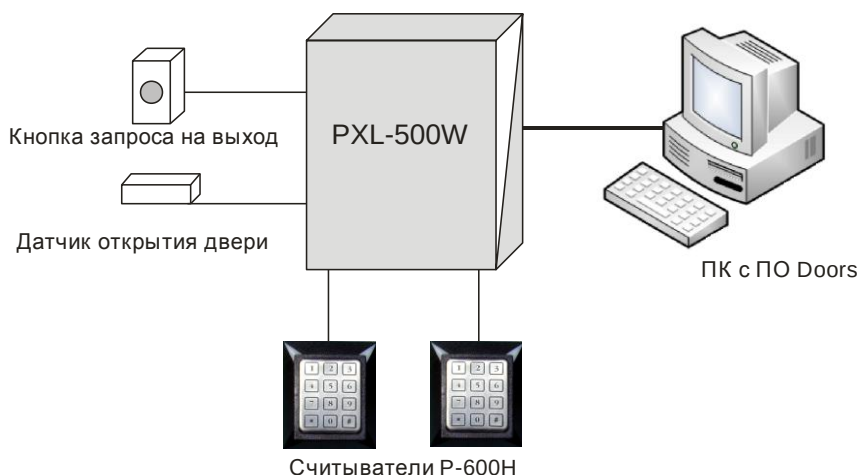


Рис. 1.1. Схема соединения устройств для изучения возможностей контроллера СКУД PXL-500W

1.1.3 Контроллер PXL-500W

Цифровой контроллер PXL-500W американской компании Keri Systems является одним из основных элементов системы контроля доступа этой компании. Контроллер получает информацию от считывателей карт доступа и автономно управляет работой различных исполнительных и управляемых преграждающих устройств системы, таких как электромеханические замки, автоматические шлагбаумы, турникеты и др. Именно контроллер принимает решение,

например, об открытии дверей, если сотруднику разрешен доступ на данную охраняемую территорию, и блокировании замка, если доступ запрещен. При необходимости контроллеры объединяют в единую систему. Число контроллеров в одной сети RS-485 ограничено 128. Однако число таких сетей, каждая из которых отдельно подключается к ПК, ограничено возможностями этого ПК (в частности, количеством доступных COM-портов).

В качестве вычислительного ядра в контроллере PXL-500W используется процессор с RISC-архитектурой. PXL-500W запоминает до 3600 событий (таких как проход пользователя, отказ в доступе, взлом двери и др.) и хранит эту информацию в энергонезависимой памяти до 5 лет.

Цифровой контроллер PXL-500W содержит необходимые входы/выходы, через которые осуществляется контроль состояния и управление дверью (подключаются датчик положения двери, кнопка выхода, до двух считывателей и исполнительное устройство).

Контроллер PXL-500W при подключении платы расширения SB-593 может управлять двумя дверьми. Плата SB-593 имеет также 6 дополнительных программируемых входов и 2 релейных выходов, которые можно использовать для подключения кнопок выхода, охранных датчиков и исполнительных устройств системы контроля доступа (электромеханических замков, турникетов, автоматических шлагбаумов).

Имеющийся в контроллере последовательный порт RS-232 обеспечивает прямое или модемное подключение PXL-500W к компьютеру, который поддерживает связь с сетью контроллеров. В то же время каждый контроллер этой серии представляет собой автономное устройство.

В контроллере имеется порт RS-485 для его соединения с другими контроллерами. По сети RS-485 могут объединяться в один узел до 128 контроллеров PXL-500W или PXL-250W (они полностью совместимы). Длина линии связи RS-485 может достигать 1200 м.

Контроллер PXL-500W поддерживает подключение любых устройств, поддерживающих передачу информации по протоколу Wiegand – стандартному протоколу для считывателей в СФЗ. На это указывает буква «W» в наименовании модели контроллера.

Схема контроллера PXL-500W приведена в приложении А.

1.1.4 Считыватель с клавиатурой P-600 Н

Считыватель с клавиатурой P-600 Н Rocky (рис. 1.2) серии Ругамid компании Keri Systems устанавливают в системы контроля доступа объектов, к которым предъявляют повышенные требования по безопасности. Считыватель P-600 сочетает в одном устройстве клавиатуру фирмы Essex, выполненную из нержавеющей стали, и считыватель карт доступа серии Ругамid. Такой считыватель с клавиатурой используется, когда требуется как использование карт доступа, так и ввод персонального идентификационного номера (ПИН).



Рис. 1.2. Внешний вид считывателя с клавиатурой P-600 Н

Считыватель имеет следующие основные особенности:

- 1) Выходные данные считывателя с клавиатурой P-600 Н имеют стандартный формат Wiegand, что обеспечивает совместимость с системами контроля доступа большинства производителей. Он может быть сконфигурирован для работы в двух стандартных форматах данных Wiegand, 8 бит Burst и 26 бит Wiegand.
- 2) Для индикации работы считывателя с клавиатурой P-600 Н имеет трехцветный (красный, зеленый и желтый) светодиодный индикатор и зуммер.

- 3) Считыватель с клавиатурой имеет несколько встроенных функций диагностики, включая самопроверку при включении и проверку линии данных.
- 4) Р-600 обеспечивает расстояние считывания до 10 см и работает при напряжении питания от 5 до 14 В постоянного тока, номинальный ток потребления составляет 90 мА. В большинстве случаев считыватель с клавиатурой может быть запитан непосредственно от панели контроля доступа.
- 5) Считыватель является вандалоустойчивым и погодозащищенным, так как блок электроники загерметизирован с помощью эпоксидного наполнителя.

1.1.4 Программное обеспечение «Doors»

С помощью программного обеспечения «Doors» осуществляется настройка и администрирование системы контроля доступа, управление оборудованием, архивирование системной информации, мониторинг параметров системы, управление файлами, содержащими данные о карточках-пропусках, формирование и подготовка различных отчетов. ПО «Doors» работает с операционной системой (ОС) Windows 9x/2000/ME/XP/NT и может обеспечивать доступ к удаленным узлам системы посредством модемного соединения или IP-сети.

Работа программного обеспечения происходит в фоновом режиме, а запуск осуществляется параллельно с другими приложениями. При этом для функционирования системы не требуется, чтобы компьютер постоянно находился на связи с сетью контроллеров. Компьютер необходим только на время начальной загрузки информации в контроллеры системы контроля доступа Keri Systems или мониторинга удаленных объектов.

Подробно работа с программой «Doors» описана в приложении Б.

1.2 Порядок выполнения работы

1. Изучить возможности оборудования по описаниям в данной лабораторной работе.

2. Провести подключение элементов лабораторного стенда в соответствии с рис. 1.1. Схема контроллера PXL-500W приведена в приложении А.

Внимание! Только после проверки подключения преподавателем можно подавать питание на элементы стенда.

3. Провести очистку памяти контроллера. Для этого необходимо до подачи питания на контроллер установить переключку JP10 (см. приложение А), нажать кнопку S1 и, удерживая её нажатой, подать питание на контроллер. Через 10 с снять питание с контроллера, убрать переключку.

4. Установить адрес контроллера в сети RS-485. Для этого надо до подачи питания на контроллер нажать кнопку S1 и, удерживая её нажатой, подать питание на контроллер, после чего отпустить кнопку. На дисплее контроллера будет отображаться текущий его адрес, а также направление его изменения. При однократном нажатии на кнопку S1 он изменяется (увеличивается или уменьшается) на 1, двукратное нажатие на кнопку меняет направление изменения адреса. Поскольку в данной лабораторной работе используется только один контроллер, ему необходимо задать адрес «1».

5. Запустить программу «Doors». Для входа в программу использовать учётную запись «Keri» (пароль «Keri»).

6. Создать учётную запись оператора «lab1» с паролем «lab1». Наделить эту учётную запись правами, необходимыми для выполнения лабораторной работы. Права определяют доступ оператора к различным возможностям программного обеспечения. Необходимый набор прав определить из описания порядка выполнения работы.

Зарегистрироваться в программе под этой учётной записью.

7. Создать учётную запись оператора «sec1» с паролем «sec1». Наделить эту учётную запись правами, необходимыми для работы оператора СКУД. Необходимый набор прав определить исходя из ранее полученных знаний о функциях оператора СКУД.

8. Настроить параметры сети в соответствии с собранной системой.

9. Настроить опции системы, включив следующие возможности программы:

- автоматический переход на летнее время и обратно;

- локальный запрет повторного прохода (ЗПП);
- временные пользователи;
- dual verification (двойная аутентификация).

10. Провести поиск контроллеров в сети. Установить правильное время в контроллере. Настроить свойства контроллера и обслуживаемой им двери.

11. Создать несколько временных интервалов доступа. Создать группу пользователей.

12. Зарегистрировать несколько карт (пользователей), присвоив им созданную группу доступа, одну из карт сделать временной.

13. Проверить работу введенных карт, режим ввода дополнительных карт, различные режимы работы ЗПП.

14. Подготовить отчет о выполненной работе по выданной преподавателем форме и защитить его.

1.3 Контрольные вопросы

1. Варианты классификации СКУД. Универсальные контроллеры.

2. Функции, выполняемые контроллерами СКУД.

3. Основные возможности контроллера PXL-500W.

4. Какие характерные функции СКУД можно реализовать на базе контроллеров PXL-500W и ПО «Doors»?

5. Какие дополнительные возможности даёт установка платы SB-593?

6. Опишите процедуру изменения параметров контроллеров.

7. Какие виды отчетов можно подготовить в ПО «Doors»?

Список литературы

1. Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов. М.: МИФИ, 2008. 584 с.

2. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования.

3. PXL – 500 Tiger Controller Quick Start Guide. Keri Systems.

4. Pyramid Series Reader Quick Reference. Farpointe Data.

5. Doors32 для Windows. Программное обеспечение контроля доступа. Руководство пользователя. Keri Sytems.

Приложение А

ПОДКЛЮЧЕНИЕ КОНТРОЛЛЕРА PXL-500W

На рис. А1 представлена схема контроллера PXL-500W, на которой используемые контактные колодки обозначены прямоугольниками с пронумерованными контактами. Назначение отдельных колодок приведено в табл. А1.

Таблица А1. Назначение контактных колодок контроллера PXL-500W

Обозначение колодки	Назначение
TB1	Подключение к сети контроллеров по протоколу RS-485
TB2	Подключение источника постоянного тока напряжением 12В
TB3	Подключение средств оповещения и исполнительных устройств
TB4	Подключение датчика положения двери и кнопки запроса на выход
TB5	Подключение считывателя № 1
TB6	Подключение считывателя № 2
TB12	Подключение контроллера к ПК или модему по протоколу RS-232

В табл. А2 – А7 описано назначение отдельных контактов в обозначенных колодках.

Таблица А2. Назначение контактов в колодке TB1 (сеть RS-485)

№ контактов	Назначение
1	Отрицательный провод сети RS-485 (TxRx -)
2	Положительный провод сети RS-485 (TxRx +)
3	Экран кабеля

Таблица А3. Назначение контактов в колодке TB2 (питание)

№ контактов	Назначение
1	+12 В
2	Отрицательный провод
3	Заземление

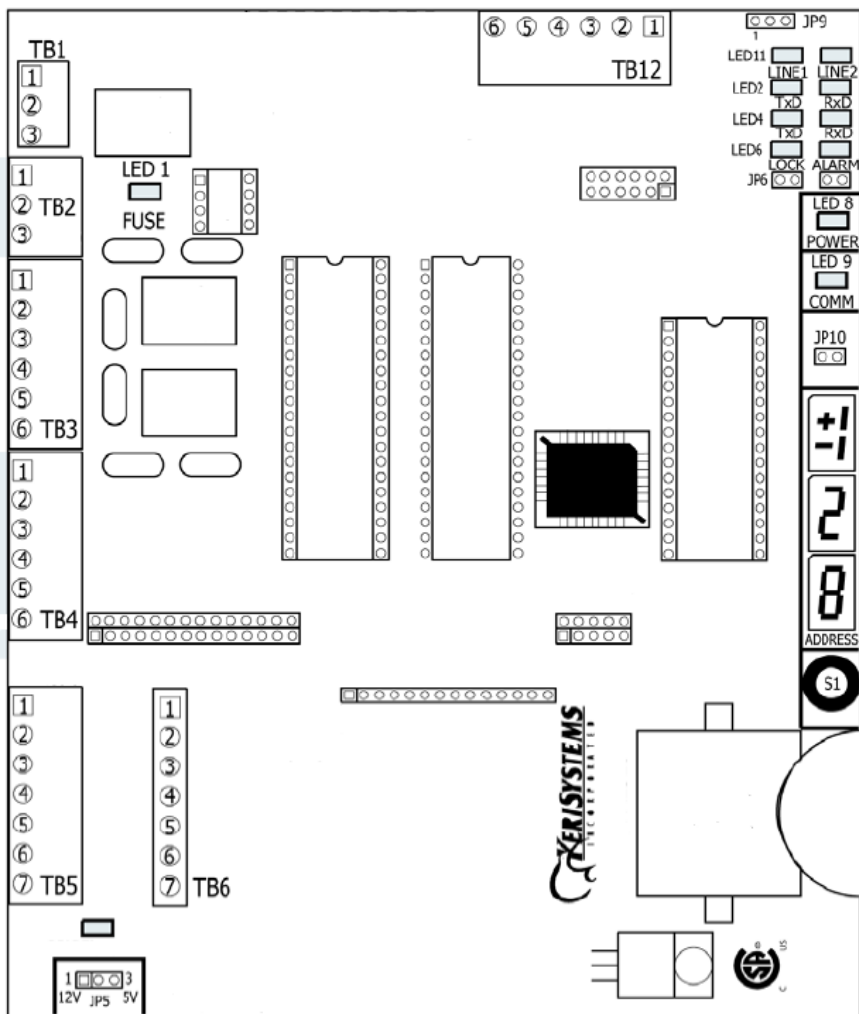


Рис. А1. Схема контроллера PXL-500W

Таблица А4. Назначение контактов в колодке ТВ3 (выходы)

№ контактов	Назначение
1	Замок – НО
2	Замок – общий
3	Замок – НЗ
4	Тревога – НО
5	Тревога – общий
6	Тревога – НЗ

Обозначения: НО – нормально открытый контакт, НЗ – нормально замкнутый контакт.

Таблица А5. Назначение контактов в колодке ТВ4 (входы)

№ контактов	Назначение
1	Датчик положения двери (НЗ)
2	Земля
3	Кнопка запроса на выход (НО)
4	Не используется
5	Земля
6	Кнопка глобальной разблокировки или запроса на выход (НО)

Обозначения: НО – нормально открытый контакт.

Таблица А6. Назначение контактов в колодках ТВ5 и ТВ6 (считыватели) и цвета проводов при подключении считывателей Р-600Н

№ контактов	Назначение	Цвет провода
1	Данные – 0	Зелёный
2	Динамик	Синий
3	Питание	Красный
4	Земля	Чёрный и серебристый
5	Зелёный светодиод	Коричневый
6	Красный светодиод	Оранжевый
7	Данные – 1	Белый

Таблица А7. Назначение контактов в колодке ТВ12 (сеть RS-232)

№ контактов	Назначение	Номер контакта в разъёме DB-9F
1	Передача данных (TxD)	2
2	Приём данных (RxD)	3
3	Не используется	—
4	Не используется	—
5	Не используется	—
6	Земля (GND)	5

Приложение Б

ПОРЯДОК РАБОТЫ С ПО «DOORS»

В данном приложении описан порядок работы с программой «Doors» для совершения действий, входящих в порядок выполнения лабораторных работ. Использование дополнительных возможностей программы, не изучаемых в лабораторных работах № 1 и № 2, здесь не описано, информацию по ним можно найти в [5] и во встроенной справке программы.

Б1. Определение операторов СКУД

Каждый оператор в системе имеет уникальный пароль входа в эту систему, позволяющий авторизовать входящего и отследить его действия во время работы с программой. Команды определения операторов позволяют создать системных операторов и предоставить им права доступа.

В системе может быть максимум 32 оператора. Окно, отображающее операторов системы, открывается при выборе пункта меню «Установки» → «Операторы...» (рис. Б1).

Установки операторов								
	Имя	Пароль	Подтверждение пароля	Установки пользователей	Установки системы	Установки временных зон	Установки групп доступа	Уст мо
1	Keri	****	****	Да	Да	Да	Да	
2	Olga	****	****	Да	Да	Да	Да	
3	User	****	****	Нет	Нет	Да	Да	
4				Нет	Нет	Нет	Нет	

Рис. Б1. Фрагмент окна ПО «Doors» для установки полномочий операторов системы контроля и управления доступом

В зависимости от требований, доступ каждого оператора определяется установкой одного из значений:

- НЕТ – оператор не имеет права управления;
- ДА – оператор имеет право управления;
- ТЧ – оператор имеет право только на чтение, т.е. оператор может читать информацию, но не имеет возможности внести изменения.

Описание различных прав, которые могут быть даны оператору, приведены в табл. Б1.

Таблица Б1. Описание прав операторов

Название	Описание
Установки пользователей	Определяет возможность просмотра и изменения информации о пользователях, в том числе и создания/удаления
Установки системы	Определяет возможность просмотра и изменения информации о системе в целом, а также об отдельных контроллерах и дверях
Установки временных зон	Определяет возможность просмотра и изменения информации о временных зонах
Установки групп доступа	Определяет возможность просмотра и изменения информации о группах доступа
Установки монитора	Определяет возможность просмотра и изменения параметров мониторинга событий
Установки операторов	Определяет возможность просмотра и изменения параметров и прав операторов

Продолжение табл. Б1

Название	Описание
Управление дверьми	Определяет возможность управления дверьми (блокирование и разблокирование)
Управление выходами	Определяет возможность управления релейными выходами платы расширения
Сброс ЗПП	Определяет возможность объявления амнистии по правилам запрета повторного прохода
Запуск монитора	Определяет возможность запуска процесса мониторинга событий
Остановка монитора	Определяет возможность остановки процесса мониторинга событий
Запуск монитора № 1	Определяет возможность открыть окно отображения событий № 1
Запуск монитора № 2	Определяет возможность открыть окно отображения событий № 2
Запуск монитора № 3	Определяет возможность открыть окно отображения событий № 3
Отчёты по событиям	Определяет возможность генерации отчётов по событиям, произошедшим в сети СКУД
Doors отчёты	Определяет возможность генерации отчётов по параметрам программы «Doors»
Launch Backup	Определяет возможность запуска программы, создающей резервную копию баз данных ПО «Doors»
Выход из программы	Определяет возможность корректно завершить выполнение ПО «Doors»
X	Не используется
Y	Определяет возможность просмотра и изменения ПИН-кода пользователей

Б2. Установка параметров системы и проверка сетевого соединения

Для правильной установки параметров системы должны быть выполнены три действия:

- 1) установка параметров сети;
- 2) установка опций системы;
- 3) сохранение параметров системы.

Для изменения конфигурации сети и опций системы необходимо выбрать пункт меню «Установки → Система...» или нажать



кнопку. Откроется окно, содержащее ряд вкладок.

Вкладка «Конфигурация сети»

Для настройки соединения между контроллером СКУД и компьютером необходимо выбрать вкладку «Конфигурация сети» и выбрать тип соединения: через последовательный порт ПК (COM1, COM2, COM3 или COM4) или через локальную сеть (ЛВС) ТСР/IP. Через последовательный порт возможно как прямое соединение ПК с контроллером, так и модемное соединение.

В лабораторных работах используется прямое подключение через порт COM1. Выберите этот порт, все остальные поля ввода надо оставить пустыми.

После ввода всех необходимых параметров надо нажать на



кнопку («Сохранить») для внесения изменений в базу данных программы.

Вкладка «Опции системы»

На вкладке «Опции системы» можно задать ряд параметров, активирующих или деактивирующих определённые возможности СКУД в целом (возможности ПО, контроллеров СКУД, различных устройств расширения).

При выполнении лабораторных работ используются следующие параметры:

«Глобальные сетевые функции» – эти установки применяются ко всем контроллерам сети контроля доступа. В данных лабораторных работах используется пункт «Автоматический переход на летнее время». Данная настройка позволяет контроллерам автоматически переводить время контроллеров в момент перехода на летнее время.

«Локальный запрет повторного прохода (ЗПП)» – по умолчанию функция ЗПП в программе отключена. Для того чтобы разре-

шить ЗПП, эта функция должна быть разрешена в программе и потом настроена для нужных контроллеров и карт/пользователей. Отменить ЗПП можно индивидуально для каждой карты, позволяя таким картам нарушать правила ЗПП. Можно запрограммировать периодическую отмену ЗПП для любого контроллера, отмену ЗПП в определённое время суток или вообще не программировать автоматическую отмену ЗПП (ЗПП может быть отменён оператором для любого пользователя вручную).

«Поиск сотрудников» – включает возможность программы выводить статус пользователя (зону в которой он находится) в реальном времени.

«Временные пользователи» – при включении этой опции появляется возможность заводить пользователей, у которых дата начала действия пропуска в будущем, однако эта возможность сокращает максимальное число пропусков в базе данных с 65535 до 19110 и действует только на контроллерах PXL-500W.

«Dual Verification» – позволяет при наличии комбинированных считывателей-кодонаборников использовать двойную аутентификацию: по карте и по коду.

Сохранение параметров системы. После того, как вся информация была введена и проверена, необходимо сохранить эти настройки в файле конфигурации. Для того чтобы новые параметры вступили в силу, необходимо выйти из программы «Doors» и запустить её заново.

Вкладка «Контроллеры»

На данной вкладке находится таблица с параметрами зарегистрированных в программе контроллеров, а также две кнопки.



При нажатии на кнопку «Автоконфигурация» () программа «Doors» опрашивает сеть контроля доступа и получает информацию, определяющую, какие контроллеры подключены к сети и настройки контроллеров/дверей. Затем эта информация заносится в базу данных программы «Doors». После того, как сервером будут

получены все данные, в окне «Установка системы/Контроллеры» будет отображена информация о настройках всех обнаруженных контроллеров сети контроля доступа.

В процессе автоконфигурации автоматически находятся подключённые платы расширения. В случае отсутствия на каком-либо контроллере установленной платы расширения программа выводит диалоговое окно, в котором пользователь может выбрать, должна ли программа для этого контроллера добавлять в базу данных вторую дверь. Варианты действий:

- «Yes» («Да») – создать вторую дверь для данного контроллера;
- «Yes To All» («Да для всех») – создавать вторые двери для всех контроллеров;
- «No» («Нет») – не создавать вторую дверь для данного контроллера;
- «No To All» («Нет для всех») – не создавать вторые двери для всех контроллеров, к которым не подключены платы расширения.



Вторая кнопка – кнопка «Установить время» (Set Time). Чтобы все события отслеживались правильно, необходимо синхронизировать время и дату между сервером и всеми контроллерами. Время и дата сервера загружаются во все контроллеры.

Описание полей таблицы контроллеров приведено в табл. Б2. Часть полей носит информативный характер, другие поля могут быть изменены пользователем.

Таблица Б2. Назначение полей таблицы контроллеров

Название столбца	Изменяемый	Назначение столбца
Адрес контроллера	Нет	Адрес контроллера в системе
Тип	Нет	Модель контроллера
Версия ПЗУ	Нет	Версия микропрограммы контроллера
Всего пользователей	Нет	Максимальное число пользователей, которое может быть занесено в память контроллера

Продолжение табл. Б2

Название столбца	Изменяемый	Назначение столбца
Всего событий	Нет	Максимальное число событий, которое может храниться в памяти контроллера
Автодозвон	Да	Если автодозвон активирован, то при заполнении памяти контроллера событиями контроллер автоматически подключается к ПК с ПО «Doors» и выгружает туда события
Порог автодозвона	Да	Процент заполнения памяти контроллера, при достижении которого происходит автодозвон
ЗПП	Да	Активировать ли на данном контроллере режим локального запрета повторного прохода
Считыватель 1 Тип Wiegand	Да	Способ управления индикацией считывателя 1
Считыватель 2 Тип Wiegand	Да	Способ управления индикацией считывателя 2

Вкладка «Двери»

Параметры дверей настраиваются на вкладке «Двери». Содержимое вкладки представляет собой таблицу, в ячейках которой размещены параметры дверей. Часть полей носит только информативный характер, другие параметры могут быть изменены пользователем. Назначение полей таблицы приведено в табл. Б3.

Таблица Б3. Назначение полей таблицы дверей

Название столбца	Изменяемый	Назначение столбца
Название двери	Да	Название двери (любая строка)
Адрес контроллера	Нет	Адрес контроллера, которому принадлежит данная дверь, в системе
Адрес двери	Нет	Адрес двери для контроллера
Класс двери	Да	Позволяет причислить дверь к произвольному классу, после чего можно будет управлять всеми дверьми одного класса одновременно

Продолжение табл. Б3

Название столбца	Изменяемый	Назначение столбца
Тип считывателя	Да	Тип считывателя: стандартный, вход в охраняемую зону, выход из охраняемой зоны, считыватель для проверки присутствия пользователя
Доступ	Да	Определяет, разрешён ли доступ через данную дверь. Доступ по нажатию кнопки разрешён всегда
Secondary ID Required Timezone	Да	Временная зона, в период действия которой будет активна двойная аутентификации
Secondary ID Wait Time	Да	Время ожидания ввода ПИН-кода, по истечении которого надо будет опять предъявлять карту
Время разблокировки	Да	Время, на которое разблокируется замок данной двери
Время открытия	Да	Если дверь остаётся открытой более заданного здесь времени, вырабатывается тревожное событие
Временная зона блок./разблок.	Да	Позволяет задать временную зону, в период которой дверь будет автоматически разблокирована
Вход первого человека	Да	Если задана временная зона разблокирования, то здесь можно задать режим, при котором автоматическое разблокирование происходит только после прохода человека с действительной картой; также можно выбрать задержку разблокирования (15, 30, 45 или 60 минут)
Выход – дверь взломана	Да	Определяет, будет ли в случае взлома двери активирован тревожный выход контроллера
Выход – дверь не закрыта	Да	Определяет, будет ли при несвоевременном закрытии двери активирован тревожный выход контроллера

Окончание табл. Б3

Название столбца	Изменяемый	Назначение столбца
Основная кнопка выхода	Да	Определяет действие контроллера при нажатии основной кнопки выхода (разблокировать дверь, не разблокировывать её или не выполнять никаких действий)
Дополнительная кнопка выхода	Да	Определяет действие контроллера при нажатии дополнительной кнопки выхода (длительное разблокирование двери, краткосрочное разблокирование двери или не выполнять никаких действий)

Переназначаемые входы/выходы платы расширения SB-293

Большинство входов и выходов контроллеров Keri имеют фиксированное назначение. Входы и выходы платы расширения SB-293 могут быть полностью (в случае использования платы только как расширитель входов/выходов) или частично (в случае использования платы для управления второй дверью – дверью В) переназначены.

Переназначенные входы и выходы могут использоваться для выполнения специальных задач, таких как дополнительная кнопка запроса на выход, датчик положения второй двери и выход тревоги взлома двери и тревоги незакрытой двери.

Настройка входов и выходов осуществляется на двух вкладках окна «Установка системы»: «Конфигурация Вх/Вых» и «Конфигурация связей».

На вкладке «Конфигурация Вх/Вых» производится настройка отдельных входов и выходов. Для этого сначала надо выбрать необходимый контроллер из выпадающего списка «Контроллеры». В нём отображаются только контроллеры, имеющие установленные платы расширения. Справа в поле «Дополнительная» будет отображена модель установленной платы.

В центре окна располагаются списки входов (слева) и выходов (справа). Входы и выходы платы расширения, имеющие фиксиро-

ванное назначение, неактивны (они серого цвета). Параметры остальных входов и выходов могут быть изменены.

Для входов можно задать следующие параметры:

- «Названия входов» – можно задать произвольное название входа для удобства оператора;
- «Переназначение» – вход 3 может использоваться как вход общего назначения, так и как дополнительный вход запроса на выход для двери В; во втором случае необходимо поставить галочку в поле «Переназначение», в этом случае изменить название входа будет нельзя;
- «Режим» – можно выбрать тип входа: нормально-разомкнутый (НР) или нормально-замкнутый (НЗ).

Для выходов можно задать следующие параметры:

- «Названия выходов» – можно задать произвольное название выхода для удобства оператора;
- «Переназначение» – выходы 3 и 4 могут использоваться как выходы общего назначения, так и для сигнализации о слишком долго открытой двери В (выход 3) или двери А (выход 4); во втором случае необходимо поставить галочку в поле «Переназначение» напротив соответствующего выхода, в этом случае изменить название выхода будет нельзя.

На вкладке «Конфигурация связей» можно запрограммировать связи входов и выходов, т.е. при поступлении сигналов на определённые входы на выход будет выдаваться сигнал. Для этого сначала надо выбрать необходимый контроллер из выпадающего списка «Контроллеры». В нём отображаются только контроллеры, имеющие установленные платы расширения. Справа в поле «Дополнительная» будет отображена модель установленной платы.

После этого из выпадающего списка «Связи» необходимо выбрать нужную связь для редактирования. Для создания новой связи



нажмите кнопку «Создать новую связь» () и в появившемся диалоговом окне укажите название новой связи.

В связи могут участвовать один или несколько входов и выходов. Входы и выходы с фиксированными назначениями, а также переназначенные входы и выходы в связи входить не могут. Для

включения входа или выхода в связь необходимо поставить галочку в поле рядом с нужным входом.

В случае, когда в связи участвуют несколько входов, необходимо в разделе «Комбинация входов» выбрать, при каком состоянии выбранных входов будет послан сигнал на выходы: когда будет сигнал хотя бы на одном из выбранных входов (режим «ИЛИ»), или когда сигнал будет одновременно на всех входах (режим «И»).

Для выходов можно выбрать параметры сигнала:

- «Режим» – будет ли происходить активация выхода (размыкание нормально-замкнутого и замыкание нормально-разомкнутого выхода) или нормализация (приведение выхода в нормальное состояние);
- «Временная» – можно выбрать временную зону, соответствующую данной связи; вход или выход из этой временной зоны не будет вызывать активацию связи, а связь будет действительна только в период этой временной зоны;
- «Задействовать выходы» – этот пункт работает в связке с пунктом «Только сообщение о событии»: может быть выбран только один из этих пунктов; если выбран пункт «Задействовать выходы», то при активации этой связи сработают реле на плате расширения; если выбран пункт «Только сообщение о событии», то при активации связи будет сгенерировано событие, а реле переключаться не будут;
- «Только сообщение о событии» – см. «Задействовать выходы»;
- «Звуковое уведомление связи» – если ПО «Doors» находится в режиме мониторинга, то появление события активации связи будет сопровождаться звуковым сигналом;
- «Тип» – этот пункт позволяет выбрать, на сколько времени выходное реле будет переключено при активации связи; возможны следующие варианты:
 - «Импульс» – реле будет переключено на число секунд, указанных в поле «Секунд»;
 - «Следящий» – реле будет переключено в течение того времени, пока связь будет активирована, т.е. будет поступать сигнал на соответствующие входы;

- «Триггер» – реле не вернётся в прежнее состояние автоматически, его должен переключить оператор.

Оператор имеет возможность управлять переназначаемыми выходами вручную. Для этого необходимо выбрать пункт меню «Управление» → «Управление выходами...». В появившемся окне надо выбрать нужный контроллер с установленной на нём платой расширения в поле «Контроллер». Ниже размещается список выходов, справа от которых расположены кнопки «Вкл» (для активации выхода) и «Выкл» (для деактивации выхода). Кнопки, соответствующие выходам с фиксированным назначением, неактивны, т.е. эти выходы не могут управляться оператором.

Состояние контроллера

Программа позволяет опросить сеть контроля доступа и получить информацию о настройках контроллера/двери. Затем эта информация заносится в базу данных программы. Это самый быстрый способ проверки того, что все контроллеры/двери распознаны системой контроля доступа и настройки контроллеров правильны. Можно получать информацию как о состоянии одного конкретного контроллера, так и всех сразу. Информация о настройках контроллеров приведена на рис. Б2.

Установка системы

Контроллеры

Двери

Конфигурация Вх/Вых

Конфигурация связей

Статус контроллеров

Конфигурация сети

Опции Системы

?

STATUS

???

STAT ALL

	Название Двери	Адрес	Есть связь	Тип контроллера	Версия ПЗУ	Конфигурация ОЗУ	События	В памяти пользователей	Да
1		C001 D1	ONLINE	PXL250s	6.3.49	Нормальная	1	6	20.04
2		C001 D2							
3		C003 D1	ONLINE	PXL500	8.4.44	Расширенная	29	2	20.04
4		C003 D2							

Рис. Б2. Фрагмент окна ПО «Doors» для отображения состояния контроллеров

Каждая строка таблицы соответствует одной двери, однако часть параметров относятся к контроллеру в целом. Поэтому, если

у контроллера сконфигурировано две двери, то в строке, соответствующей второй двери, часть полей пуста. Описание всех полей таблицы приведено в табл. Б4.

Таблица Б4. Назначение полей таблицы состояния контроллеров

Название столбца	Назначение столбца
Название двери	Заданное оператором название двери
Адрес	Адрес двери, состоящий из адреса контроллера и адреса двери на этом контроллере
Есть связь	Показывает, была ли установлена связь с контроллером (зелёная надпись «ONLINE») или нет (красная надпись «OFFLINE»)
Тип контроллера	Показывает тип контроллера, при этом, если к контроллеру подключена плата расширения, то указывается её модель, а не самого контроллера
Версия ПЗУ	Показывает версию микропрограммы контроллера
Конфигурация ОЗУ	Показывает размер памяти контроллера: нормальная или расширенная
События	Показывает число событий в памяти контроллера
В памяти пользователей	Показывает число зарегистрированных в контроллере пользователей
Дата	Показывает дату, установленную в контроллере на момент опроса его состояния
Время	Показывает время, установленное в контроллере на момент опроса его состояния
Холодных сбросов	Показывает число «холодных» сбросов контроллера, при которых питание контроллера отключалось, а затем подавалось вновь
Горячих сбросов	Показывает число «горячих» сбросов контроллера, при которых его процессор «зависал» и контроллер автоматически перезагружался
Ошибка самотестирования	Число ошибок самотестирования контроллера при его включении, вызванных ошибками в памяти контроллера или ненадлежащего напряжения питания

Продолжение табл. Б4

ЗПП	Показывает, применяются ли в данном контроллере правила локального запрета повторного прохода
Доступ	Показывает, разрешён ли доступ через данную дверь (контроллер может разблокировать её) или нет (контроллер игнорирует предъявленные карты)
Тип считывателя	Показывает тип считывателя, подключённого к контроллеру
Secondary ID Required Timezone	Временная зона, в период действия которой будет активна двойная аутентификации
Secondary ID Wait Time	Время ожидания ввода ПИН-кода, по истечении которого надо будет опять предъявлять карту
Статус дверей	Показывает состояние двери на момент опроса контроллера (открыта, закрыта, взломана и т.п.)
Блокировка дверей	Показывает состояние замка двери на момент опроса контроллера (разблокирован, заблокирован, разблокирован автоматически и т.п.)
Время разблокировки двери	Число секунд, на которое будет разблокирован дверной замок после предъявления действительной карты
Время открытия двери	Число секунд, которое может быть открыта дверь до генерации тревоги
ВЗ разблокировки двери	Временная зона разблокировки/блокировки данной двери
Auto Unlock/Lock Status	Определяет состояние сопоставленной данной двери временной зоны (активна или приостановлена)
Вход первого человека	Отображает значение параметра «Вход первого человека» для данной двери (значение параметра см. в табл. Б3)
Выход – дверь взломана	Показывает выходное реле контроллера, соответствующее событию «Дверь взломана»

Окончание табл. Б4

Выход – дверь не закрыта	Показывает выходное реле контроллера, соответствующее событию «Дверь не закрыта»
Основная кнопка выхода	Определяет, как контроллер должен реагировать на сигнал «Основная кнопка выхода»
Дополнительная кнопка выхода	Определяет, как контроллер должен реагировать на сигнал «Дополнительная кнопка выхода»

Б3. Настройки пользователей (карт доступа)

Для создания и настройки пользователей необходимо сделать следующее:

- создать временные зоны;
- создать группы доступа;
- зарегистрировать карты доступа;
- настроить параметры зарегистрированных карт.

Выполнение этих действий подробно описано ниже.

Создание и редактирование временных зон

Настройка временных зон производится в окне, открываемом выбором пункта меню «Установки» → «Временные зоны...» или



нажатием кнопки

Основная настройка производится на вкладке «Временная зона». Для редактирования определённой зоны надо её выбрать из выпадающего списка «ИМЕНА ВРЕМЕННЫХ ЗОН». Для создания



новой временной зоны необходимо нажать кнопку и ввести её название в поле «ИМЕНА ВРЕМЕННЫХ ЗОН». Может быть создано до 32 временных зон.

Для каждого из дней «10-дневной недели» (7 дней недели плюс 3 типа праздников) может быть задано до 4 временных интервалов,

либо значения «Всегда» (весь день), «Никогда» (в этот день доступа нет) или «Не используется» (возможно только для праздников). Для определения временного интервала надо ввести время его начала в поле «Старт» и время окончания в поле «Стоп».

Для редактирования списка праздников необходимо открыть соответствующую вкладку («Список праздников 1», «Список праздников 2» или «Список праздников 3») и в таблице заполнить соответствующие поля («Даты» и «Имена»).

Создание и настройка групп доступа

Команды настройки групп доступа позволяют совместить временные зоны и двери в набор информации, которая применяется к владельцам карт. Совместно с временными зонами группы доступа дают возможность определить, какие двери владельцу карт разрешено использовать, в какое время дня и в какой день недели. Настройка временных зон производится в окне, открываемом выбором пункта меню «Установки» → «Группы доступа...» или нажа-



тием кнопки и представляет собой последовательный ответ на вопросы программы. Перемещение между этапами управляется кнопками «<< Начало», «< Назад», «Далее >» и «Конец >>» в нижней части окна.

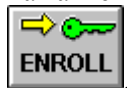
Достаточные инструкции к каждому этапу приводятся в нижней части окна. После выполнения всех необходимых действий закройте окно, нажав на крестик в его верхнем правом углу.

Регистрация новых карт

Для регистрации новых карт необходимо открыть окно «Установка карт» выбором пункта меню «Установки» → «Карты» или



нажатием кнопки, а в открывшемся окне нажать кнопку



Существует два способа ввода карт: пакетный ввод путём задания интервала номеров карт и индивидуальный ввод карт путём

поднесения каждой карты к считывателю карт мастер-контроллера. Первый способ лучше использовать, когда вводится большое количество карт с последовательными ID номерами. Второй способ – при вводе небольшого количества карт или когда их номера идут не по порядку.

При выполнении лабораторных работ используется способ с поднесением карт к считывателю. Для выбора этого способа необходимо нажать на кнопку «Считывать карты Wiegand».

Из списка «Channels» необходимо выбрать, от какого считывателя ожидать коды карт: только от первого («Read on A Only»), только от второго («Read on B Only») или от обоих («Read on A and B, Both»). Из списка «Primary Format» («Основной формат») необходимо выбрать формат карт. При выполнении данных лабораторных работ выберите пункт «26 Bit Wiegand».

После выполнения описанных в предыдущем абзаце предварительных настроек нажмите кнопку «Старт Регистрация» и последовательно поднесите к считывателю карты, которые надо зарегистрировать. Затем нажмите кнопки «Стоп Регистрация» и «Конец регистрации >>». На открывшейся странице нажмите кнопки «ВЫПОЛНИТЬ РЕГИСТРАЦИЮ» и «Закрыть».

После выполнения этих действий в списке карт доступа окна «Установка карт» появятся строки, соответствующие вновь зарегистрированным картам.

Настройка параметров зарегистрированных карт

Настройка параметров карт производится в окне «Установка карт». В центре окна расположена таблица, строки которой соответствуют отдельным картам, а назначение полей описано в табл. Б5.

Таблица Б5. Назначение полей таблицы зарегистрированных карт

Название столбца	Назначение столбца
Фамилия	Фамилия владельца карты
Имя	Имя владельца карты
Отчество	Отчество владельца карты
Внутренний номер	Внутренний номер карты, используемый для её идентификации
Номер карты	Номер карты, напечатанный на ней; данный номер не обязателен для работы системы
Поиск сотрудников	Определяет, будет ли отслеживаться местоположение этой карты
Группа доступа	Группа доступа, к которой принадлежит данная карта
Отдел	Название отдела, в котором работает владелец карты; может использоваться, например, для сортировки списка карт
Вкл/Выкл	Позволяет активировать и деактивировать отдельные карты
ЗПП	Позволяет отключать проверку правила «локальный запрет повторного прохода» для отдельных карт
Secondary ID	ПИН-код пользователя, используемый при двойной аутентификации
Secondary Format	Формат, в котором считыватель будет передавать ПИН-код
Secondary Status	Вариант действия двойной аутентификации для владельца данной карты: – Required – пользователь всегда должен вводить ПИН-код; – No Access – пользователь не может получить доступ через те двери, где поддерживается двойная аутентификация; – Exempt – пользователь не должен вводить ПИН-код
Дата регистрации	Дата, когда пользователь был впервые активирован
Время регистрации	Время, когда пользователь был впервые активирован
Дата аннулирования	Дата, когда пользователь был аннулирован оператором

Продолжение табл. Б5

Время аннулирования	Время, когда пользователь был аннулирован оператором
Активировать Дата	Для временных пользователей – дата начала действия карты
Активировать Время	Для временных пользователей – время начала действия карты
Дата окончания	Для временных пользователей – дата окончания действия карты
Время окончания	Для временных пользователей – время окончания действия карты

Б4. Быстрое обновление сети контроля доступа

При быстром обновлении программа загружает рабочую информацию в сеть контроля доступа. Изменения, сделанные в какой-либо из баз данных программы «Doors», не вступят в силу в сети контроля доступа до тех пор, пока они не будут загружены в сеть.

Для того чтобы вызвать окно обновления сети контроллеров, необходимо выбрать пункт меню «Управление» → «Обновить

сеть» или нажать кнопку .

В верхней части окна находится таблица, имеющая следующие поля:

- «Требуется обновление» – вносились ли в базы данных программы «Doors» изменения после последнего обновления сети;
- «Быстрое обновление сети» – если выбрать этот пункт (надпись «SKIP» сменится на надпись «UPDATE» на зелёном фоне), то в сеть контроллеров будет загружена только обновлённая информация;
- «Полное обновление сети» – если выбрать этот пункт, то в сеть будет загружена полная конфигурационная информация;
- «Сбор событий» – если выбрать этот пункт, то из контроллеров будет загружена информация по событиям;
- «Статус» – текущее состояние операции обновления сети контроля доступа.

После выбора необходимого действия надо нажать кнопку «Начать» и начнётся процесс обновления сети и/или сбора событий. Можно указать число попыток, которое будет делать программа в случае какого-либо сбоя. Также можно указать, чтобы обновление началось не в данный момент, а через определённое время, например ночью.

Б5. Мониторинг событий

Команды настройки окон монитора позволяют настроить до трёх различных окон для возможности упорядоченного наблюдения за сетью контроля доступа в реальном времени.

Настройка команд монитора и событий осуществляется в окне «Установки монитора», открываемом выбором пункта меню «Установки» → «Монитор и события...». Окно имеет несколько вкладок.

На первой вкладке, «Опции мониторинга», можно задать следующие параметры:

- «Предупреждение о переполнении буфера» определяет, должен ли сервер получать информацию о событиях из буфера памяти событий контроллера при его заполнении. Это позволяет гарантировать, что по мере поступления новых событий, старые события не будут удалены для освобождения места для новых событий. Если буфер контроллера достигает определённого предела, контролер загружает содержимое своего буфера в сервер, освобождая буфер;
- «Тип файла событий» определяет, как часто текущий файл событий будет закрываться, а события будут помещаться в новый файл. Это позволит регулярно архивировать файлы событий, а также предотвратит чрезмерное увеличение файла событий;
- «Имя первого окна», «Имя второго окна», «Имя третьего окна» – программа «Doors» имеет 3 окна для отображения текущих событий. Эти поля позволяют задать произвольные наименования для окон просмотра событий.

На второй вкладке, «Сообщения доступа», может производиться настройка параметров для каждого типа сообщения. На вкладке

расположена таблица, строки которой представляют различные события, а по столбцам расположены следующие параметры:

- «Текст сообщения» – текст сообщения, который будет отображаться в окне отображения событий;
- «Сохранить в файл» – определяет, будет ли данное событие сохраняться в файле событий;
- «Отображать в первом окне», «Отображать во втором окне», «Отображать в третьем окне» – определяют, в каких из трёх окон отображения событий будет выводиться данное событие;
- «Звуковое предупреждение» – при поступлении события, для которого включено звуковое оповещение, начинает периодически выдаваться звуковая тревога, которая выключится после того, как оператор подтвердит прочтение сообщения;
- «Контроллер Отчёты События» – определяет, будет ли данное событие генерироваться контроллером (применимо только к событиям, происходящим в сети контроля доступа).

Для включения режима мониторинга и открытия окон просмотра событий необходимо открыть окно «Управление монитором», для чего выбрать пункт меню «Управление» → «Включить мони-



тор...» или нажать кнопку . Окно «Управление монитором» на фоне трёх открытых окон просмотра событий показано на рис. БЗ.

По горизонтали окно «Управление монитором» делится на три части:

- «Статус соединения» – информация о состоянии подключения к сети СКУД;
- «Просмотр окон» – три кнопки, позволяющие открыть три окна просмотра событий; закрытие окон производится нажатием на кнопку с крестиком в правом верхнем углу соответствующего окна;

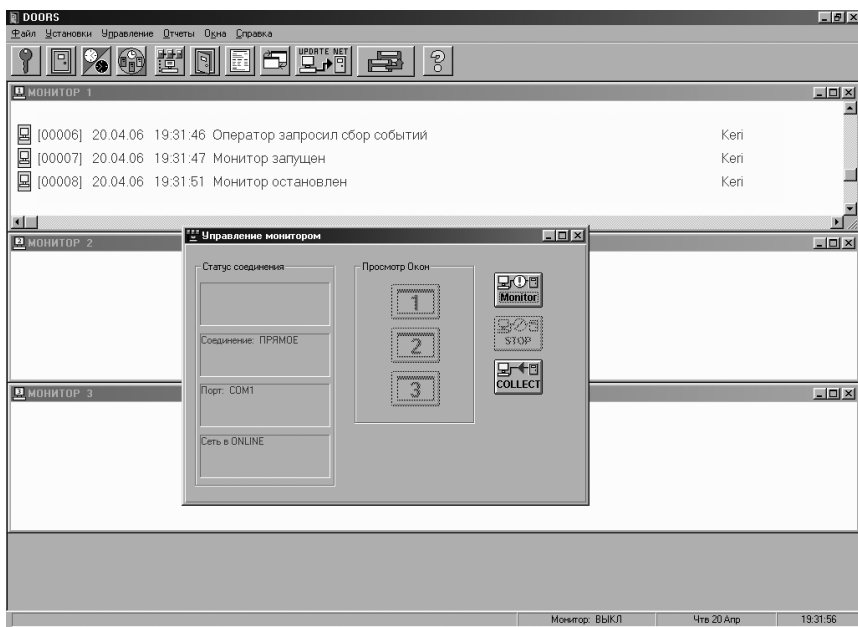


Рис. Б3. Окно ПО «Doors» для управления мониторами событий

- кнопки: запуска процесса мониторинга () , остано-
ва процесса мониторинга () и сбора накопленных
контроллерами СКУД событий () .

Б6. Управление дверьми

Оператор имеет возможность управлять состоянием дверей: разблокировать, блокировать их, отменять действие автоматического разблокирования на основе временных зон. Управление дверьми осуществляется из окна «Управление дверями» (рис. Б4). От-

крытие этого окна происходит при выборе пункта меню «Управление» → «Двери...» или нажатием кнопки



«Двери...» или нажатием кнопки

Управление может осуществляться сразу несколькими дверями. Для этого надо выбрать или их по отдельности (на панели «ДВЕРИ»), или сразу целый класс дверей (на панели «КЛАССЫ ДВЕРЕЙ»). Управление осуществляется кнопками, расположенными вдоль правой стороны окна, назначение кнопок приведено в табл. Б6.

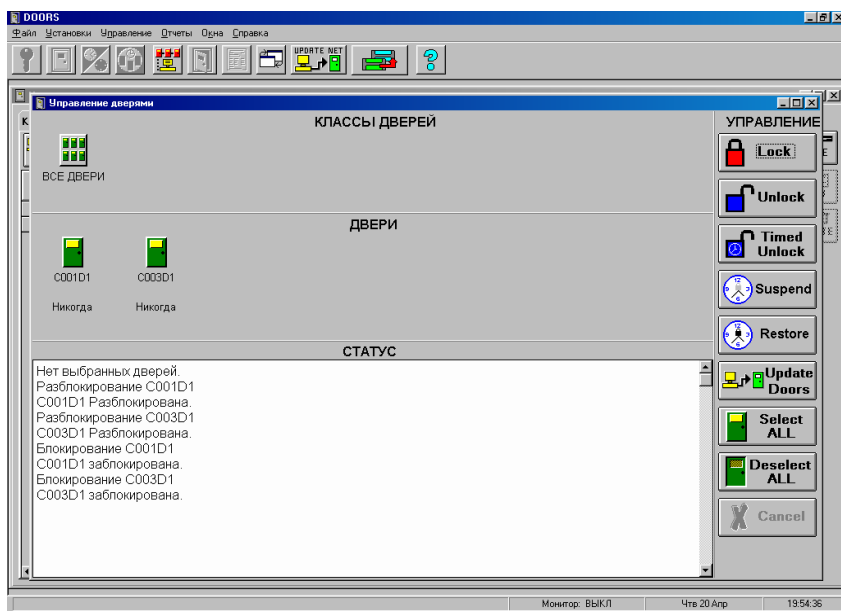


Рис. Б4. Окно ПО «Doors» для управления дверями с консоли

Таблица Б6. Кнопки управления дверями

Изображение кнопки	Выполняемое действие
	Блокирование выбранных дверей
	Разблокирование выбранных дверей
	Разблокирование выбранных дверей на задаваемое оператором время
	Отмена действия временных зон автоматического разблокирования/блокирования выбранных дверей
	Восстановление действия временных зон автоматического разблокирования/блокирования выбранных дверей
	Посылка в сеть информации о параметрах выбранных дверей
	Выбор всех дверей, зарегистрированных в системе
	Отмена выбора всех дверей
	Отмена выполнения операции

Б7. Создание и просмотр отчётов

Существует два типа отчётов: отчеты по настройкам системы и отчёты по событиям. Для просмотра быстрых отчётов необходимо выбрать пункт меню «Отчёты» → «Отчёты...» или нажать кнопку



, в результате чего откроется окно, представленное на рис. Б5. В данном окне надо нажать кнопку, соответствующую нужному

типу отчёта, после чего в появившемся окне выбрать дату и время, за которые нужен отчёт, и нажать кнопку «Print». Отчёт будет выведен в новом окне.

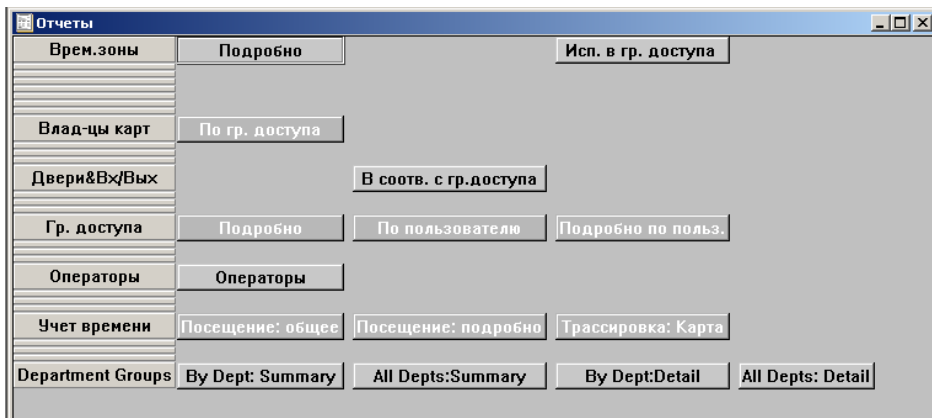


Рис. Б5. Окно ПО «Doors» для получения отчётов по настройкам

Для получения отчётов по событиям необходимо выбрать пункт меню «Отчёты» → «По событиям...». Внешний вид открывающегося при этом окна «Отчёт по событиям» приведён на рис. Б6.

На окне «Отчёт по событиям» расположены четыре вкладки:

- «Быстрый поиск»;
- «Расширенный поиск»;
- «Библиотека»;
- «Опции».

На вкладке «Быстрый поиск» можно выбрать параметры поиска из небольшого списка наиболее часто используемых критериев поиска (двери, владельцы карт, события, даты). По умолчанию выбран вывод всех событий, однако можно конкретизировать вывод событий.

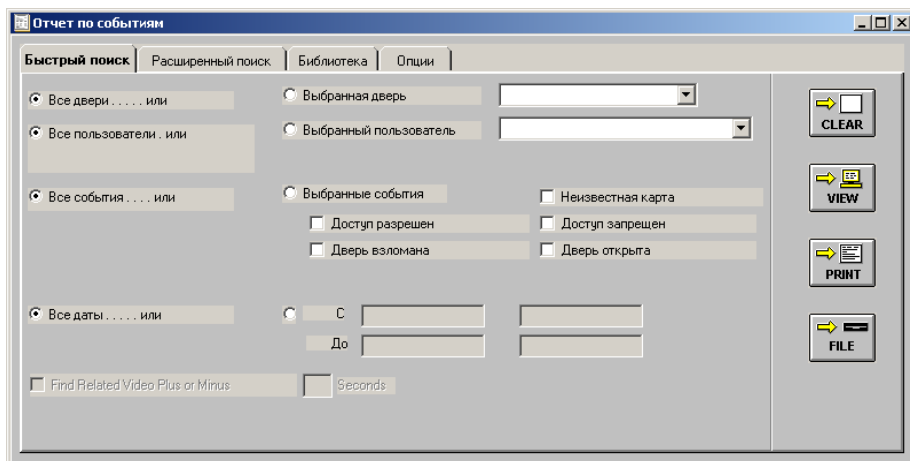


Рис. Б6. Окно ПО «Doors» для получения отчёта по событиям

На вкладке «Расширенный поиск» можно создать выражение поиска из списка событий, логических операторов, значений полей и связующих операторов.

Однажды созданное выражение расширенного поиска может быть сохранено в библиотеке для дальнейшего использования. Сохранение и загрузка шаблонов поиска событий осуществляется на вкладке «Библиотека».

На вкладке «Опции» можно изменить два параметра:

- «Реверсировать порядок сортировки» – при выборе этого параметра записи будут сортироваться в порядке от большего к меньшему;
- «ИН карты/ИН пользователя в файле отчёта (Рабочее время)» – при выборе этого параметра в отчёте, сохраняемом в файл, вместо имён пользователей будут указываться их номера.

Лабораторная работа № 2
ИЗУЧЕНИЕ ВОЗМОЖНОСТЕЙ ПОСТРОЕНИЯ
РАСПРЕДЕЛЁННОЙ СКУД НА ОСНОВЕ ОБОРУДОВАНИЯ
КОМПАНИИ KERI SYSTEMS

Цель работы:

- 1) Изучение основных возможностей построения распределённых СКУД, предоставляемых контроллерами компании Keri Systems, США.
- 2) Приобретение практических навыков создания и использования распределённых СКУД на примере контроллеров производства компании Keri Systems, США.

2.1 Описание объекта лабораторного исследования

В данном разделе описывается оборудование, используемое для выполнения лабораторной работы, и основные возможности этого оборудования.

2.1.1 Состав лабораторного стенда

Лабораторная работа выполняется на общем стенде по системам телевизионного наблюдения, однако для данной работы используется только перечисленное ниже оборудование:

- контроллер PXL – 250W;
- контроллер PXL – 500W;
- расширительная плата SB-293;
- 2 считывателя карт доступа с клавиатурой P-600H;
- считыватель карт доступа P – 300;
- считыватель карт доступа H-Reader;
- персональный компьютер с установленной ОС Windows XP, имеющий COM-порт;
- монитор;
- программное обеспечение СКУД «Doors».

Также использовалось вспомогательное оборудование:

- бесконтактные карты доступа;

- блок бесперебойного питания 12 В постоянного тока;
- 2 имитатора кнопки запроса на выход;
- 3 имитатора датчика открытия двери;
- соединительные провода.

Схема соединения используемого в данной работе оборудования показана на рис. 2.1.

Ниже приводится краткое описание используемого оборудования.

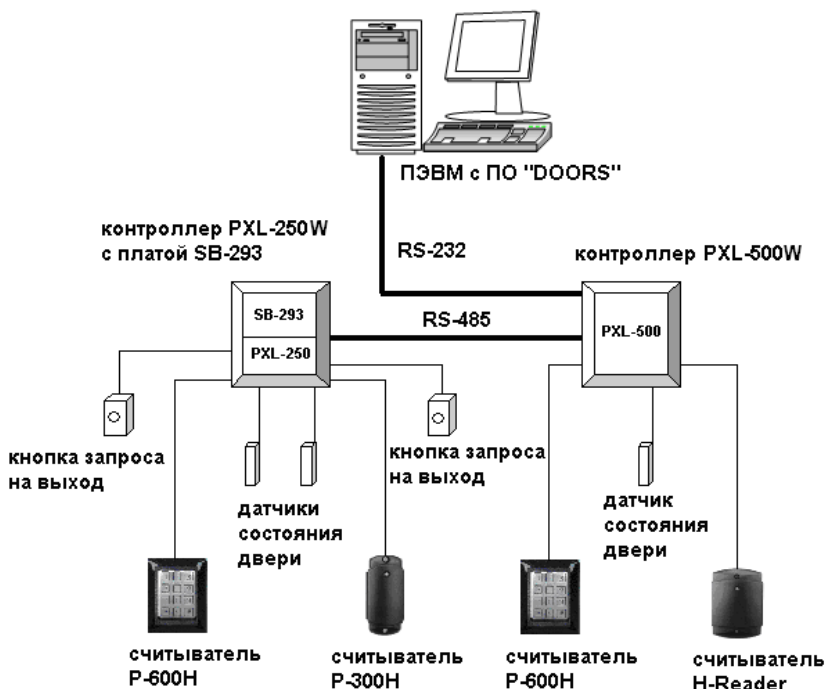


Рис. 2.1. Схема соединения устройств для изучения распределённой СУД

2.1.2 Контроллер PXL-250W

Контроллер PXL-250W американской компании Keri Systems является одним из основных элементов системы контроля доступа. Контроллер получает информацию от считывателей карт доступа и

может автономно управлять работой различных исполнительных и управляемых преграждающих устройств системы, таких как электрозамки, шлагбаумы, турникеты и др.

На рис. 2.2 изображён внешний вид контроллера PXL-250W.

Возможности контроллера PXL-250W почти совпадают с возможностями контроллера PXL-500W (см. лабораторную работу № 1). Отличия от PXL-500W следующие:

- отсутствие поддержки некоторых дополнительных устройств (которые в данных лабораторных работах не использованы);
- поддержка платы расширения SB-293 (для контроллера PXL-500W может использоваться плата SB-593);
- меньший объём памяти для хранения данных о зарегистрированных пользователях (PXL-250W позволяет хранить информацию о 11 тысячах пользователей, PXL-500W – о 65 тысячах пользователей);
- отсутствие поддержки временных пользователей;
- пластмассовый бокс (у PXL-500W – металлический).



Рис. 2.2. Внешний вид контроллера PXL-250W

2.2 Порядок выполнения работы

1. Изучить возможности оборудования и стенда как единой системы по приведённым описаниям.

2. Провести подключение элементов лабораторного стенда в соответствии с рис. 2.1.

Внимание! Только после проверки подключения преподавателем можно подавать питание на элементы стенда.

3. Провести очистку памяти контроллеров. Для этого необходимо до подачи питания на контроллер установить перемычку JP10 для контроллера PXL-500W или JP3 для контроллера PXL-250W, нажать кнопку S1 и, удерживая её нажатой, подать питание на контроллер. Через 10 секунд снять питание с контроллера, убрать перемычку.

4. Установить адрес контроллеров в сети RS-485 (адрес PXL-500W – 1, PXL-250W – 2). Для этого надо до подачи питания на контроллер нажать кнопку S1 и, удерживая её нажатой, подать питание на контроллер, после чего отпустить кнопку. На дисплее контроллера будет отображаться текущий его адрес, а также направление его изменения. При однократном нажатии на кнопку S1 он изменяется (увеличивается или уменьшается) на 1, двукратное нажатие на кнопку меняет направление изменения адреса.

5. Плату SB-293 перевести в режим работы с двумя дверьми.

6. Запустить программу «Doors». Для входа в программу использовать учётную запись «Keri» (пароль «Keri»).

7. Настроить параметры сети в соответствии с собранной системой.

8. Настроить опции системы, включив следующие возможности программы:

- автоматический переход на летнее время и обратно;
- локальный запрет повторного прохода;
- временные пользователи;
- поиск сотрудников.

9. Провести поиск контроллеров в сети. Установить правильное время в контроллерах. Настроить свойства контроллера и обслуживаемой им двери.

10. Зарегистрировать несколько карт (пользователей).

11. Изучить возможности поиска сотрудника.
12. Изучить возможности управления состоянием дверей.
13. Создать аналог охранной системы путём настройки входов и выходов платы расширения SB-293.
14. Подготовить отчёт о выполненной работе по выданной преподавателем форме и защитить его.

2.3 Контрольные вопросы

1. Каковы отличия контроллера PXL-500W от контроллера PXL-250W?
2. Каким образом происходит объединение контроллеров в единую сеть?
3. В каких режимах может работать плата расширения SB-293?
4. Каким образом работает функция «поиска сотрудника»?
5. Какие возможности по управлению исполнительными устройствами есть у оператора СКУД?
6. Какие возможности по использованию дополнительных входов и выходов даёт плата SB-293?

Список литературы

1. Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов. М.: МИФИ, 2008. 584 с.
2. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования.
3. PXL – 250 Tiger Controller Quick Start Guide. Keri Systems.
4. PXL – 500/510 Tiger Controller Quick Start Guide. Keri Systems.
5. Pyramid Series Reader Quick Reference. Farpointe Data.

Приложение В

ПОДКЛЮЧЕНИЕ КОНТРОЛЛЕРА PXL-250W

На рис. В1 представлена схема контроллера PXL-250W, на которой используемые контактные колодки обозначены прямоугольниками с пронумерованными контактами. Назначение отдельных колодок приведено в табл. В1.

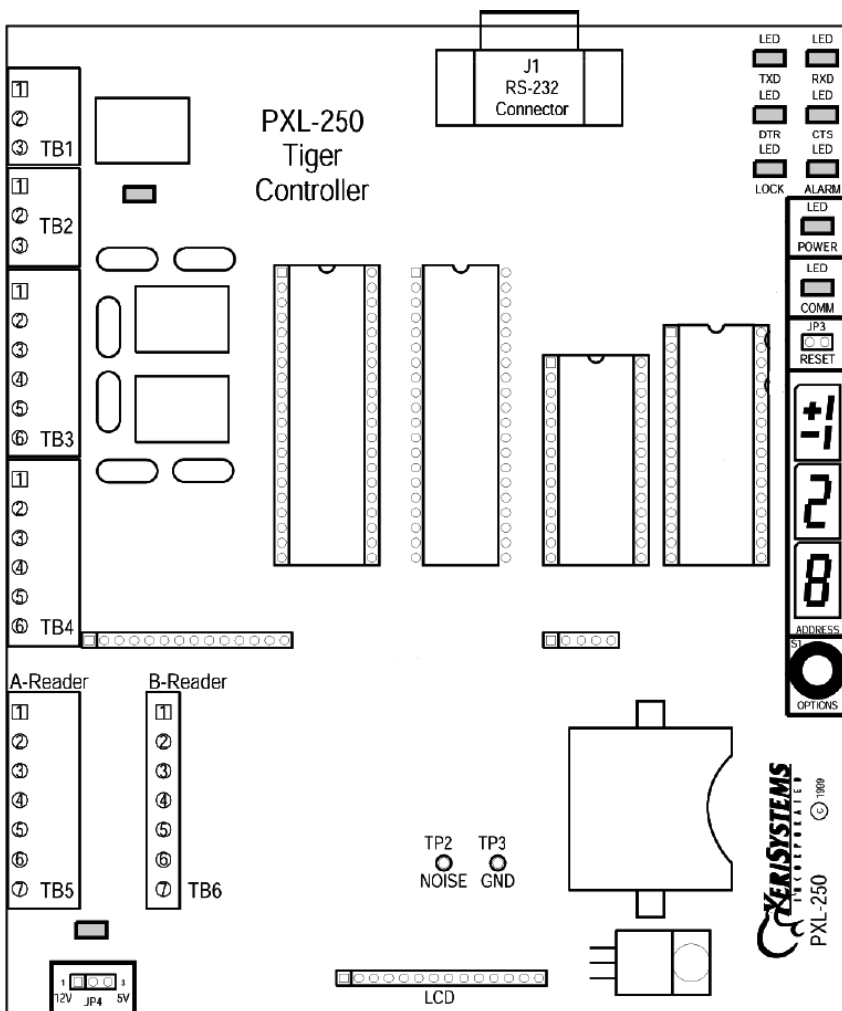


Рис. В1. Схема контроллера PXL-250W

Таблица В1. Назначение контактных колодок контроллера PXL-250W

Обозначение колодки	Назначение
TB1	Подключение к сети контроллеров по протоколу RS-485
TB2	Подключение источника постоянного тока напряжением 12В
TB3	Подключение средств оповещения и исполнительных устройств
TB4	Подключение датчика состояния двери и кнопки запроса на выход
TB5	Подключение считывателя № 1
TB6	Подключение считывателя № 2

В табл. В2 – В6 описано назначение отдельных контактов в обозначенных колодках.

Таблица В2. Назначение контактов в колодке TB1 (сеть RS-485)

№ контактов	Назначение
1	Отрицательный провод сети RS-485 (TxRx -)
2	Положительный провод сети RS-485 (TxRx +)
3	Экран кабеля

Таблица В3. Назначение контактов в колодке TB2 (питание)

№ контактов	Назначение
1	+12 В
2	Отрицательный провод
3	Заземление

Таблица В4. Назначение контактов в колодке TB3 (выходы)

№ контактов	Назначение
1	Замок – НО
2	Замок – общий
3	Замок – НЗ
4	Тревога – НО
5	Тревога – общий
6	Тревога – НЗ

Обозначения: НО – нормально открытый контакт, НЗ – нормально замкнутый контакт.

Таблица В5. Назначение контактов в колодке ТВ4 (входы)

№ контактов	Назначение
1	Датчик положения двери (НЗ)
2	Земля
3	Кнопка запроса на выход (НО)
4	Не используется
5	Земля
6	Кнопка глобальной разблокировки (НО) или запроса на выход (НО)

Обозначения: НО – нормально открытый контакт.

Таблица В6. Назначение контактов в колодках ТВ5 и ТВ6 (считыватели) и цвета проводов при подключении считывателей Р-600Н

№ контактов	Назначение	Цвет провода
1	Данные – 0	Зелёный
2	Динамик	Синий
3	Питание	Красный
4	Земля	Чёрный и серебристый
5	Зелёный светодиод	Коричневый
6	Красный светодиод	Оранжевый
7	Данные – 1	Белый

Приложение Г

ПОДКЛЮЧЕНИЕ ПЛАТЫ РАСШИРЕНИЯ SB-293

На рис. Г1 представлена схема платы расширения SB-293, на которой используемые контактные колодки обозначены прямоугольниками с пронумерованными контактами.

Переключение режима работы платы производится с помощью перемычки, устанавливаемой на разъём, обозначенный на рис. Г1 как «JP12». Если перемычка установлена, то плата работает в режиме увеличения числа входов и выходов общего назначения. Если перемычка снята, то плата работает в режиме контроля и управления второй дверью.

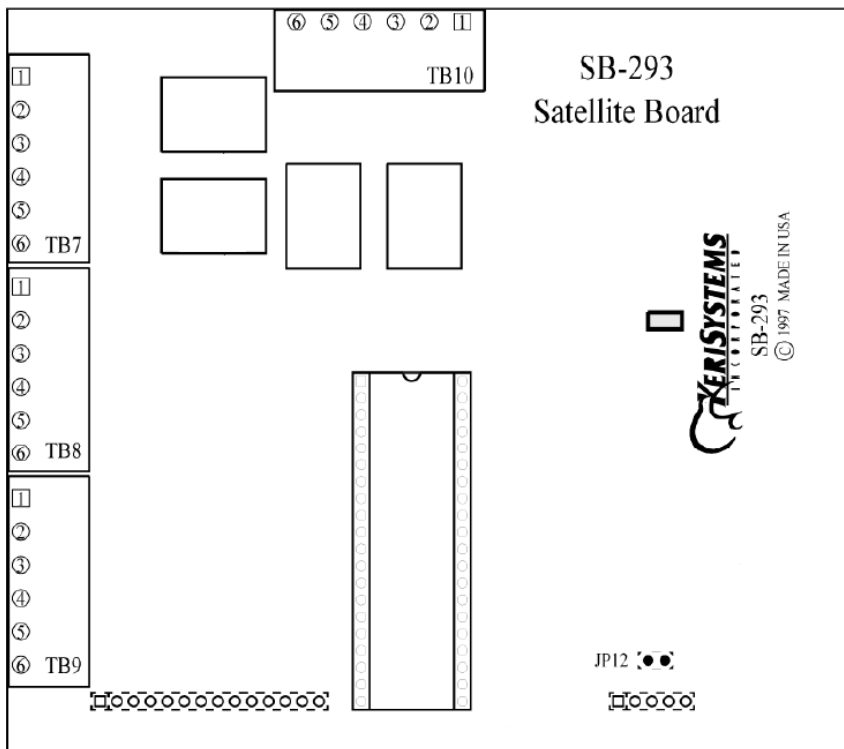


Рис. Г1. Схема платы расширения SB-293

Колодки TB7 и TB10 являются выходными, колодки TB8 и TB9 – входными. Назначение контактов различается в зависимости от режима работы платы и приведено в табл. Г1 – Г4.

Таблица Г1. Назначение контактов в колодке TB7

№ контактов	Назначение в режиме общих входов/выходов	Назначение в режиме второй двери
1	Выход общего назначения № 1 – НО	Замок – НО
2	Выход общего назначения № 1 – общий	Замок – общий
3	Выход общего назначения № 1 – НЗ	Замок – НЗ

Продолжение табл. Г1

№ контактов	Назначение в режиме общих входов/выходов	Назначение в режиме второй двери
4	Выход общего назначения № 2 – НО	Тревога – НО
5	Выход общего назначения № 2 – общий	Тревога – общий
6	Выход общего назначения № 2 – НЗ	Тревога – НЗ

Таблица Г2. Назначение контактов в колодке ТВ8

№ контактов	Назначение в режиме общих входов/выходов	Назначение в режиме второй двери
1	Вход общего назначения № 1	Датчик положения двери (НЗ)
2	Земля	Земля
3	Вход общего назначения № 2	Кнопка запроса на выход (НО)
4	Вход общего назначения № 3	Дополнительная кнопка за- проса на выход (НО)
5	Земля	Земля
6	Вход общего назначения № 4	Вход общего назначения № 4

Таблица Г3. Назначение контактов в колодке ТВ9

№ контактов	Назначение (для обоих режимов)
1	Вход общего назначения № 5
2	Земля
3	Вход общего назначения № 6
4	Вход общего назначения № 7
5	Земля
6	Вход общего назначения № 8

Таблица Г4. Назначение контактов в колодке ТВ10

№ контактов	Назначение в режиме общих входов/выходов	Возможное переназначение
1	Выход общего назначения № 3 – НО	Вторая дверь оставлена от- крытой – НО
2	Выход общего назначения № 3 – общий	Вторая дверь оставлена от- крытой – общий
3	Выход общего назначения № 3 – НЗ	Вторая дверь оставлена от- крытой – НЗ
4	Выход общего назначения № 4 – НО	Первая дверь оставлена от- крытой – НО
5	Выход общего назначения № 4 – общий	Первая дверь оставлена от- крытой – общий
6	Выход общего назначения № 4 – НЗ	Первая дверь оставлена от- крытой – НЗ

Лабораторная работа № 3

УСТРОЙСТВА БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Цель работы:

- 1) Изучение основных возможностей устройств биометрической идентификации.
- 2) Приобретение практических навыков работы с устройствами биометрической идентификации на основе технологий анализа радужной оболочки человеческого глаза, формы кисти руки, отпечатка пальца.

Введение

Под системой физической защиты (СФЗ) объекта понимается комплекс мер, включающий нормативные документы, организационные и технические меры, направленные на обеспечение безопасности объекта и его ценностей.

СФЗ состоит из нескольких подсистем, одной из которых является система контроля и управления доступом (СКУД). СКУД представляет собой совокупность технических и программных средств, инженерно-технических сооружений и организационных мер, обеспечивающих контролируемый доступ на объект и на отдельные его составляющие, а также запрещает такой доступ всем, кто не имеет соответствующих полномочий.

Для выполнения основной задачи системе управления доступом необходимо определить, имеет ли право субъект выполнить запрашиваемое действие или нет. Для этого, прежде всего, надо ответить на два вопроса: «Кто этот человек?» и «Тот ли он, за кого себя выдает?». Точность, с которой можно ответить на эти вопросы, определяет надежность СКУД. Существует мнение, что если нет возможности точно определить пользователя, то все другие средства безопасности не имеют смысла.

Идентификацией называется процесс отождествления объекта с одним из известных системе объектов. Другими словами, идентификация – выяснение того, кто есть человек, предъявивший системе некоторые данные (идентификатор).

Аутентификация – проверка соответствия пользователя предъявляемому им идентификатору. Иначе говоря, аутентификация

(употребляют термины верификация, отождествление) – это ответ на вопрос: «Является ли человек тем, кем представился?». Предположим, что человек с предъявленным идентификатором зарегистрирован в СКУД. Аутентификация заключается в сравнении дополнительно вводимых признаков этого человека с хранящимися в базе данных (БД) эталонами (полученными во время контрольного заполнения БД).

Различие между идентификацией и аутентификацией на практике не всегда наблюдается – процедуры могут выполняться одновременно одним и тем же способом.

Так, предъявляя пропуск охране, человек «представляется» и одновременно подтверждает личность (по фотографии). Применительно к аппаратно-программным средствам СКУД разница между процедурами идентификации и аутентификации заключается в следующем: при идентификации система просматривает всю БД зарегистрированных пользователей, сравнивая имеющиеся записи с введенным идентификатором, и если подобная запись найдена, система определяет уровень привилегий и другую информацию о субъекте. При аутентификации уже известно имя (идентификатор) субъекта, и для подтверждения его личности системе достаточно выполнить единственное сравнение – сопоставить дополнительно вводимые данные с данными о пользователе в базе данных.

Основные проблемы, связанные с применением идентификаторов в СКУД, – вероятность их потери или кражи. Идентификатор также можно забыть где-нибудь. Не исключена возможность изготовления злоумышленниками копии идентификатора.

На практике почти всегда для увеличения безопасности систем применяют одновременно несколько способов аутентификации. Например, перед считыванием магнитных карт система может требовать ввода пароля, а перед сканированием отпечатков пальцев – предъявление смарт-карты.

СКУД, построенные с использованием биометрической аутентификации, имеют ряд преимуществ перед системами на основе паролей или идентификаторов и встречаются в последнее время все чаще. Для повышения уровня безопасности на практике биометрическая аутентификация часто дополняется вводом ПИН (пароля) и/или предъявлением идентификаторов.

Устройства биометрической идентификации в СКУД

В число современных биометрических систем контроля доступа к информации входят системы проверки по форме кисти руки, рисунку кожи пальцев, сетчатке или радужной оболочке глаза, фотографии лица, динамике подписи и по голосу. Все биометрические системы характеризуются высоким уровнем безопасности прежде всего потому, что используемые в них данные не могут быть утеряны пользователем или похищены, копирование их сложно.

Биометрические системы представляют собой единственное решение проблемы контроля доступа на особо важных объектах. Например, биометрические системы используются при организации доступа в важные зоны ядерно-опасных объектов.

Метод распознавания по радужной оболочке глаза

Технология распознавания человека с помощью данных его радужных оболочек глаз – это способ идентифицировать человека с образом радужной оболочки (радужная оболочка – это тонкая пленка спереди глазного яблока в форме пластины, называемая также ирисом). Метод распознавания по радужной оболочке основан на уникальности рисунка радужной оболочки глаза (окрашенной части). Даже у однояйцовых близнецов рисунки радужек разные. Радужная оболочка защищена от внешней среды роговицей и тканевой жидкостью; в отличие от сетчатки, однако, радужная оболочка ясно видна на расстоянии. Случайные рисунки ириса созданы сплетением сетчатой структуры соединительной ткани и других видимых признаков (слоев, борозд, корон, впадин, пятен и т.п.). Рисунок радужной оболочки глаз человека (ириса) стабилен в течение всей жизни. Образ радужной оболочки левого глаза отличается от правого.

Пример рисунка радужной оболочки показан на рис. 3.1.

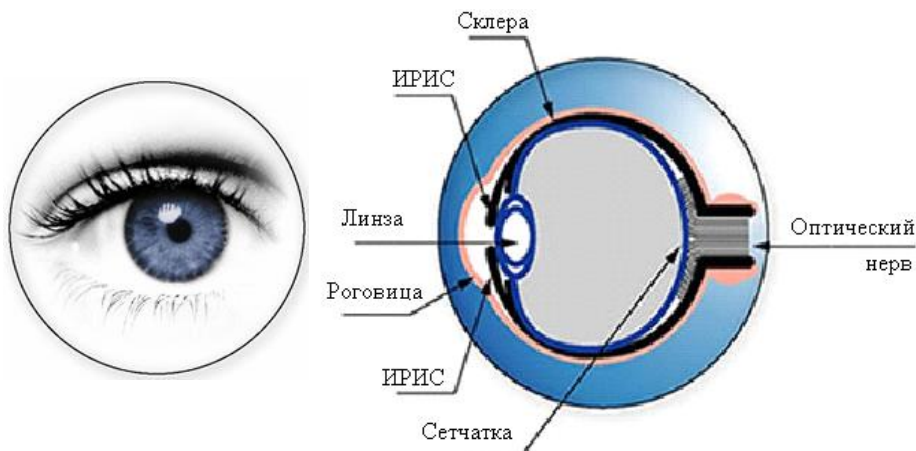


Рис. 3.1. Рисунок радужной оболочки человеческого глаза

Для реализации метода необходима фото- или видеокамера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, позволяющее выделить из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Системы аутентификации на основе анализа особенностей глаза обладают очень высокой точностью. Одним из преимуществ этого метода является то, что пользователям не нужно касаться никаких устройств в момент распознавания.

Метод распознавания по форме кисти руки

Принцип аутентификации по кисти руки человека поясняет рис. 3.2. С помощью системы зеркал, позволяющей получать трехмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), получают измерения, необходимые для получения уникального цифрового кода, идентифицирующего человека.

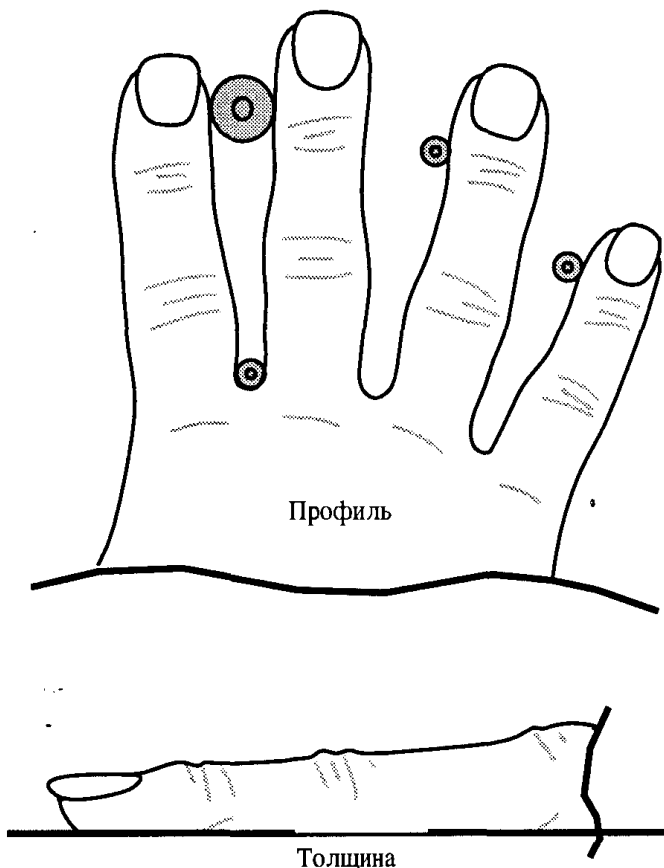


Рис. 3.2. Аутентификация по форме кисти руки

К примеру, Система *Digi-2* фирмы BioMet Partners, Inc. идентифицирует человека по форме и трехмерным характеристикам двух пальцев (указательного и среднего), расположенных в форме латинской буквы V.

Системы аутентификации по форме руки просты и удобны в эксплуатации. К недостаткам следует отнести меньшую, чем, например, у сканеров отпечатков пальцев, точность. Области применения – аутентификация посетителей в производственных помеще-

ниях, где из-за грязи затруднено применение сканеров отпечатков пальцев.

Несмотря на изменение формы кисти как с течением жизни человека, так и за относительно короткие сроки, практически постоянными остаются отношения размеров, форма пальцев, расположение суставов. В современных системах распознавания по форме руки применяется компенсация – образец (шаблон) корректируется при каждой успешной аутентификации.

Метод распознавания по отпечатку пальца

Устройства биометрической идентификации по отпечатку пальца работают на основании научно доказанного утверждения о том, что у разных людей не может быть одинаковых отпечатков пальцев (папиллярных узоров). При попытке субъекта получить доступ к объекту (пройти через дверь, турникет и т.п.) или просто сделать отметку в журнале о своем присутствии, устройство сравнивает сохраненный ранее шаблон с полученным образом отпечатка пальца, проверяя идентичность пользователя.

Проверка производится, когда пользователь или вводит ID номер или использует идентификационную карту (например, смарт-карту или другую карту доступа) с помощью Wiegand-считывателя, затем помещает палец на считывающий датчик для сравнения с сохраненным шаблоном. В результате этой операции получается некоторое число, которое показывает, насколько полученный образ совпадает с шаблоном. Если это число превышает некоторую фиксированную константу, называемую порогом безопасности, то субъект признается идентифицированным и ему разрешается доступ и/или делается запись в журнале (список событий). Порог безопасности в свою очередь определяет уровни ошибки первого рода FAR (False Accept Rate – вероятность того, что система идентифицирует подлинность отпечатка пользователя, не зарегистрированного в системе) и ошибки второго рода FRR (вероятность того, что система не идентифицирует подлинность отпечатка пальца зарегистрированного пользователя).

В настоящее время выделяют три класса алгоритмов сравнения отпечатков пальцев.

- 1) Корреляционное сравнение — два изображения отпечатка пальца накладываются друг на друга, и подсчитывается коэффициент корреляции (по уровню интенсивности) между соответствующими пикселями, вычисленная для различных выравниваний изображений друг относительно друга (например, путем различных смещений и вращений); по соответствующему коэффициенту принимается решение об идентичности отпечатков. Из-за сложности и длительности работы данного алгоритма, особенно при решении задач идентификации (сравнение «один-ко-многим»), системы на его основе сейчас практически не используются.
- 2) Сравнение по особым точкам — по одному или нескольким изображениям отпечатков пальцев со сканера формируется шаблон, представляющий собой плоскость, на которой выделены конечные точки и точки ветвления. На отсканированном изображении отпечатка также выделяются эти точки, их расположение сравнивается с шаблоном, и по количеству совпавших точек принимается решение по идентичности отпечатков. В работе алгоритмов данного класса реализуются механизмы корреляционного сравнения, но при сравнении положения каждой из предположительно соответствующих друг другу точек. В силу простоты реализации и скорости работы алгоритмы данного класса наиболее широко распространены. Единственный существенный недостаток данного метода сравнения — достаточно высокие требования к качеству получаемого изображения (500 точек на дюйм).
- 3) Сравнение по узору — в данном алгоритме сравнения используются непосредственно особенности строения папиллярного узора на поверхности пальцев. Полученное со сканера изображение отпечатка пальца разбивается на множество мелких ячеек (размер ячеек зависит от требуемой точности). Расположение линий в каждой ячейке описывается параметрами некоторой синусоидальной волны, т. е. задается начальный сдвиг фазы, длина волны и направление ее

распространения. Полученный для сравнения отпечаток выравнивается и приводится к тому же виду, что и шаблон. Затем сравниваются параметры волновых представлений соответствующих ячеек. Преимущество алгоритмов сравнения этого класса в том, что они не требуют изображения высокого качества.

Устройства, использующие описанные принципы биометрической идентификации человека, будут изучаться в данной лабораторной работе.

3.1 Описание объекта лабораторного исследования

В данном разделе описывается оборудование, используемое для выполнения лабораторной работы, и основные возможности этого оборудования.

3.1.1 Состав лабораторного стенда

При выполнении лабораторной работы используется следующее оборудование:

- УБИ Iris Camera BM-ET 300 AE фирмы Panasonic;
- УБИ ID3D HandKey фирмы Recognition Systems;
- УБИ FingerScan V20 фирмы Identix;
- компьютер с установленной ОС Windows XP, имеющий COM-порт и сетевую карту Ethernet;
- монитор;
- программное обеспечение администратора BM-ES300AE;
- программное обеспечение HandNet for Windows Version 2.0.0.23;
- программное обеспечение Fingerlan 4.6;
- адаптер DC-102 для подключения УБИ ID3D к ПК;
- проксимити-считыватель фирмы Keri Systems Inc.;
- проксимити-карты;
- 2 блока питания ББП-20 (220-12В);
- соединительные провода и кабели.

На рис. 3.3 – 3.5 представлены схемы лабораторных установок для изучения УБИ и методов их применения.

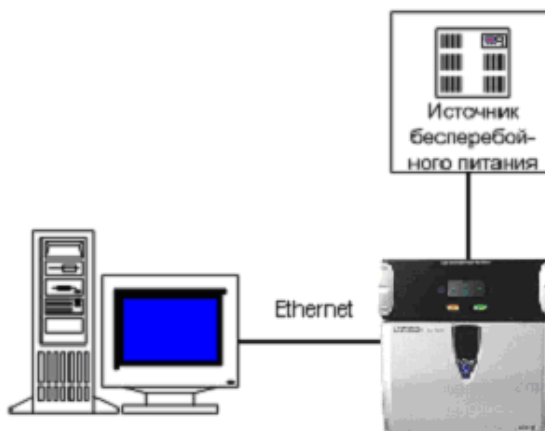


Рис. 3.3. Схема лабораторного стенда для изучения УБИ Iris Camera BM-ET 300 AE фирмы Panasonic

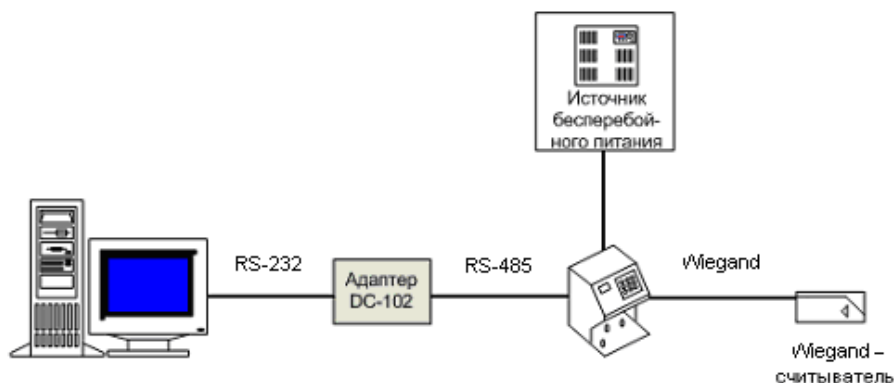


Рис. 3.4. Схема лабораторного стенда для изучения УБИ ID3D HandKey фирмы Recognition Systems

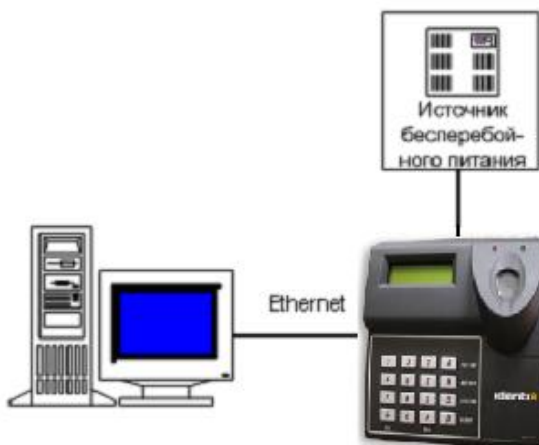


Рис. 3.5. Схема лабораторного стенда для изучения УБИ FingerScan V20 фирмы Idenix

3.1.2 Устройство биометрической идентификации с технологией распознавания радужной оболочки глаз Iris Camera BM-ET 300 AE фирмы Panasonic

УБИ Iris Camera BM-ET 300 AE фирмы Panasonic использует технологию анализа радужной оболочки человеческого глаза. Оно имеет следующие режимы работы и возможности.

Режим регистрации

Одним из режимов работы УБИ Iris Camera является режим регистрации – сканирование образа радужной оболочки глаза пользователя и регистрация его на сервере (ПК с программным обеспечением администратора BM-ES300AE). УБИ Iris Camera формирует данные о радужной оболочке из сканированных образов и передает их через локальную вычислительную сеть (ЛВС) в Сервер. После того как данные радужной оболочки попадают в Сервер, они регистрируются в базе данных. Существует возможность зарегистрировать до 5000 пользователей.

Для регистрации данных радужной оболочки глаза необходимо установить дополнительное программное обеспечение администратора BM-ES300AE и пользовательскую лицензию на программное обеспечение BM-EU30000E Series на ПК с установленной операционной системой семейства Microsoft Windows. Общее количество пользователей, которые могут быть зарегистрированы, зависит от приобретенной лицензии (100, 1000, 3000 или 5000). Работа с ПО BM-ES300AE описана в приложении Д.

Режим верификации

Основным режимом работы УБИ Iris Camera является режим верификации, в котором собственно и происходит распознавание человека (пользователя) по его образу радужной оболочки глаза. Данные 1000 пользователей могут храниться в памяти УБИ. Если данные о пользователе находятся в памяти УБИ, то процесс распознавания пользователя занимает около 1,5 с. Если соответствующих данных нет, то УБИ Iris Camera передает их в Сервер, который сравнивает переданные данные с данными, хранящимися в базе данных зарегистрированных пользователей (процесс занимает около 10 с). Пользователь может увидеть результат верификации на передней панели УБИ Iris Camera: в зависимости от результата подсвечивается один из индикаторов АСЦЕПТ/РЕЦЕПТ (Принять/Отклонить).

Время распознавания может отличаться в зависимости от условий сканирования. УБИ Iris Camera сканирует образ радужной оболочки обоих глаз одновременно, но данные радужной оболочки каждого глаза регистрируются отдельно. Также возможно провести регистрацию/распознавание, используя один глаз. Сканирование производится во время регистрации пользователя. Пользователь распознается по данным радужной оболочки любого глаза. До 256 УБИ Iris Camera (регистрации и распознавания) и сервер могут быть объединены в сеть по протоколу Ethernet.

Автоматическое управление. Голосовая и визуальная помощь пользователю в процедуре распознания

Когда пользователь находится в пределах 50 см перед УБИ Iris Camera, включается голосовое управление. Пользователю необходимо перемещается так, чтоб были видны оба глаза в зеркале, следуя указаниям голоса и индикаторов (стрелок, появляющихся на зеркале), образы радужных оболочек глаз пользователя будут просканированы автоматически, при этом пользователь должен находиться в 30 – 40 см от УБИ.

Встроенная камера видеонаблюдения

УБИ Iris Camera имеет встроенную цветную мини-видеокамеру. При использовании дополнительного оборудования (например, видеорегистратора) это позволяет делать запись лица пользователя. Можно записывать только пользователей, которые не были признаны, используя выход сигнала REJECT («Отклонить»).

Система контроля и управления доступом

УБИ Iris Camera поддерживает стандарт Wiegand, который является одним из распространённых интерфейсов, используемых в СКУД. Любое устройство, поддерживающее интерфейс Wiegand, может быть непосредственно связано с УБИ Iris Camera. С помощью УБИ Iris Camera и Сервера можно составить систему контроля и управления доступом, в которую также будут входить считыватель карт доступа, электрический замок или другое исполнительное устройство.

3.1.3 Устройство биометрической идентификации ID3D HandKey фирмы Recognition Systems

Считыватель ID3D HandKey фирмы Recognition Systems является устройством биометрической идентификации человека по форме руки (ширина ладони и пальцев в нескольких местах, длина, ширина и толщина пальцев).

Принцип действия УБИ ID3D HandKey следующий: рука освещается инфракрасными лучами, а установленная сверху видеока-

мера регистрирует ее вид. В поле зрения камеры оказывается также боковое зеркало, дающее представление о толщине ладони. При необходимости устройство может работать с частью кисти, если сканирование всей кисти невозможно (например, отсутствует палец).

Полученная электронная фотография кисти обрабатывается встроенным процессором считывателя, информация об особенностях формы кисти сжимается до 9 байт.

В режиме регистрации эта информация сохраняется в памяти считывателя, а также передаётся программному обеспечению HandNet и другим считывателям, правом прохода через которые наделяется пользователь – обладатель данной кисти. Общее время процедуры составляет от 10 с до 1 мин.

В режиме идентификации полученная информация о форме кисти руки сверяется с ранее сохранёнными данными, а также проверяется уровень полномочий для этого пользователя. Сохранённая информация о кисти корректируется при каждой успешной идентификации.

Идентификация пользователя

Проверка идентификации проходит по следующему алгоритму. Пользователь вводит свой ID-номер. Устройство проверяет существование такого номера в базе данных, и если этот номер есть, то «просит» поместить руку на специальную панель для снимка руки, в противном случае выдает звуковой сигнал об отказе в доступе. Идентификация может проходить от 1 до 3 раз за один сеанс (если полученная с первого раза информация о кисти руки сильно отличается от сохранённой в базе данных устройства). Если же устройство не идентифицировало руку пользователя, то происходит отказ в доступе (при этом может передаваться сигнал тревоги в цепь управления) и блокирование ID-номера (УБИ ID3D HandKey не реагирует на ввод этого ID-номера) до удачно прошедшей идентификации пользователя с другим ID-номером.

Необходимо отметить одну важную особенность УБИ ID3D HandKey. В случае, когда пользователь не может предоставить для проверки правую руку, он может использовать левую, положив ее

ладонью кверху. У большинства людей руки симметричны, если не было травм и все пальцы на месте. Для снижения несоответствия симметрии во время регистрации просят снимать кольца и другие предметы.

Поддержка стандартных интерфейсов

Поддерживается стандарт Wiegand. Любое устройство, поддерживающее интерфейс Wiegand, может быть непосредственно связано с УБИ ID3D HandKey.

Это может быть считыватель карт, и тогда поднесение карты к считывателю заменит ручной ввод ID-номера.

УБИ ID3D HandKey также можно подключить по протоколу Wiegand к контроллеру СКУД, и тогда с точки зрения контроллера УБИ будет функционировать как обычный считыватель.

Адаптер DC-102

Адаптер DC-102 используется для подключения УБИ ID3D HandKey к ПК. Данное устройство служит мостом между интерфейсами RS-232 и RS-485 (либо RS-422). На рис. 3.6 представлен вариант подключения сети УБИ ID3D HandKey к ПК.

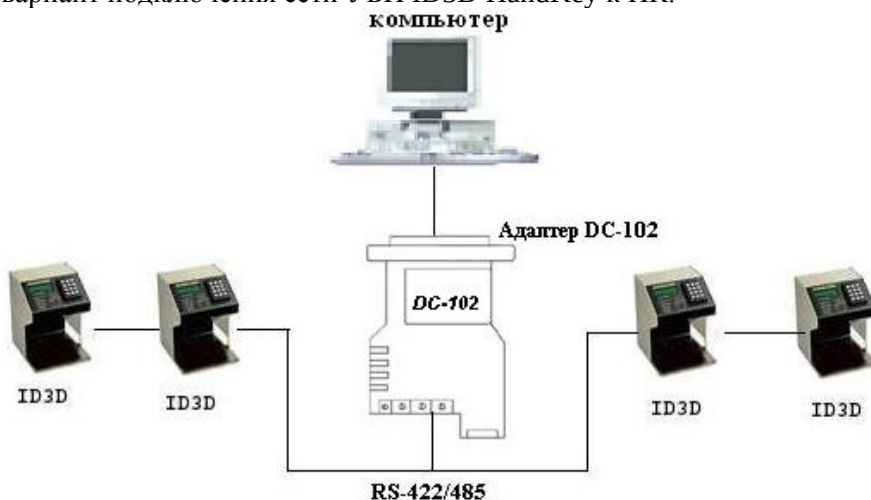


Рис. 3.6. Подключение УБИ ID3D HandKey к ПК

Программное обеспечение HandNet for Windows Version 2.0.0.23

Программное обеспечение (ПО) HandNet for Windows Version 2.0.0.23 предназначено для управления сетью УБИ ID3D HandKey. Установив данное ПО на ПК, можно в масштабе реального времени осуществлять мониторинг большого количества точек доступа. Удаленные точки доступа контролируются посредством модема или сети Ethernet. УБИ ID3D HandKey может выполнять функции контроллера СКУД, поэтому, подключив компьютер, можно создать полноценную систему контроля и управления доступом (естественно, при использовании исполнительных механизмов).

Обеспечивается полный мониторинг состояния точек доступа в масштабе реального времени, а также удаленный контроль и отслеживание несанкционированных действий. Если связь с центральным компьютером была потеряна, то каждая из точек доступа системы продолжает работать автономно.

Основные характеристики ПО HandNet

Из характеристик ПО HandNet for Windows Version 2.0.0.23 необходимо отметить следующие:

- мониторинг (наблюдение, отслеживание ситуации) более 1000 устройств биометрической идентификации ID3D в реальном времени;
- администрирование до 100000 пользователей. Добавление, удаление и отслеживание пользователей с компьютере. Местонахождение пользователей отслеживается посредством пользовательского окна, в котором отражается информация о последнем использованном считывателе, а также дата и время использования;
- автоматическое управление шаблонами руки. Регистрация пользователей может проводиться посредством любого УБИ, подключенного к сети. Данные о шаблоне автоматически сохраняются на компьютере и в соответствии с командой передаются на выбранные точки доступа системы;
- уполномоченные операторы могут открыть любую дверь;

- нет потребности в выделенном компьютере. Пока на компьютере выполняются другие задачи, ПО HandNet for Windows Version 2.0.0.23 может работать на заднем фоне;
- возможность назначения 60 временных зон с четырьмя интервалами для каждой из них. Может быть задано неограниченное число режимов доступа. Таблица праздников поддерживает неограниченный список;
- автоматическое архивирование списка событий. Можно задать процесс архивирования на основе размера файла, временного периода или дня месяца;
- специализированные отчеты о деятельности. Источником могут быть либо текущие, либо заархивированные данные.

3.1.4 Устройство биометрической идентификации FingerScan V20 фирмы Identix

УБИ FingerScan V20 фирмы Identix предназначено для контроля доступа в помещение путем идентификации личности по отпечатку пальца. Проверка производится, когда пользователь или вводит ID номер, или использует идентификационную карту (например, смарт-карту или другую карту доступа) с помощью Wiegand-считывателя, затем помещает палец на считывающий датчик для сравнения с сохраненным шаблоном. В результате этой операции получается некоторое число, которое показывает, насколько полученный образ совпадает с шаблоном. Если это число превышает некоторую фиксированную константу, называемую порогом безопасности, то субъект признается идентифицированным и ему разрешается доступ и/или делается запись в журнале (списке событий).

Порог безопасности, в свою очередь, определяет уровни ошибки первого рода FAR (False Acceptance Rate – вероятность того, что система идентифицирует подлинность отпечатка пользователя, не зарегистрированного в системе) и ошибки второго рода FRR (False Rejection Rate – вероятность того, что не идентифицирует подлинность отпечатка пальца зарегистрированного пользователя).

Если упомянутое число меньше порога безопасности, пользователю будет предложено сделать повторную попытку считывания отпечатка пальца, либо, если количество допустимых попыток исчерпано (по умолчанию их 3), отказать в доступе. При этом в журнале также может быть сделана соответствующая запись.

Для того чтобы пользователь мог получать доступ или отмечаться в журнале, он должен быть предварительно зарегистрирован в базе данных устройства. Перед регистрацией отпечатка пальца пользователю присваивается его личный ID-номер. Этот номер используется, чтобы определить, с каким шаблоном изображения отпечатка пальца из базы данных сравнивать полученное изображение при каждой следующей аутентификации.

Затем регистрируемый пользователь должен приложить палец к оптическому сенсору для получения изображения, которое в дальнейшем будет использоваться как шаблон.

Уровни полномочий

При регистрации сотруднику присваивается уровень полномочий. УБИ Fingerscan V20 имеет четыре уровня полномочий:

- *Пользователи* – люди, которые должны быть идентифицированы, чтобы получить доступ к объекту или отметить их присутствие;
- *Регистраторы (Enrollers)* – пользователи, которые уполномочены регистрировать новых пользователей в системе и создавать шаблоны отпечатков пальцев для сохранения в базе данных;
- *Супервизоры* имеют статус Регистратора и могут изменять настройки системы, устанавливать временные зоны, изменять установки тревог, добавлять и удалять шаблоны;
- *Менеджеры* – пользователи с доступом ко всем функциям системы. Менеджер может сбросить все настройки системы (стереть все данные) и запретить менять Супервизору настройки. Менеджер не может быть удален из системы за исключением сброса всей системы или удаления другим Менеджером. Менеджеры не могут удалять себя из системы.

Это условие гарантирует, что в системе есть по крайней мере один пользователь со статусом Менеджера.

Некоторая информация, хранящаяся в базе данных, может быть изменена Менеджерами, Супервизорами или Регистраторами. В частности, можно изменить уровень полномочий конкретного пользователя, однако производящий такую операцию не может присвоить уровень выше своего. Также можно полностью удалить пользователя из базы данных.

Шаблоны отпечатка пальца

Шаблоны обычно хранятся в базе данных шаблона (в УБИ Fingerscan), но могут быть сохранены в другом месте – на персональном компьютере, смарт-карте или любом другом подходящем носителе. Внешнее хранение шаблона может как дополнять, так и заменять базу данных устройства. Шаблоны могут храниться в базе данных двумя способами в зависимости от преследуемых целей. Первый способ основан на точках миниатюр (используется по умолчанию) и отличается меньшей базой данных и более быстрой регистрацией пользователей; второй способ основан на методе корреляций и сохраняет совместимость с базами данных предыдущих версий УБИ Fingerscan. Способ хранения шаблонов влияет также на процесс регистрации новых пользователей. При регистрации пользователя и создании шаблона производится оценка качества последнего. Однако решение о пригодности к использованию данного шаблона зависит от используемого способа хранения в базе данных.

Связь с внешними устройствами

УБИ Fingerscan V20 имеет три коммуникационных порта, любые два из которых могут использоваться в одно и то же время (один как основной порт и один как дополнительный). Настройка основного канала позволяет УБИ Fingerscan V20 обмениваться данными, в том числе и в сети стандарта RS-485. Настройка вспомогательного канала требуется при необходимости использования второго порта. Если основной канал подключен к RS-485 порту, то RS-232 порт доступен как вспомогательный порт для связи.

Подсоединив принтер к УБИ Fingerscan V20 можно распечатывать события системы. Опция печатания списка событий из журнала позволяет пользователю выбрать, какие события печатать: либо все события с момента последней распечатки, либо события с определенным порядковым номером.

Временные зоны

Есть возможность усилить ограничения по доступу пользователям, используя временные зоны. Временные зоны – это интервалы времени, прикрепляемые к учетным записям пользователей, в течение которых они могут получить доступ. За исключением этих временных зон, доступ запрещен. В УБИ Fingerscan V20 может быть определено до тридцати глобальных временных зон. Каждому пользователю может быть назначено до двух временных зон.

Если создана временная зона по умолчанию, всем новым пользователям назначается эта зона. Кроме того, пользователю может быть дополнительно назначена еще одна временная зона.

Установки безопасности

К установкам безопасности УБИ Fingerscan V20 относятся порог безопасности и количество идентификаций для получения доступа. При использовании этой функции для получения доступа потребуется распознать заданное количество сотрудников вместо одного. Также можно изменять порог безопасности. Порог безопасности – число, которое определяет степень, с которой можно быть уверенным, что идентифицируемый действительно является тем, за кого он себя выдает. По умолчанию порог безопасности равен 50. Изменять его можно в пределах от 0 до 200. Каждому новому регистрируемому назначается этот уровень. В табл. 3.1 указаны рекомендуемые уровни порога безопасности в зависимости от требований ситуации.

Таблица 3.1. Рекомендуемые настройки порога безопасности УБИ Fingerscan V20

Требования ситуации	Рекомендуемый уровень	
	Алгоритм с точками миниатюр	Алгоритм методом корреляции
Высокая пропускная способность, умеренный уровень безопасности	30-40	50-80
Коммерческий, промышленный уровень безопасности	40-50	~100
Высокий уровень безопасности	>70	125

Необходимо отметить, что за одним ID-номером может быть зарегистрировано до трех шаблонов отпечатков пальца пользователя. Лучше, когда на каждой руке зарегистрировано по пальцу, тогда, если пользователь повредил зарегистрированный палец (руку), можно использовать дополнительный шаблон пальца. Сам ID-номер может иметь до девяти разрядов. Длина по умолчанию – четыре разряда. У всех пользователей длина ID номера должна быть одинакова. При необходимости к номеру могут быть спереди добавлены нули.

Исполнительные входы и выходы

Каждое УБИ Fingerscan V20 имеет четыре релейных входа и выхода для связи с периферийными устройствами. Входы могут использоваться для создания записей в журнале событий УБИ. Обычно входы используются вместе с датчиками состояния двери, вызывающими тревоги. Например, датчик состояния двери может быть использован, чтобы в случае, если она оставалась открытой слишком долго, выработать сигнал тревоги.

Выходы могут использоваться, чтобы включить внешние устройства типа тревоги или устройства дозвона. Все входы и выходы имеют заводскую установку на нормально открытый контакт (НОК), но при необходимости любой из них может быть перепрограммирован на нормально замкнутый (НЗК).

Программное обеспечение Fingerlan 4.6 фирмы Identix

Специальное программное обеспечение компании Identix позволяет организовать централизованную систему контроля доступа, которая может объединять несколько биометрических считывателей. Управление и настройка всех устройств осуществляется с одного компьютера. При этом зарегистрировать шаблон отпечатка пальца можно на любом УБИ Fingerscan V20 системы. После сканирования пальца нового сотрудника оператор задает адреса считывателей, на которые записывается данный шаблон. Контроль доступа удаленных объектов с использованием биометрического считывателя Fingerscan V20 возможен посредством модемной связи или по сети Ethernet.

Функциональные возможности

ПО Fingerlan 4.6 – система управления доступом высокого уровня, которая позволяет управлять сетью устройств Identix Fingerscan V20 с помощью одного компьютера. Данный программный продукт обеспечивает следующие функциональные возможности:

- конфигурирование и управление сетью УБИ Fingerscan V20;
- управление правами доступа пользователей;
- управление уровнями полномочий пользователей;
- хранение протокола событий;
- управление базой данных пользователей, содержащей пользовательскую информацию и шаблоны отпечатков пальцев;
- управление и синхронизация хранения шаблонов отпечатков пальцев на ПК и УБИ Fingerscan V20;
- обеспечивает наблюдения за работой подключённых устройств в реальном масштабе времени.

3.2 Порядок выполнения работы

1. Теоретически изучить возможности лабораторного оборудования.

УБИ Iris Camera

2. Изучить возможности голосовой помощи УБИ Iris Camera.
3. Ознакомиться с возможностями встроенной камеры видеонаблюдения УБИ Iris Camera.
4. Изучить программное обеспечение администратора BM-ES300AE для Iris Camera BM-ET 300 AE фирмы Panasonic.
5. Зарегистрировать пользователей. Какие трудности возникли при регистрации? Что мешало осуществлению регистрации (отразить это в отчете)?
6. Пройти процедуру идентификации пользователей.

УБИ ID3D

7. Изучить программное обеспечение HandNet for Windows Version 2.0.0.23.
8. Добавить пользователя и назначить уровень доступа к УБИ ID3D.
9. Пройти идентификации в УБИ ID3D.
10. Изучить настройки временных зон УБИ ID3D.
11. Изучить функцию прохода по принуждению.
12. Создать специализированные отчеты о настройке УБИ.

УБИ Fingerscan V20

13. Изучить программное обеспечение Fingerlan 4.6 фирмы Identix.
14. Зарегистрировать пользователей.
15. Изучить функции порога безопасности. Что происходит при его изменении?
16. Изучить функцию «количество идентификаций для получения доступа» (правило 2-х, 3-х лиц).
17. Зарегистрировать несколько пальцев на один ID. Изучить возможность применения альтернативных шаблонов.

3.3 Контрольные вопросы

1. На каких УБИ можно реализовать функцию нескольких идентификаций?
2. Возможно ли объединение УБИ в «сеть»?
3. Что необходимо для построения «сети» УБИ?

4. Какие специальные функции можно реализовать в «сети» УБИ?
5. Дополнительные функции УБИ относительно считывателей СКУД.
6. Как можно сократить время идентификации пользователей?
7. В системах распознавания по форме руки применяется компенсация. Что это и на чем она основывается?
8. Какие классы алгоритмов сравнения отпечатков пальцев существуют?
9. Какова область применения УБИ? На чем основывается выбор в пользу конкретного способа биометрической идентификации?
10. Что такое ошибки первого и второго рода?

Список литературы

1. Administration Software User's Manual Model No BM-ES300AE. Panasonic.
2. Iris Camera Software Installation Guide Model No BM-ET300AE. Panasonic.
3. Iris Camera Setup Manual Model No BM-ET300AE. Panasonic.
4. HandNet User Guide for Windows. Recognition Systems.
5. Fingerscan V20 User's Guide. Identix.
6. Fingerlan 4.6 User's Guide. Identix.
7. Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов. М.: МИФИ, 2008. 584 с.

Приложение Д

ОПИСАНИЕ РАБОТЫ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ АДМИНИСТРАТОРА VM-ES300AE ДЛЯ IRIS CAMERA VM-ET 300 AE ФИРМЫ PANASONIC

При входе в программное обеспечение администратора перед вами появляется окно главного меню, в центре которого расположены пять кнопок (табл. Д1).

Таблица Д1. Главное меню программного обеспечения администратора

Визуальное представление	Название кнопок
	Информация о пользователях
	Настройки и обслуживание камер
	Информация о событиях
	Резервирование и восстановление
	Настройки системы

При щелчке по кнопке «Информация о пользователях» появляется одноименное окно (рис. Д1), в котором можно выделить четыре области:

- «User Search» («Поиск пользователей»);
- «User List» («Список пользователей»);
- блок кнопок для работы со списком пользователей;
- расположенная отдельно кнопка «Close» («Заккрыть») предназначена для выхода из этого окна.

Блок «User Search» («Поиск пользователей») предназначен для поиска в базе данных пользователей, удовлетворяющих неким критериям. Список критериев приведён в табл. Д2. После ввода критериев необходимо нажать кнопку «Search» («Искать») и список пользователей появится в блоке «User List» («Список пользователей»). Кнопка «Clear» («Очистить») предназначена для очистки всех полей ввода критериев поиска. При поиске с незадаанными критериями будет выведен список всех пользователей.

The screenshot shows a software window titled "User Information". It is divided into several functional areas. The top section, "User Search", contains input fields for "User ID:", "Name:", "Card ID:", "Group:", "Department:", and "Camera:". There are "Search" and "Clear" buttons below these fields. The "Group:" and "Camera:" fields have "Select" buttons next to them. Below the search section is a "User List" section which contains a table with the following headers: "User ID", "Name", "Iris Data", "Group", and "Department". The table body is currently empty. At the bottom of the window, there is a row of buttons: "New", "Details", "Delete", "Import", "Export", "Select All", "Clear All", and a "Close" button in the bottom right corner.

Рис. Д1. Окно информации о пользователях

Таблица Д2. Критерии поиска пользователей

Название критерия	Описание
User ID	Идентификатор пользователя
Name	Имя пользователя
Card ID	Код карты пользователя (например, проксимити)
Group	Группы, к которым принадлежит пользователь
Department	Отдел, в котором работает пользователь
Camera	Пользователи, занесённые в заданные УБИ Iris Camera

В блоке «User List» («Список пользователей») выводятся результаты поиска в виде таблицы. Значения колонок этой таблицы соответствуют критериям поиска (табл. Д2). Также в этом блоке находятся две кнопки для работы со списком:

- «Select All» («Выбрать всех») – для выбора всех пользователей в таблице;
- «Clear All» («Очистить всё») – для снятия выделения со всех пользователей в таблице.

Кнопки описаны в табл. Д3.

Таблица Д3. Описание кнопок для работы со списком пользователей

Название кнопки	Перевод на русский язык	Описание
Delete	Удалить	Удаляет пользователей, выбранных в списке пользователей
Details	Детализация	Показывает подробную информацию о пользователях, которые в этот момент показаны в списке пользователей
Export	Экспортировать	Экспортирует информацию о пользователях в файл или другие серверы
Import	Импортировать	Импортирует пользовательскую информацию из файла в пакет регистрационной информации. Эта функция также используется, чтобы импортировать пользовательскую информацию из других серверов системы
New	Новый	Регистрация нового пользователя

Регистрация пользователей

Для регистрации нового пользователя нужно нажать кнопку «New» («Новый») в форме «User Information» («Информация о пользователях»), появится форма регистрации новых пользователей («New User Enrollment»). Вид ее представлен на рис. Д2.

В табл. Д4 описаны поля формы «New User Enrollment» («Регистрация нового пользователя»).

The screenshot shows a software window titled "New User Enrollment". It features two tabs: "Information" and "Image". The "Information" tab is active and contains the following fields:

- User ID: [text input]
- Name: [text input]
- Group: [text input] with a "Select Group" button below it.
- Card ID: [text input]
- Site Code: [text input]
- User Code: [text input]
- Department: [text input]
- Telephone: [text input]
- Facsimile: [text input]
- E-mail Address: [text input]
- Memo: [text input]

Below the "Information" tab is an "Iris" section. It includes "Iris Data:" followed by a red box containing the text "No Image Captured". To the right of this are two buttons: "Capture" (with an eye icon) and "Clear" (with a trash can icon).

At the bottom of the window are two buttons: "Enroll" (with a floppy disk icon) and "Cancel" (with an 'X' icon).

Рис. Д2. Форма регистрации нового пользователя

Таблица Д4. Описание полей формы «New User Enrollment» («Регистрация нового пользователя»)

Название полей формы	Перевод на русский язык	Описание полей формы
User ID	Код пользователя	Можно ввести до 16 алфавитно-цифровых знаков. Нельзя использовать следующие символы: \, /, :, ,, ;, *, <, >, ?. Нельзя также использовать тот же код, что и у зарегистрировано ранее пользователя
Name	Имя	Используется для ввода имени пользователя. Можно ввести не более 20 символов
Group	Группа	Список групп доступа, к которым принадлежит пользователь. Выбор групп осуществляется в окне, появляющемся при нажатии кнопки «Select Group» («Выбрать группу»)
Card ID	Код карты	У всех пользователей должно быть одинаковое количество цифр в полях «Site Code» («Код местоположения») и «User Code» («Код пользователя»). Код карты регистрируется также, если поле «Site Code» будет пустым. Нельзя использовать тот же номер карты, что и у ранее зарегистрированного пользователя
Department	Отдел	Отдел, где работает пользователь
Telephone	Телефон	Номер телефона пользователя
Facsimile	Факс	Номер факса пользователя
E-mail Address	Адрес электронной почты	Адрес электронной почты пользователя
Memo	Дополнительная информация	Дополнительная информация о пользователе

Продолжение табл. Д4

Название полей формы	Перевод на русский язык	Описание полей формы
Iris Data	Данные радужной оболочки	Показывает статус сканирования данных радужной оболочки. Цвет фона изменяется соответственно статусу «захвата»: • Нет отсканированного образа (красный фон). Образ радужной оболочки еще не отсканирован; • Образ отсканирован/ не зарегистрирован (желтый фон). Образ радужной оболочки был снят, но пока не занесен в информацию о пользователе. Если возвратиться к форме «User Information» («Информация о пользователях»), то образ радужной оболочки будет отвергнут; • Зарегистрирован (голубой фон). Радужная оболочка была отсканирована и зарегистрирована в данных о пользователе
Capture	Сканирование	Сканирование образа радужной оболочки. Для того чтобы кнопка «Capture» стала активной, надо установить камеру для регистрации (см. пункт «Установка камеры для регистрации»)
Enroll	Регистрация	Регистрация пользователя

Поля, названия которых написаны синим шрифтом, являются обязательными для регистрации пользователя.

Сканирование образа радужной оболочки

Перед тем как начать сканирование радужной оболочки, необходимо выбрать камеру для регистрации (см. пункт «Установка камеры для регистрации»).

Нажмите кнопку «Capture» («Сканировать»). Перед вами появится сообщение «Capturing of the iris image has started» («Началось сканирование радужной оболочки глаз»). При выводе сообщения «Do you want to save this iris image?» («Вы хотите сохранить этот образ радужной оболочки глаз?») нажмите «Yes» («Да»).

Когда появится сообщение «The camera will capture four iris images. Please wait for a while» («Пожалуйста, подождите, пока камера сфотографирует четыре образа радужной оболочки глаз»), встаньте перед камерой, и сканирование начнется. Смотрите в камеру не мигая, пока не будут взяты четыре образа.

Проверьте показанный результат. Если сканирование было успешным, то образ радужной оболочки может быть зарегистрирован. Если сканирование было неудачным, то появится сообщение о его повторном прохождении. Для этого нажмите «Recapture» («Пересканировать»). Повторите процедуру, пока не появится сообщение на зеленом фоне для обоих глаз «Capturing of iris image is complete. (excellent)» («Сканирование образов радужных оболочек глаз выполнено (отлично)»).

После этого нажмите кнопку «Enroll» («Зарегистрировать»). Появится сообщение, что процедура сканирования образа радужной оболочки глаз завершена. Нажмите «Ok» для продолжения – это вернет вас к форме «New User Enrollment» («Регистрация нового пользователя») (или «User Information Details»). В поле «Iris Data» («Данные о радужных оболочках») появится сообщение на желтом фоне «Image captured/Unenrolled» («Образ отсканирован/Незарегистрирован»). Нажмите кнопку «Enroll» («Зарегистрировать») или «Update» («Обновить»), чтобы зарегистрировать образ радужной оболочки.

Процедура регистрации нового пользователя полностью завершена.

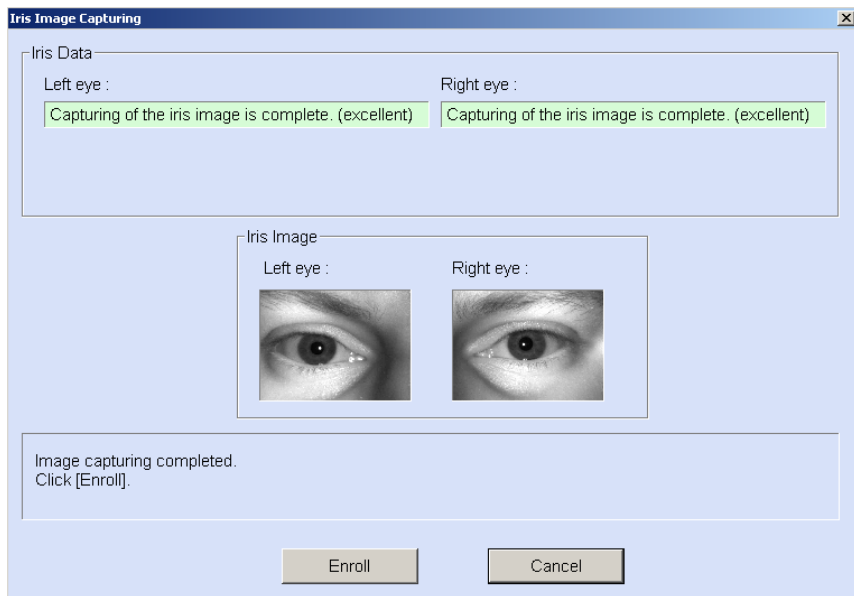


Рис. Д3. Пример успешного сканирования

Установка камеры для регистрации

В главном меню нажмите кнопку «Environment Settings» («Установки оборудования»), перед вами откроется одноимённое меню. В табл. Д5 представлено краткое описание меню «Environment Settings» («Установки оборудования»).

Таблица Д5. Описание меню Environment Settings

Визуальное представление	Название кнопок
	Настройки групп
	Настройки электронной почты
	Настройки безопасности сетевого окружения
	Настройки автоматической перезагрузки
	Информация об операторах системы

Продолжение табл. Д5

Визуальное представление	Название кнопок
	Настройки УБИ по умолчанию
	Настройки УБИ для регистрации пользователей

Далее нажмите кнопку «Enrollment Camera Settings» («Настройка УБИ для регистрации пользователей»). Появится форма выбора камеры для регистрации.

В поле «Use Enrollment Camera» («УБИ, используемое для регистрации») нажмите «Select» («Выбрать»), чтобы выбрать нужное УБИ (в данной лабораторной работе оно одно). Нажмите «Ok» для подтверждения изменений. Перед вами появится сообщение «The enrollment camera is set» («Камера для регистрации установлена»), нажмите «Ok» – это закроет текущее окно.

После того как камера установлена, она работает только для регистрации новых пользователей (сканирования образов радужной оболочки) и не может быть использована для идентификации пользователей. Для того чтобы камера стала работать для распознавания, надо выбрать другую камеру для регистрации или убрать совсем в установках камеру для регистрации (например, если камера всего одна). Для этого в окне «Enrollment Camera Settings» («Настройка УБИ для регистрации пользователей») нужно нажать кнопку «Clear» («Очистить») и «Ok». После этого камера вновь работает для идентификации пользователей.

Приложение Е

ОПИСАНИЕ РАБОТЫ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ HANDNET FOR WINDOWS VERSION 2.0.0.23 ФИРМЫ RECOGNITION SYSTEMS

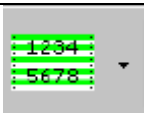
Для удобства работы с программой HandNet часто используемые функции выведены на инструментальную панель. Ее вид представлен на рис. Е1.



Рис. Е1. Инструментальная панель программы HandNet

В табл. Е1 рассмотрены функции кнопок инструментальной панели.

Таблица Е1. Функции кнопок инструментальной панели

Визуальное представление	Описание кнопки
	Если данная кнопка видна на инструментальной панели, администратор не зарегистрировался (не запущен сеанс администратора) в HandNet. Чтобы зарегистрироваться, необходимо щелкнуть по этой кнопке. Без регистрации невозможно будет вносить какие-либо изменения, можно только просмотреть основную информацию
	После регистрации кнопка «Login» («Зарегистрироваться») изменяется на «Logout» («Выйти»). Кнопка «Logout» завершает сеанс и позволяет предотвратить несанкционированные изменения в момент отсутствия администратора на рабочем месте
	Позволяет создавать проверочные отчеты о событиях системы

Продолжение табл. Е1

Визуальное представление	Описание кнопки
	Эта кнопка отвечает за архивирование старых событий системы
	Открывает окно событий. Окно событий выводит список всех действий HandNet и тревог от каждого УБИ
	Эта кнопка открывает окно пользователей. Выводится список каждого, кто потенциально способен получить доступ к УБИ
	Открывает окно локальной сети. Окно локальной сети выводит список всех контрольных точек доступа и УБИ и показывает их текущий статус
	Эта кнопка отправляет к настройкам профиля доступа. Профили доступа позволяют управлять, к каким считывателям и когда различные типы пользователей имеют доступ
	Эта кнопка отправляет к настройкам доступа в выходные дни
	Эта кнопка отправляет к настройкам временных зон
	Эта кнопка вызывает функцию помощи при работе с HandNet

Все функции по работе с программой доступны из главного меню. На рис. Е2 представлено главное меню HandNet.



Рис. E2. Главное меню

В табл. E2 кратко рассмотрены разделы главного меню.

Таблица E2. Описание разделов главного меню

Название разделов	Перевод на русский язык	Описание разделов
Site	Контрольная точка доступа	Позволяет добавлять и изменять настройки контрольных точек доступа
Reader	Считыватель (УБИ)	Позволяет добавлять, удалять и переименовывать считыватели в локальной сети HandNet. Также можно отпирать, запирасть и блокировать выбранный считыватель, регистрировать пользователя в выбранном считывателе, активировать и деактивировать дополнительные устройства, загружать время, временные зоны, пользователей и конфигурацию установок в выбранное УБИ
User	Пользователь	Позволяет добавлять, удалять и переименовывать пользователей, изменять информацию выбранного пользователя и предусмотреть вводимые данные, чтобы собрать дополнительную информацию о пользователях
View	Представление	Позволяет открывать окно пользователей, событий и локальной сети. Также позволяет включать или выключать панель инструментов. И также позволяет добраться до профиля доступа, праздников, фильтров событий, временных зон и системных настроек

Продолжение табл. Е2

Название разделов	Перевод на русский язык	Описание разделов
Window	Окно	Позволяет переключаться между открытыми окнами, плиткой горизонтально расположенных открытых окон на экране или включать панель в пределах окна локальной сети
Help	Помощь	Позволяет вызвать функцию помощи

Ниже описаны основные приёмы работы с программой.

Добавление пользователей

На рис. Е3 показано окно «Users» («Пользователи»). В этом окне выводится список пользователей, зарегистрированных в Hand-Net. Чтобы открыть это окно, выберите пункт «Users» («Пользователи») в меню «View» («Представление») или нажмите комбинацию клавиш CTRL-U.

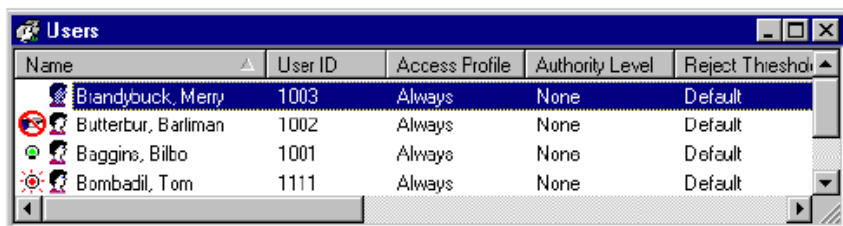


Рис. Е3. Окно пользователей

В табл. Е3 дано описание символов, отображающих статус пользователя. В табл. Б4 приведено описание колонок таблицы пользователей.

Таблица Е3. Иконки слева от имени пользователя

Иконка	Описание
	Если слева ничего нет, то пользователь зарегистрирован и может использовать любой считыватель, разрешенный его профилем доступа
	Перечеркнутая рука – данное изображение показывает, что пользователь еще не зарегистрирован, и, следовательно, не будет иметь доступ ни к одному считывателю. Вы должны зарегистрировать пользователя, чтобы дать ему доступ
	Зеленая лампочка показывает, что пользователь в настоящее время имеет доступ, и что функция ограниченного доступа была использована, так что этот доступ автоматически истечет в некоторый момент
	Черный сигнал показывает, что функция ограниченного доступа была использована, чтобы установить начало и конец времени доступа пользователя, и пользователь не имеет доступ, потому что установленное время для доступа еще не началось
	Красный показывает, что функция ограниченного доступа была использована, чтобы установить начало и конец времени доступа пользователя, и пользователь не имеет доступ, потому что установленное время для доступа уже истекло

Таблица Е4. Колонки информации в окне «Users» («Пользователи»)

Название колонки	Перевод на русский язык	Описание колонки
Name	Имя	Полное имя пользователя
User ID	ID номер пользователя	ID номер пользователя должен быть введен для получения доступа
Access Profile	Профиль доступа	Профиль определяет, к каким УБИ пользователь имеет доступ. Профиль доступа настраивается в меню View, используя Access Profiles. Вы можете изменить профиль доступа пользователей на закладке Security в User/Properties
Authority Level	Уровень полномочий	Показывает, разрешен ли пользователю доступ в командное меню УБИ. Вы можете изменить уровень полномочий пользователей на закладке Security в User/Properties

Продолжение табл. Е4

Название колонки	Перевод на русский язык	Описание колонки
Reject Threshold	Порог отклонения	Порог отклонения управляет, на сколько точно рука пользователя должна соответствовать сохраненному профилю для получения доступа. Если стоит Default, тогда HandNet использует значение параметра «Порог отклонения» («Reject Threshold») на вкладке «Конфигурация» («Configuration») в окне «Свойства УБИ» («Reader Properties»). Если стоит Default со звездочкой, это значит, что пользователю не нужно распознавать руку, чтобы получить доступ, потому что он был настроен со специальной регистрацией. Либо может стоять числовое значение. Более низкое число требует очень точного совпадения для получения доступа, высокое число требует, чтобы рука совпадала менее точно, 250 – самое высокое
Last Site	Последняя точка доступа	Регистрирует последнюю точку доступа, через которую пользователь прошел
Last Reader	Последнее УБИ	Регистрирует последнее УБИ, которое использовал пользователь
Last Time Used	Время последнего использования	Показывает дату и время последнего прохода
Limited State	Состояние ограничений	Unlimited – для пользователей, у которых нет ограничения в допуске по времени прохода. Для пользователей, которые имеют ограничения по времени прохода, имеются три позиции: Waiting – если период для прохода еще не начался, Limiting – если пользователю в настоящее время разрешен проход, Expired – если отведенное время для прохода истекло

Окончание табл. Е4

Название колонки	Перевод на русский язык	Описание колонки
Limited Start Time	Время начала ограничения	Если пользователь имеет ограничение на проход во времени, то это поле показывает дату и время момента, с которого пользователь получает разрешение на проход. До этого момента HandNet не позволит осуществить проход. Для других пользователей это поле будет пустым
Limited End Time:	Время окончания ограничения	Если пользователь имеет ограничение на проход во времени, то это поле показывает дату и время момента, до которого пользователь имеет разрешение на проход. После этого момента HandNet не позволит осуществить проход. Для других пользователей это поле будет пустым

Добавления пользователей без использования ПО

Изначально ПО HandNet настроено только на возможность добавлять пользователей с использованием ПО УБИ. Если вы хотите добавить и зарегистрировать нового пользователя в УБИ без добавления его сначала в программу:

1. Зайдите в меню «View» («Представление»).
2. Выберите пункт «Settings» («Настройки»).
3. Откройте вкладку «Security» («Безопасность») (рис. Е3).
4. Проверьте элемент «Do not delete unauthorized enrollments» («Не удалять неавторизованные регистрации»).
5. Под ним указывается, какой профиль доступа должен быть дан пользователю, который добавлен в УБИ.
6. Нажмите кнопку «Ok» внизу формы.

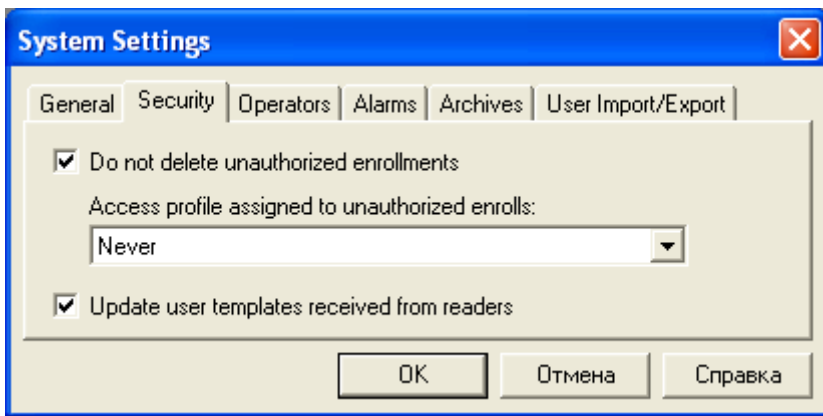


Рис. Е4. Настройка раздела безопасности

Добавление одного нового пользователя с использованием HandNet

1. В меню «User» («Пользователь») выберите «Add New» («Добавить нового»). Это откроет форму «New User Wizard» («Мастер добавления пользователя») (рис. Е5).

2. Автоматически будет выбрано «Add a single new user» («Добавить одного нового пользователя»), нажмите кнопку «Далее>» для продолжения.

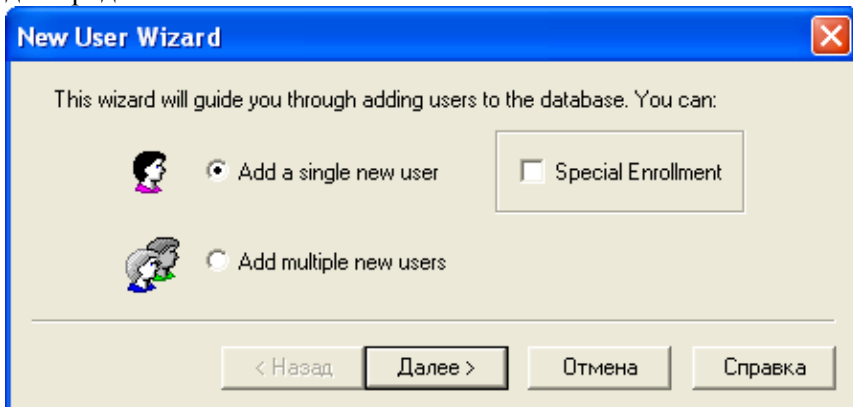
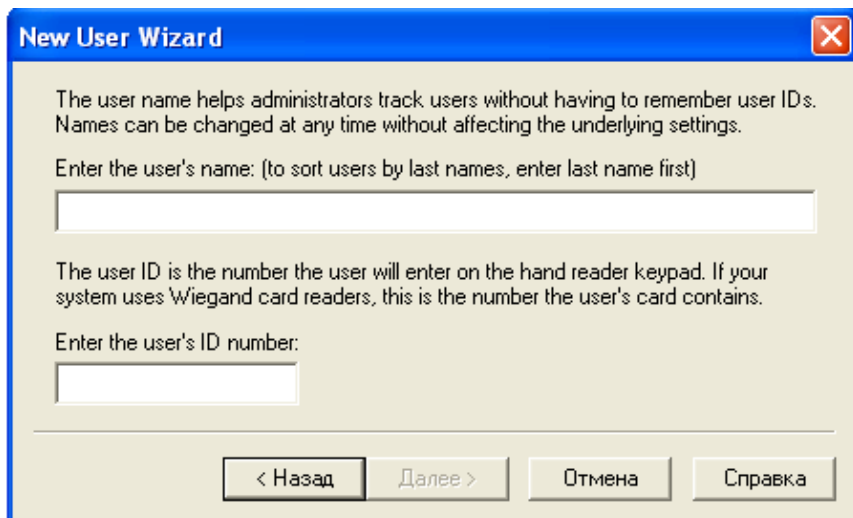


Рис. Е5. Добавление нового пользователя

3. Введите имя пользователя и номер ID (рис. Е6), которые вы присваиваете данному пользователю, нажмите кнопку «Далее>» для продолжения.



New User Wizard

The user name helps administrators track users without having to remember user IDs. Names can be changed at any time without affecting the underlying settings.

Enter the user's name: (to sort users by last names, enter last name first)

The user ID is the number the user will enter on the hand reader keypad. If your system uses Wiegand card readers, this is the number the user's card contains.

Enter the user's ID number:

< Назад Далее > Отмена Справка

Рис. Е6. Окно ввода имени и идентификационного номера пользователя

4. Выберите профиль доступа, уровень полномочий и другие настройки безопасности (рис. Е7). После настройки параметров нажмите «Готово».



Рис. Е7. Окно настройки безопасности

5. Вы добавили пользователя, но вы должны зарегистрировать пользователя, до того как пользователь будет иметь доступ.

Регистрация пользователей

До того как пользователь будет иметь доступ к УБИ, вы должны добавить пользователя в УБИ и создать шаблон руки пользователя. Перед тем как регистрировать пользователя, добавьте его в программу.

1. Выберите пункт «Network» («Сеть») в меню «View» («Представление»).

2. В окне «Network» («Сеть») выберите УБИ для регистрации пользователя.

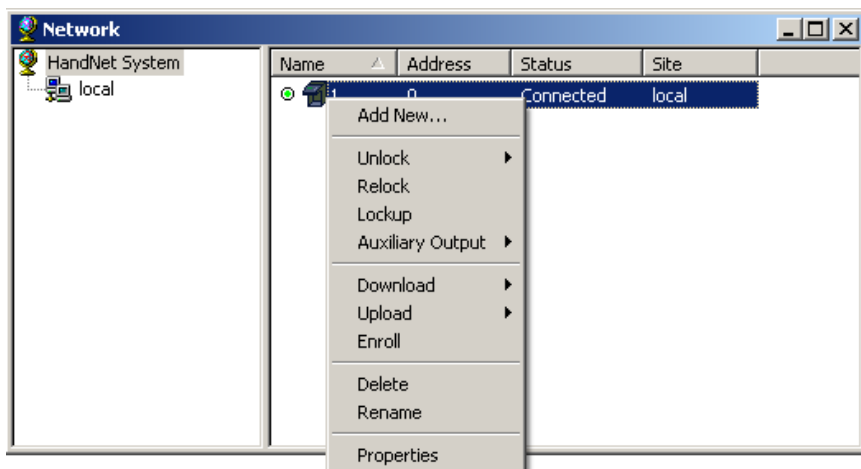


Рис. Е8. Выбор считывателя и его настройки

3. Зайдите в меню «Reader» («УБИ») и выберите «Enroll» («Регистрация»). Появится окно, показанное на рис. Е9.

4. Если регистрируемый пользователь не показан, выберите его вручную в разворачиваемом списке. Нажмите «Enroll now» («Зарегистрировать сейчас»).

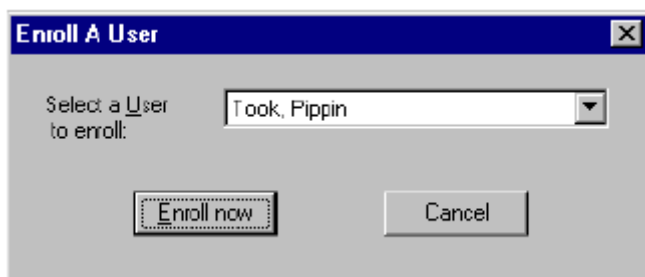


Рис. Е9. Регистрация пользователя

5. УБИ попросит пользователя поместить и убрать руку три раза, если считыватель попросит более трех раз – значит, пользователь неправильно помещает свою руку в устройство.

6. Если не возникло сообщение о какой-либо проблеме, то пользователь теперь является зарегистрированным.

Приложение Ж

ОПИСАНИЕ РАБОТЫ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ FINGERLAN 4.6 ФИРМЫ IDENTIX

Для того чтобы начать работу с ПО и добавить нового пользователя, необходимо определить несколько установок пользователя.

Определение установок пользователя

В окне «Fingerlan Sites» («Площадки Fingerlan») должны быть определены две пользовательские установки. Выберите в меню задач пункт «Fingerlan Sites» («Площадки Fingerlan») в левой стороне экрана. Информация показана на правой стороне экрана (рис. Ж1).

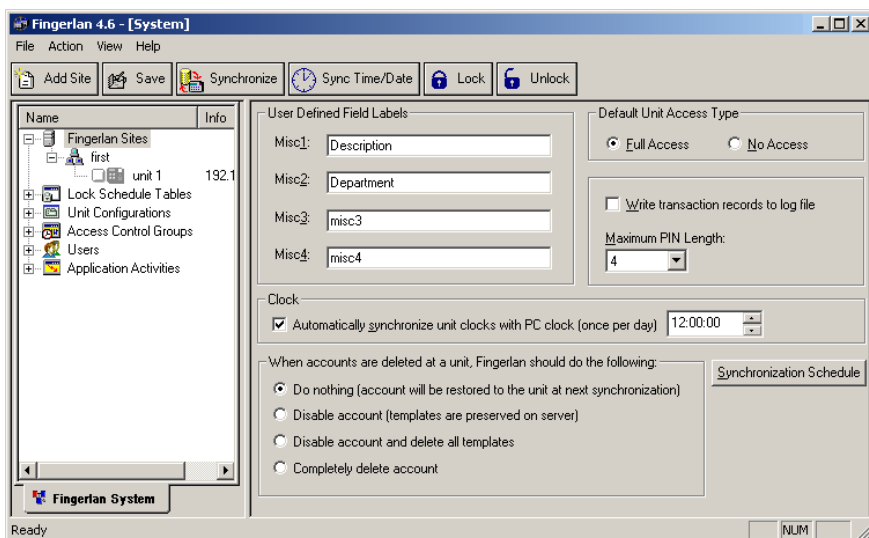


Рис. Ж1. Окно Fingerlan Sites. Меню задач

В списке зарегистрированных пользователей есть четыре дополнительных колонки, названия которых можно изменять. Это делается на панели «User Defined Field Labels» («Заданные пользо-

вателем заголовки полей»). Значения по умолчанию для этих полей – «Description» («Описание»), «Department» («Подразделение»), «Misc3» и «Misc4».

Также необходимо выбрать соответствующий переключатель в разделе «When accounts are deleted at a unit, Fingerlan should do the following» («При удалении учётных записей пользователей из устройства Fingerlan должен сделать следующее»):

- «Do nothing (account will be restored to the unit at next synchronization)» – «Ничего не делать (учётная запись будет загружена во время следующей синхронизации)» – все шаблоны останутся в других устройствах и в базе данных Сервера. Во время следующей синхронизации шаблоны будут загружены в УБИ;
- «Disable account (templates are preserved on server)» – «Отключение учётной записи (сохранение шаблонов на сервере)» – шаблоны будут удалены из всех устройств системы, и учётная запись пользователя будет отключена. Шаблоны тем не менее будут сохранены в базе данных Сервера;
- «Disable account and delete all templates» – «Отключение учётной записи и удаление всех шаблонов» – шаблоны будут удалены из всех устройств системы, и учётная запись будет отключена. Шаблоны будут удалены и из базы данных Сервера;
- «Completely delete account» – «Полное удаление учётной записи» – шаблоны будут удалены из всех устройств системы, и будет удалена учётная запись пользователя. Шаблоны будут удалены и из базы данных Сервера.

После внесения изменений необходимо нажать кнопку «Save» («Сохранить»). Также это можно сделать через меню «Action→Save» («Действие→Сохранить»).

Добавление пользователя

Выберите в меню задач пункт «Users» («Пользователи») в левой стороне экрана. Пользовательская информация показана на правой стороне экрана (рис. Ж2).

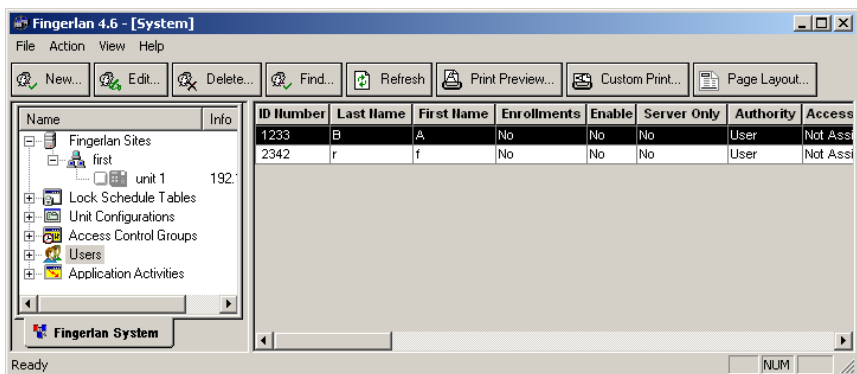


Рис. Ж2. Окно «Users» («Пользователи»)

Нажмите кнопку «New...» («Новый...»). Также это можно сделать через меню «Action→New» («Действие→Новый»). Появится диалоговое окно «Edit User» («Редактирование пользователя»). Его вид представлен на рис. Ж3.

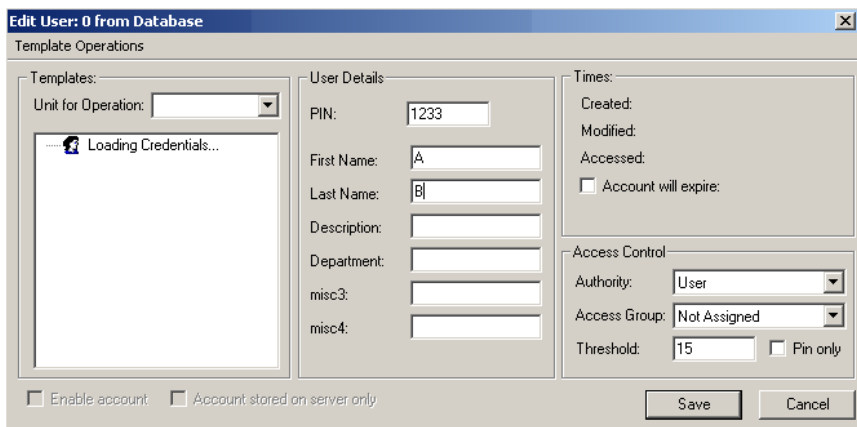


Рис. Ж3. Окно редактирования свойств пользователя

Введите PIN-код для нового пользователя. Это число должно быть уникальным в пределах СКУД и должно быть характерной длины, установленной во время определения пользовательских ус-

тановок. Введите имя пользователя (поле «First Name») и его фамилию (поле «Last Name»).

Введите информацию в дополнительные поля, названия которых задаются на панели «User Defined Field Labels» («Заданные пользователем заголовки полей»).

Поля «Created» («Создан»), «Modified» («Изменен») и «Accessed» («Получал доступ») в разделе «Times» («Времена») показывают информацию о том, когда учётная запись пользователя была создана, изменена и недавно задействована.

Если срок действия учётной записи должен истечь в определенное время, выберите «Account will expire» («Срок действия учётной записи истечёт») в разделе «Times» («Времена»). Тогда появится поле времени. Выберите необходимое время, используя выпадающее меню или стрелки вверх и вниз.

Выберите соответствующий уровень полномочий (Обычный пользователь, Регистрирующий пользователь, Супервизор (контролер) и Менеджер) в разделе «Access Control» («Контроль доступа»).

Выберите группу доступа, которую вы хотите присвоить пользователю, в поле «Access Group» («Группа доступа»).

Определите минимальный порог верификации для отпечатка пальца пользователя в поле «Threshold» («Порог»). Самое высокое значение – более точное сканирование. Диапазон значений от 1 до 200. По умолчанию 15.

Если это необходимо, выберите флажок «PIN only» («Только ПИН-код»), чтобы показать, что пользователь может проходить через дверь, используя только ПИН-код. Этот метод используется для лиц, еще не зарегистрированных и не идентифицируемых по какому-нибудь отпечатку пальца.

Чтобы сохранить учётную запись пользователя только на сервере, выберите флажок «Account stored on server only» («Учётная запись сохраняется только на сервере»). Чтобы сохранить счет пользователя в УБИ Fingerscan V20, не выбирайте этот флажок.

Чтобы включить учётную запись, выберите флажок «Enable account» («Включить учётную запись»). Чтобы отключить учётную запись, снимите флажок «Enable account» («Отключить учётную запись»).

Для сохранения нажмите кнопку «Save» («Сохранить»). Учётная запись пользователя сохранена.

Регистрация и верификация пользователей

Регистрация и идентификация включают в себя следующие шаги:

- добавление пальца (цев) в программе Fingerlan;
- регистрация пальца (цев) в УБИ Fingerscan V20;
- идентификация пальца (цев).

Добавление пальцев

Выберите в меню задач в левой стороне экрана пункт «Users» («Пользователи»).

Выберите учётную запись пользователя в правой стороне экрана.

Нажмите кнопку «Edit» («Редактировать»). Также это можно сделать через меню «Action→Edit» («Действие→Редактировать»).

Появится диалоговое окно «Edit User» («Редактирование пользователя»). Его вид представлен на рис. ЖЗ.

В разделе «Templates» («Шаблоны») в поле «Unit for Operation» («Применяемое устройство») выберите УБИ, которое будет использовано для регистрации.

Выберите в меню «Template Operations» («Действия с шаблонами») пункт «Add Finger» («Добавить палец»), чтобы добавить палец. Также вы должны определить, какой палец вы хотите добавить, например «Template Operations → Add Finger → Right → Index» («Действия с шаблонами→Добавить Палец→Правый→Указательный»).

Добавленный палец будет показан в разделе «Templates» («Шаблоны») диалогового окна (рис. Ж4).

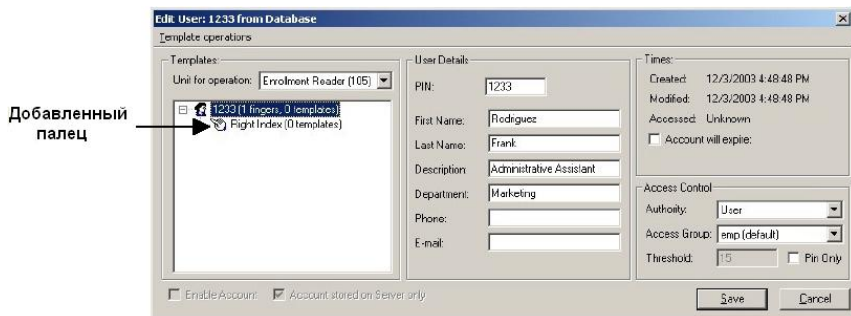


Рис. Ж4. Регистрация шаблона отпечатка пальца

Регистрация пальцев

В разделе «Templates» («Шаблоны») выберите палец, который вы хотите зарегистрировать.

Выберите в меню «Template Operations» («Действия с шаблонами») пункт «Enroll Template» («Зарегистрировать шаблон»).

Поместите регистрируемый палец в выемку для пальца на УБИ. Вы услышите характерный звук, когда шаблон будет зарегистрирован. После этого в разделе «Templates» («Шаблоны») диалогового окна появится зарегистрированный шаблон, включающий показатель детализации шаблона.

Чтобы сохранить изменения, нажмите кнопку «Save» («Сохранить»).

Лабораторная работа № 4

СОЗДАНИЕ МОДЕЛИ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ТОЧКОЙ ДОСТУПА

Цель работы:

- 1) Изучение основных возможностей контроллера ADEMANT-500F и турникета PERCo – RTD – 01.
- 2) Создание точки доступа на базе контроллера ADEMANT-500F и турникета PERCo – RTD – 01.

4.1 Описание объекта лабораторного исследования

В данном разделе описывается оборудование, используемое для выполнения лабораторной работы, и основные возможности этого оборудования.

4.1.1 Состав используемого оборудования

Для разработки рабочей модели системы контроля и управления точкой доступа в лабораторной работе используется следующее оборудование:

- контроллер ADEMANT-500F;
- турникет PERCo – RTD – 01.
- компьютер с установленной ОС Windows XP, имеющий COM-порт и сетевую карту Ethernet;
- монитор;
- ПО «ФОРПОСТ-СТАНДАРТ»;
- 1 кнопка (НЗК/НОК);
- 2 считывателя H-READER;
- соединительные провода.

Вся необходимая информация о характеристиках оборудования изложена ниже. Характеристики других устройств не приводятся, поскольку не являются важными для функционирования лабораторной установки.

4.1.2 Функции и характеристики контроллера ADEMANT-500F

Контроллер ADEMANT-500F является главным звеном в создаваемой лабораторной системе контроля и управления точкой дос-

тупа. Контроллер, имея энергонезависимую память с буфером на 2048 карт и журнал событий на 1952 события, при выходе из строя компьютера или линии связи накапливает информацию о проходах, продолжая обеспечивать работу системы в полном режиме. Контроллер ADEMANT-500F расположен в боксе «СКАТ-1200КР» с источником бесперебойного питания. На рис. 4.1 изображён внешний вид контроллера ADEMANT-500F в боксе «СКАТ-1200КР».



Рис. 4.1. Внешний вид контроллера ADEMANT-500F в боксе «СКАТ-1200КР»

В состав контроллера входят:

- двухпроводный интерфейс (линия связи) RS485 для объединения нескольких контроллеров и их администрирования с персонального компьютера;
- возможность подключения 2-х считывателей бесконтактных карт с выходом формата Weigand 26, Weigand 34;
- два входа подключения герконов (датчиков положения дверей);
- два входа подключения кнопок открытия двери;

- два реле управления замками или иными запирающими устройствами;
- два дополнительных выхода управления (открытый коллектор);
- энергонезависимая память на 2048 карт и журнал событий на 1952 события;
- часы реального времени с автономным питанием;
- аппаратная схема предотвращения зависаний и кнопку RESET;
- встроенный источник бесперебойного питания самого контроллера и считывателей бесконтактных карт;
- защита источников питания отдельными предохранителями.

Контроллер поддерживает конфигурации:

- две точки прохода в конфигурации два проксимити-считывателя, две кнопки на выход, два геркона, два замка;
- одну точку прохода с двумя считывателями на вход-выход в конфигурации два проксимити-считывателя, один геркон, один замок [1].

Возможно использование контроллера для организации шлюза, подключения биометрических считывателей.

Контроллер поддерживает работу практически со всеми стандартными считывателями, с форматом выходных данных weigand-26 (26 бит) и weigand-34 (34 бит) и питание 12 В постоянного тока.

Контроллер автоматически определяет: данные от считывателя имеют формат weigand-26 или weigand-34, никаких настроек в контроллере или программном обеспечении делать не надо.

Кроме того, могут подключаться считыватели с выходом формата TouchMemory при использовании преобразователя форматов ADEMANT-100.02.

Используется «нормально открытый» тип подключения кнопки открытия двери.

Для управления замками используются два реле с группами контактов на переключение, установленные на плате контроллера.

Возможно управление любым устройством (электромагнитный замок, турникет, шлагбаум, шлюз автоматический привод и т.д.).

4.1.3 Описание лабораторной установки, созданной на базе контроллера ADEMANT-500F

На рис. 4.2 представлена схема рабочей модели лабораторной установки с использованием контроллера ADEMANT-500F, подключённого к персональному компьютеру по магистрали (интерфейс RS-232). На персональном компьютере установлено программное обеспечение «ФОРПОСТ-СТАНДАРТ». К контроллеру ADEMANT-500F подключается роторный турникет PERCo-RTD-01.

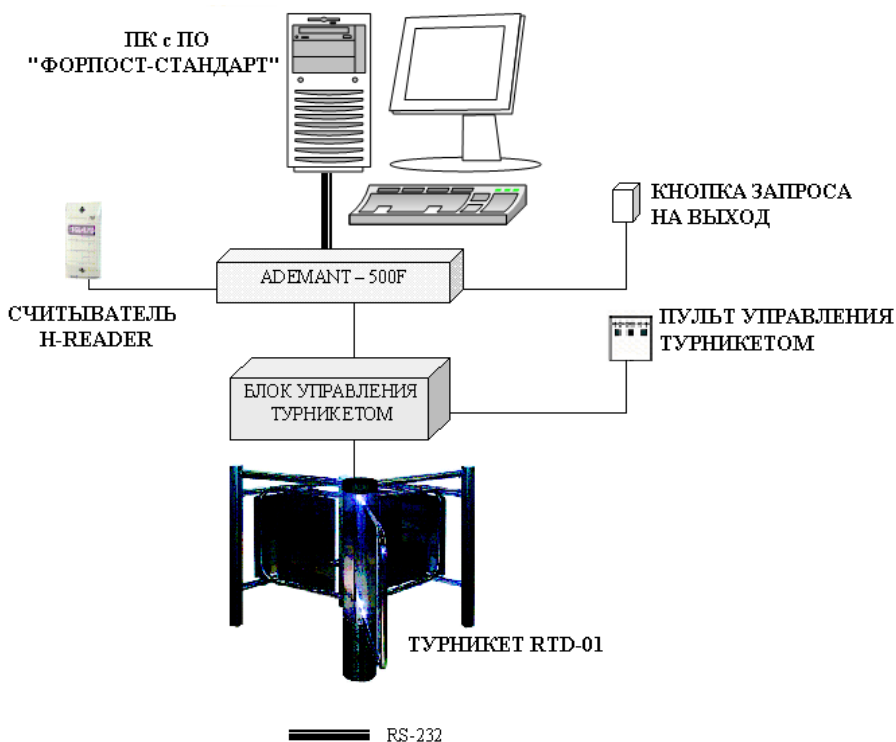


Рис. 4.2. Схема рабочей модели лабораторной установки с использованием контроллера ADEMANT-500F

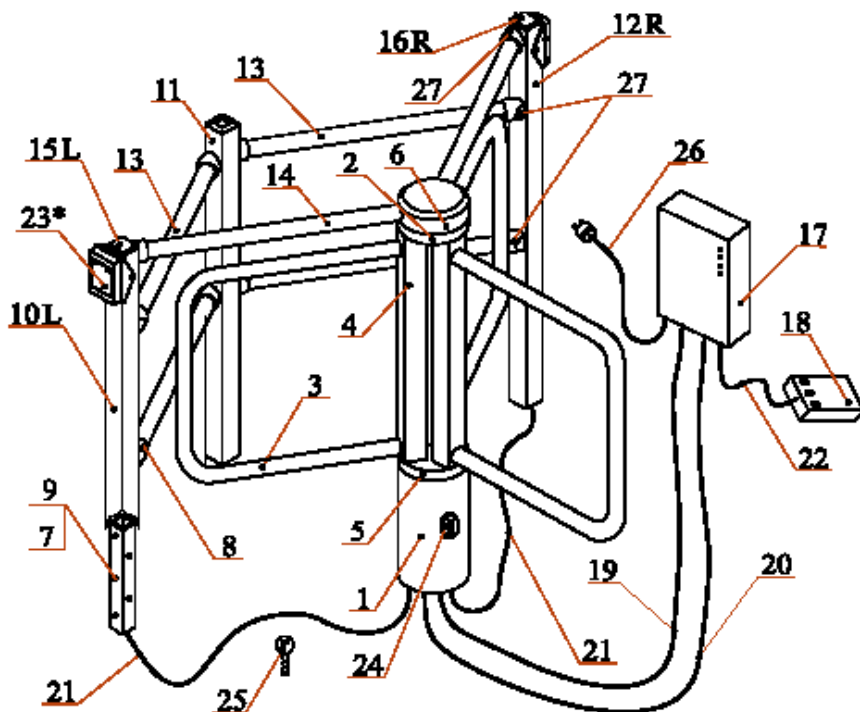
4.1.4 Функции и характеристики турникета PERCo – RTD–01

Турникет PERCo – RTD–01 предназначен для управления потоками людей на проходных промышленных предприятий, в банках, административных учреждениях и других объектах. Турникет питается от сети переменного тока 220 В с частотой переменного тока 50 Гц. Мощность, потребляемая турникетом от сети, не более 60 Вт. Напряжение питания стойки турникета (постоянного тока) не более 27 В. Напряжение внешнего резервного источника питания (РИП) (постоянного тока) 24-27 В. Турникет имеет 5 режимов прохода.

Особенности турникета PERCo – RTD–01:

- турникет может работать как автономно, от пульта управления или устройства радиоуправления, так и под управлением СКУД;
- на стойку турникета подается безопасное для человека напряжение питания – не более 36 В;
- турникет имеет низкое энергопотребление – не более 60 Вт;
- бесперебойную работу турникета при отключении сетевого питания в течение 1,5 ч или 1200 проходов обеспечивает внутренний резервный источник питания блока управления, в состав которого входят 2 герметичных свинцово-кислотных аккумулятора;
- в режимах однократного прохода турникет обеспечивает автоматический доворот преграждающих створок до исходного состояния после каждого прохода;
- демпфирующее устройство обеспечивает плавную бесшумную работу турникета;
- блок датчиков поворота ротора, установленный в основании стойки турникета, позволяет корректно фиксировать факт прохода при использовании турникета в составе СКУД;
- в стойку турникета встроен замок механической разблокировки, позволяющий в случае необходимости с помощью ключа разблокировать турникет (обеспечить свободный поворот преграждающих створок).

Общий вид и состав турникета представлен на рис. 4.3.



Обозначения:

1 – основание стойки турникета; 2 – верхний фланец; 3 – преграждающая створка; 4 – стойка крепления преграждающей створки; 5 – нижний фланец; 6 – планшайба с демпфирующим устройством; 7 – клиновой анкер КА 20х170; 8 – патрубок; 9 – узел крепления стойки ограждения; 10L – стойка ограждения левая; 11 – стойка ограждения центральная; 12R – стойка ограждения правая; 13 – поручень ограждения; 14 – поручень; 15L – модуль индикации левый; 16R – модуль индикации правый; 17 – блок управления; 18 – пульт управления; 19 – кабель вторичного электропитания; 20 – кабель управления; 21 – кабель индикации; 22 – кабель пульта управления; 23 – считыватель бесконтактных карт с кронштейном; 24 – замок механической разблокировки; 25 – ключ замка механической разблокировки; 26 – сетевой кабель

Рис. 4.3. Общий вид турникета

Турникет состоит из стойки турникета с преграждающими створками и комплекта V-образного ограждения. Стойка турникета

состоит из основания стойки, ротора и планшайбы с демпфирующим устройством. В основании стойки турникета (1) смонтированы: привод ротора, стопорные устройства, блок датчиков поворота ротора и плата силового модуля. Ротор собран на массивных нижнем (5) и верхнем (2) фланцах. Нижний фланец связан через конус Морзе с валом привода, а верхний – через демпфирующее устройство с планшайбой (6), которая жестко связана через поручни (14) со стойками ограждения (10L, 12R).

В комплект V-образного ограждения входят: стойка ограждения левая (10L), стойка ограждения правая (12R), стойка ограждения центральная (11) и поручни ограждения (13). Стойки ограждения имеют узлы крепления (9), которые крепятся к полу клиновыми анкерами КА 20х170 (7). На стойках ограждения (10L, 12R) размещены соответственно модули индикации (15L, 16R).

Стойка турникета подключается к блоку управления (17) с помощью кабеля вторичного электропитания (19) и кабеля управления (20). Модули индикации подключаются с помощью кабелей индикации (21) к плате силового модуля.

Пульт управления (18) выполнен в виде небольшого настольного прибора в корпусе из ударопрочного пластика и предназначен для задания и индикации режимов работы турникета при ручном управлении. Пульт управления подключается к блоку управления гибким многожильным кабелем (22) через разъем «RC». На лицевой панели корпуса пульта управления расположены 3 кнопки управления для задания режимов работы турникета. Над кнопками расположены индикаторы. Средняя кнопка (далее — кнопка STOP) предназначена для переключения турникета в режим «Запрет прохода». Левая и правая кнопки предназначены для разблокировки турникета в выбранном направлении. Пульт управления снабжен зуммером для формирования звуковых сигналов. Сигналы о нажатии кнопок от пульта управления поступают на блок управления.

Управление турникетом может осуществляться:

- с помощью пульта управления или устройства радиоуправления;
- от СКУД.

С помощью пульта управления или устройства радиоуправления можно задавать следующие режимы работы турникета (табл. 4.1):

- запрет прохода;
- однократный проход в заданном направлении;
- однократный проход в обоих направлениях;
- свободный проход в заданном направлении;
- свободный проход.

В режиме однократного прохода турникет автоматически закрывается после прохода человека в данном направлении. Если проход не выполнен в течение времени ожидания прохода (это время при поставке турникета равно 5 с), турникет также автоматически закрывается. Предусмотрена возможность изменения времени ожидания прохода установкой перемычек на плате процессорного модуля. Управление турникетом с помощью устройства радиоуправления идентично управлению от пульта управления. Кнопки на брелоке радиоуправления расположены так же, и выполняют те же функции, что и на пульте управления.

Управление турникетом от системы контроля и управления доступом возможно через системный разъем «ACS» блока управления. Подключение СКУД производится с помощью кабеля СКУД к разъему «ACS» блока управления. Управление турникетом от СКУД через разъём «ACS» блока управления осуществляется замыканием контактов «RIGHT», «STOP», «LEFT» с контактом «GND» (Общий) или подачей входного сигнала низкого уровня. Управляющим элементом в СКУД могут быть нормально разомкнутый контакт реле или схема с открытым коллекторным выходом.

Проход через турникет фиксируется с помощью датчиков поворота ротора, расположенных в основании стойки турникета. Направление прохода определяется последовательностью срабатывания датчиков.

При проходе (повороте преграждающей створки) на контактах «PASS R» и «PASS L» разъёма «ACS» блока управления формируются соответствующие сигналы высокого уровня, длительность которых зависит от скорости вращения ротора турникета. При совершении прохода в выбранном направлении и повороте ротора на угол 8-10° срабатывает один из датчиков поворота. При этом, в зависимости от направления прохода, формируется сигнал высокого уровня на выходе «PASS L» или «PASS R». Сигнал высокого уровня удерживается до тех пор, пока не будет совершен проход, и ро-

тор не вернется в исходное состояние. В выходных каскадах блока управления используется схема с открытым коллекторным выходом.

После включения питания, исходное состояние турникета – режим «Запрет прохода» (при закрытом ключом замке механической разблокировки турникета). Задание режимов работы турникета с пульта управления и их индикация осуществляются в соответствии с табл. 4.1.

Таблица 4.1. Задание режимов работы турникета с пульта управления и их индикация

№ п/п	Режим работы турникета	Действия на пульте управления	Индикация на пульте управления	Индикация на стойках ограждения
1	Запрет прохода (турникет закрыт для входа и выхода)	Нажатие средней кнопки STOP	Горит красный индикатор над кнопкой STOP	Горят красные индикаторы на обеих стойках
2	Однократный проход в заданном направлении (открыт для прохода человека в выбранном направлении)	Нажатие кнопки, соответствующей направлению прохода	Горит зелёный индикатор над кнопкой, соответствующей направлению прохода, и красный индикатор над кнопкой STOP	Горят зелёные индикаторы, соответствующие направлению прохода
3	Однократный проход в обоих направлениях (открыт для прохода одного человека в одном направлении)	Одновременное нажатие двух крайних кнопок: левой и правой	Горят два зелёных индикатора (левый и правый) и красный индикатор над кнопкой STOP	Горят зелёные индикаторы на обеих стойках

Продолжение табл. 4.1

№ п/п	Режим работы турникета	Действия на пульте управления	Индикация на пульте управления	Индикация на стойках ограждения
4	Свободный проход в заданном направлении (открыт для свободного прохода одного человека в выбранном направлении)	Одновременное нажатие кнопки STOP и кнопки, соответствующей направлению прохода	Горит зелёный индикатор над кнопкой, соответствующей направлению прохода	Горят зелёные индикаторы, соответствующие направлению прохода
5	Свободный проход (открыт для свободного прохода в двух направлениях)	Одновременное нажатие всех трёх кнопок	Горят два зелёных индикатора (левый и правый)	Горят зелёные индикаторы на обеих стойках

Некоторые особенности режимов работы турникета с пульта управления:

- установка любого режима производится путем нажатия кнопок пульта управления;
- при нажатии кнопки STOP турникет осуществляет установку режима «Запрет прохода», доворачивая ротор до исходного состояния;
- при задании режима однократного прохода (в одну из сторон или в обе стороны) турникет открывает стопорный механизм, соответствующий выбранному направлению, и находится в открытом состоянии некоторое время, называемое временем ожидания прохода (при поставке это время составляет 5 с). Для совершения прохода необходимо повернуть преграждающую створку на 8-10° в направлении прохода. Привод турникета автоматически довернет ротор до исходного состояния в направлении прохода;

- если в режиме однократного прохода проход не выполнен в течение времени ожидания прохода, турникет автоматически закроется и перейдет в режим «Запрет прохода». При разрешении однократного прохода в обоих направлениях, после совершения прохода в одну из сторон, турникет переходит в режим «Запрет прохода»;
- во время выполнения доворота в режиме однократного прохода установка другого режима блокируется, а введенная в этот момент с пульта управления последующая команда режима прохода записывается в буфер памяти процессора. После завершения доворота и установки в исходное состояние турникет автоматически переходит к выполнению команды из буфера;
- в режимах свободного прохода (в одну или в обе стороны) привод турникета не включается, позволяя свободно вращать ротор. При задании с пульта управления нового режима однократного прохода турникет переходит в этот режим, предварительно осуществив доворот ротора до исходного состояния.

При отключении сетевого питания работоспособность турникета сохраняется, турникет переходит на питание от внутреннего резервного источника питания. При снижении напряжения аккумуляторов РИП до уровня 22,5 В на пульте управления включается прерывистый звуковой сигнал, предупреждая о разряде аккумуляторов. При снижении напряжения аккумуляторов РИП до уровня 20,5 В турникет перейдет в аварийный режим. Задание режимов прохода от пульта управления и от СКУД заблокировано. При дальнейшем снижении напряжения произойдет автоматическое отключение блока управления. В аварийном режиме управление турникетом возможно только с помощью ключа замка механической разблокировки. При восстановлении сетевого напряжения турникет переходит на питание от сети. При этом подзарядка аккумуляторов внутреннего РИП производится в автоматическом режиме. Время работы турникета от внутреннего РИП составляет 1,5 ч, или 1200 проходов при условии полного заряда аккумуляторов РИП [2].

4.1.5 Описание алгоритма функционирования лабораторной точки доступа

Контроль точки доступа на базе лабораторного оборудования осуществляется благодаря системе контроля и управления доступом СКД «ФОРПОСТ». Система контроля доступа «ФОРПОСТ» разработки ООО «ШЭЛНИ» реализована на базе контроллеров серии ADEMANТ-500F. Программное обеспечение «ФОРПОСТ–СТАНДАРТ» – несетевая (работа только с 1 персональным компьютером (ПК)) версия программного обеспечения, предназначенная для конфигурации оборудования СКД «ФОРПОСТ».

Основная задача системы контроля доступа – разрешить проход уполномоченным субъектам (сотрудникам, посетителям) и запретить проход всем остальным.

Также система контроля доступа отслеживает события, происходящие в системе СКУД. На основании полученных данных решается еще одна актуальная на сегодняшний день задача – учет рабочего времени.

Организация прохода под управлением системы

Проходы под управлением системы производятся по следующему алгоритму:

- пользователь системы предъявляет идентификатор считывателю системы. Штатным идентификатором личности в СКД «ФОРПОСТ» являются проксимити-карты. Но использование идентификатора зависит от типа подключаемых к системе считывателей кода. Внешний же вид идентификатора для системы не имеет значения (могут быть карты, брелоки, метки и т.д.);
- при прикладывании карты к считывателю, считыватель считывает её код и передает его контроллеру ADEMANТ-500F;
- контроллер ADEMANТ-500F проверяет полученный код и определяет статус данной карты доступа по отношению к данному считывателю системы. Если данной карте доступа проход запрещен по статусу, на выходах индикации сигнализируется запрет доступа, в системе вырабатывается одно из

событий запрета доступа по статусу. Обработка предъявленной карты на этом прекращается;

- контроллер ADEMAN-T-500F определяет, разрешен ли проход обладателю данной карты доступа через данную точку доступа по времени. Дальнейшее поведение контроллера зависит от параметров режима доступа; в простейшем случае на выходах индикации сигнализируется запрет доступа, в системе вырабатывается событие запрета доступа по времени. Обработка предъявленной карты на этом прекращается;
- контроллер ADEMAN-T-500F принимает решение о том, что проход предъявителю данной карты доступа разрешен или запрещён. При подтверждении контроллером получения кода легальной карты подается сигнал на реле;
- к реле подключен турникет PERCo – RTD-01. При подаче сигнала на реле механизм турникета разблокируется, и индикаторы модулей индикации на стойках ограждения сообщают, что проход открыт.

Считыватель H-READER имеет управление красным и зеленым светодиодами и звуковым индикатором и самостоятельно вырабатывает индикацию.

При поднесении карты считыватель мигает зеленым светодиодом и подаёт короткий звуковой сигнал.

Дверь закрыта – горит красный светодиод.

Поднесена действительная карта – 2 мигания зеленого светодиода и 2 коротких звуковых сигнала.

Поднесена недействительная карта – 3 мигания зеленого светодиода и 3 коротких звуковых сигнала.

Дверь открыта (после поднесения действительной карты, нажатия кнопки, команды с компьютера) – индикация погашена.

Дверь взломана или незакрыта более установленного времени – мигает красный-зеленый, прерывистый звуковой сигнал.

С компьютера, используя программное обеспечение «ФОРПОСТ – СТАНДАРТ», можно заносить новые карты в память контроллера, регистрировать сотрудников, получать журнал событий, устанавливать длительность открытия замка и открытого состояния двери, конфигурацию контроллера и многое другое.

Информация о событии (проходе, запрете доступа, отказе от прохода, взломе и т.д.) заносится в журнал событий контроллера ADEMANТ-500F и по запросу передается по магистрали связи в компьютер для последующей обработки.

Система поддерживает также возможность возложить принятие решения о допуске (недопуске) пользователя системы на объект на оператора системы. Оператор может разрешить или запретить проход как с помощью кнопок, расположенных на пульте дистанционного управления, так и из окна программы «Наблюдатель».

Права доступа

Права данной карты по доступу на объекты системы (проходу через считыватели системы) задаются отдельно для каждого считывателя системы. Возможность прохода данной карты через данную точку доступа определяется статусом карты на данной точке доступа (на данном считывателе), временем прохода через данную точку доступа и местоположением владельца карты доступа относительно территории объекта, контролируемого системой.

Типы карт доступа:

- неизвестный ключ. Контроллер ADEMANТ-500F не имеет никакой информации относительно данной карты доступа. Проход предъявителю данной карты доступа запрещен;
- ключ сотрудника (действительная карта). Такая карта имеет право прохода через данную точку доступа в указанное для неё время. Эта карта подвержена контролю местоположения.

Ограничения по доступу карты на объект, связанные с ее статусом, т.е. запрет доступа карты данного типа на считывателе, функционирующем в данном режиме доступа, являются ограничениями по статусу.

Разграничение доступа по времени

Карты типа «ключ сотрудника» имеют право доступа через точку доступа только в определенное время. Время доступа данной карты через данный считыватель может изменяться от одного дня к другому в соответствии с временной зоной. Система поддерживает 16 временных зон.

Контроль местоположения

Карты «Ключ сотрудника» подвержены контролю местоположения. Суть его заключается в следующем: вся территория объекта, подконтрольного системе, может быть разбита на пространственные зоны. Система «знает» о местоположении пользователя с точностью до зоны. Если система считает, что обладатель определенной карты находится в зоне А, а карта предъявлена считывателю, ведущему из зоны В, то система считает, что произошло нарушение зональности – пользователь вел себя некорректно по отношению к системе. В этой ситуации обладателю обычного пропуска проход может быть запрещен. Возможно установление состояния АРВ (где АРВ – от antipassback – невозможность дважды подряд пройти в одну пространственную зону, не выходя из нее).

События в системе

Ниже приведен перечень наиболее распространенных событий СКД «ФОРПОСТ»:

- предъявлен ключ;
- ограничение доступа по времени;
- считан неизвестный ключ;
- дверь открыта кнопкой;
- дверь открыта оператором;
- дверь навсегда открыта оператором;
- дверь навсегда закрыта оператором;
- дверь разблокирована оператором;
- дверь закрыта;
- дверь открыта;
- дверь взломана;
- пользователь не пропущен дважды.

Дополнительная информация по программированию и настройке лабораторной установки приведена в приложении 3 и руководствах производителей [1, 2].

4.2 Порядок выполнения работы

1. Изучить возможности оборудования и лабораторной установки как единой системы по приведённым в практикуме описаниям.

2. Провести подключение элементов лабораторного стенда в соответствии с рис. 4.2.

Внимание! Только после проверки подключения преподавателем можно подавать питание на элементы установки.

3. Провести поиск контроллера и конфигурирование точки доступа.

4. Провести настройку временных зон по заданию преподавателя.

5. Провести регистрацию заданных карт в системе и создать список виртуальных сотрудников системы.

6. После моделирования функционирования системы сформировать и подготовить отчет о функционировании и отчет об учете рабочего времени сотрудников.

7. Подготовить отчет о выполненной работе по выданной преподавателем форме и защитить его.

4.3 Контрольные вопросы

1. Какие существуют способы управления турникетом PERCo – RTD-01?

2. Перечислите режимы работы турникета PERCo – RTD-01.

3. Как организовать проход сотрудников через турникет PERCo – RTD-01 по электронным картам доступа?

4. Какие специфичные функции СКУД можно реализовать на контроллере ADEMANT-500F?

Список литературы

1. Инструкция по монтажу контроллера ADEMANT-500F. ООО «ШЕЛНИ».

2. Турникет роторный электромеханический RERCo – RTD – 01. Паспорт и руководство по эксплуатации.

ОСНОВНЫЕ ВОЗМОЖНОСТИ СКУД «ФОРПОСТ» С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ «ФОРПОСТ- СТАНДАРТ»

31. Конфигурация точек доступа

Конфигурация точек доступа осуществляется из окна модуля «Управление модулями СКД». После того как был выполнен поиск контроллера, и он был успешно обнаружен, можно задать названия точек доступа и контроллера, находясь в меню «Свойства» контроллера. На рис. 31 изображено окно для задания точек доступа.

Свойства: контроллер_ademant-500

Общие | Сведения | **Параметры**

Адрес модуля: 1

Название: контроллер_ademant-500

Версия прошивки:
☐ 65 ☒ 66 (62)

Количество дверей: 2

Дверь 0: турникет вход

Дверь 1: турникет выход

Дверь 2:

Дверь 3:

☐ Отключен

Ok Отмена

Рис. 31. Конфигурация точек доступа

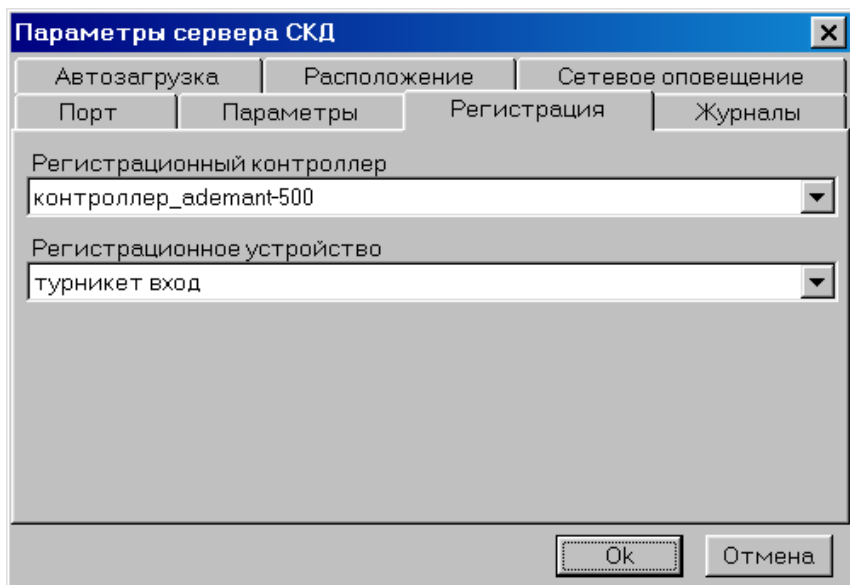


Рис. 32. Регистрационные данные

Для данной системы регистрационным контроллером является «контроллер_ademant-500», а в качестве регистрационного считывателя был выбран считыватель «турникет вход».

32. Настройка временных зон

Данная система позволяет задать до 16 временных зон. Для задания временных зон в главном меню «Управление модулями СКД» в разделе «Настройка» следует выбрать «Временные зоны». Далее для каждой временной зоны требуется задать её название и указать параметры категории доступа. После ввода всех параметров необходимо поочередно нажать кнопки «Исправить», «Записать в контроллеры», «Сверить». На рис. 33 показан перечень временных зон.

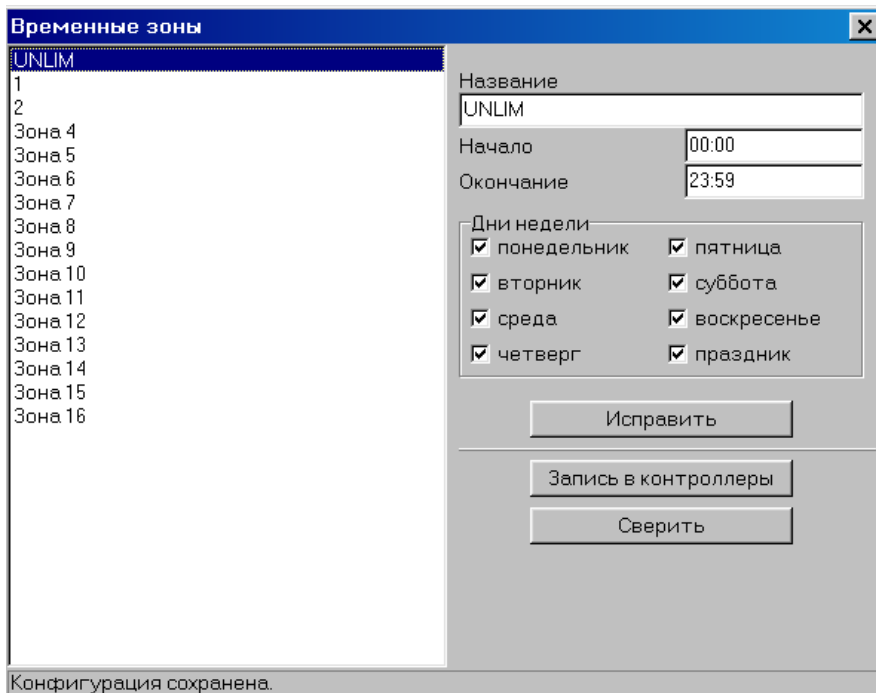


Рис. 33. Временные зоны

33. Организация списка сотрудников и регистрация их карт

Для того чтобы организовать список сотрудников, следует в главном окне программы выбрать «Список сотрудников». Далее из предложенного списка выбрать «Все сотрудники» и в разделе «Сотрудник» выбрать «Добавить», после чего в появившемся окне ввести ФИО сотрудника. При желании можно указать файл фотографии (если такой имеется) и звуковой файл, который должен запускаться при проходе этого сотрудника. Сотрудников можно определять в группы. На рис. 34 отражены параметры регистрации нового сотрудника.

The image shows a Windows-style dialog box titled "Свойства: USER1". It contains several input fields and buttons. The first field is "Фамилия сотрудника" (Employee Surname) with the text "USER1" entered. Below it is "Номер карты" (Card Number) with an empty field and an "Изменить" (Change) button to its right. The next field is "Фотография" (Photograph) with an empty field and a file selection icon (floppy disk with a plus) to its right. Below that is "Звуковой файл" (Sound file) with an empty field and two icons: a file selection icon and a play button. At the bottom of the dialog are "Ok" and "Отмена" (Cancel) buttons.

Рис. 34. Регистрация нового сотрудника

После занесения информации о сотруднике, не закрывая приложение «Управление модулями СКД», запустить приложение «СКД - Наблюдатель». Как только приложение «СКД - Наблюдатель» загрузилось, не выключая его, нужно вернуться в приложение «Управление модулями СКД». Нажав правой кнопкой мыши в списке сотрудников на нововведенном сотруднике в появившемся меню выбрать «Зарегистрировать карту». Далее, чтобы зарегистрировать карту, следует приложить регистрируемую карту к регистрационному считывателю и в меню правее от формы выбрать точку прохода (контроллер), через которую можно ходить по данной карте.

Для того чтобы для данного сотрудника задать временные зоны, нужно выделить интересующего сотрудника или группу сотрудников щелчком мыши по строке в списке, тогда в правой части окна панель «Временные зоны» будет доступна для редактирования. После чего необходимо выбрать «Разрешать доступ» в панели «Временные зоны», указать доступные для данного сотрудника категории доступа и сохранить данные. На рис. 35 показано соответствие сотрудника разрешённой ему временной зоне.

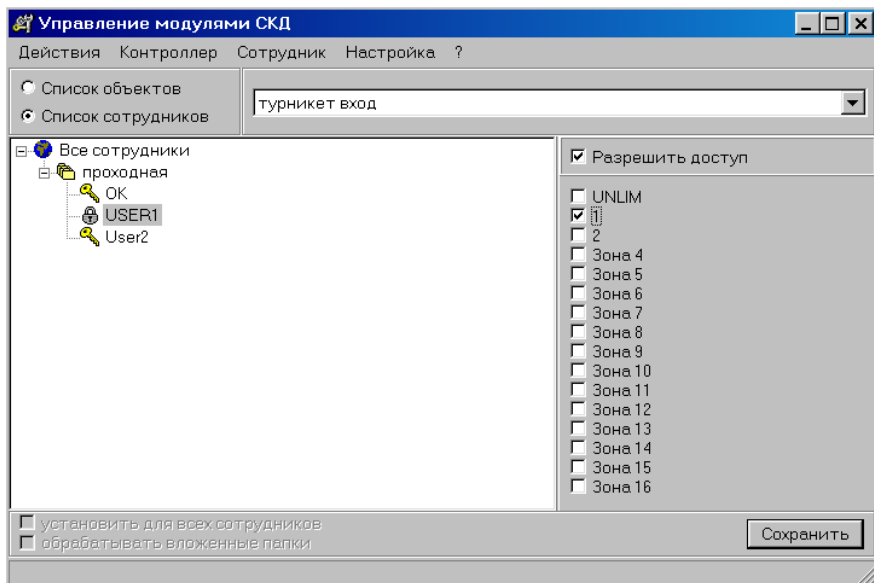


Рис. 35. Соответствие сотрудника разрешённой ему временной зоне

Чтобы записать эту информацию в контроллер, в главном меню в разделе «Действия» выбрать «Записать конфигурацию» и «Загрузить данные в контроллеры».

34. Формирование отчетов и учет рабочего времени

Данные обо всех произошедших событиях в системе хранятся в LOG-файлах системы: журнал событий (event.log), системный журнал (system.log), журнал ошибок (error.log), журнал обращений к контроллеру (hardware.log). Эти файлы можно открыть в текстовом редакторе или в Excel как таблицу и отсортировать нужные события средствами этих приложений, или воспользоваться приложением Report 2, идущим в комплекте с программой. Report 2 формирует отчет учета рабочего времени с функцией экспорта данных и вывода фото на основании данных LOG-файла.

Кроме этого, информацию о произошедших в системе событиях можно просмотреть во вкладке «Журнал» программы «Наблюда-

тель». Рис. 36 демонстрирует список событий, произошедших в системе.

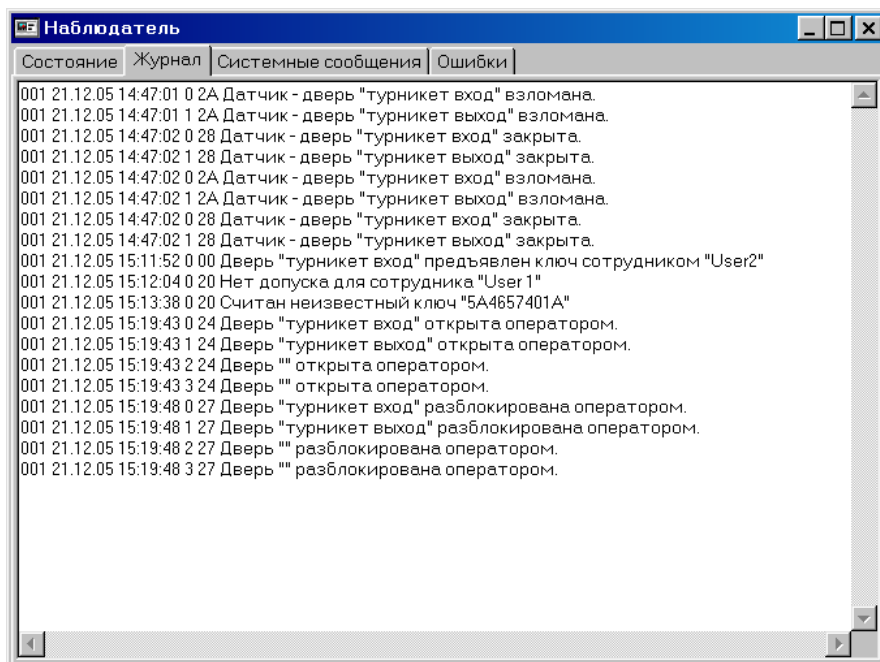


Рис. 36. Список событий

Александр Владимирович Бадиков
Павел Викторович Бондарев

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Лабораторный практикум

Редактор Е.Е. Шумакова

Оригинал-макет изготовлен
А.В. Бадиковым

Подписано в печать 10.12.2009. Формат 60х84 1/16
Печ.л. 8,0. Уч.-изд.л. 8,0. Тираж 200 экз.
Изд. № 1/3/72 Заказ № 24

Национальный исследовательский ядерный университет «МИФИ».
115409, Москва, Каширское ш., д. 31

ООО «Полиграфический комплекс «Курчатовский».
144000, Московская область, г. Электросталь, ул. Красная, д. 42