ООО «Компания Семь печатей»

117216, Москва, ул. Феодосийская, д. 1, тел.(факс): (495)) 225 25 31

E-mail: info@sevenseals.ru Web-Page: http://www.sevenseals.ru

Система контроля и управления доступом

TSS-OFFICE

TSS-PROFI

ВЕРСИЯ 6

Общее описание

руководство администратора

Москва

2006

Оглавление

Компания "Семь печатей" благодарит Вас за приобретение системы контроля доступа марки TSS. Надеемся, что Вы не пожалеете о своем выборе.

Мы заранее приносим свои извинения за возможные расхождения данного описания с действующей версией программного обеспечения, которое постоянно совершенствуется. Мы также будем Вам благодарны за любые замечания и предложения, связанные с функционированием Системы и ее отдельных модулей.

Желаем Вам успешной работы!

Система контроля и управления доступом марки TSS (далее СКУД) предназначена для осуществления автоматического и/или автоматизированного контроля и управления доступом в здания, зоны и помещения владельцев идентификаторов - «электронных ключей» (далее - ключей). Данные о перемещении людей, зафиксированные системой, используются для формирования разнообразных отчетов, в т.ч. для учета рабочего времени сотрудников.

СКУД марки ТСС может поставляться в рамках интегрированных систем безопасности, включающих, кроме контроля доступа, охранно-пожарную сигнализацию и видеонаблюдения. Интегрированная система безопасности может быть построена либо полностью на оборудовании и программном обеспечении марки ТСС, либо на оборудовании сторонних фирм. При использовании систем ТСС в рамках комплексных систем безопасности **категорически запрещается использовать возможности СКУД для обеспечения массовой эвакуации людей** (разблокировка дверей, включение средств пожаротушения и т.п.).

СКУД марки ТСС также может интегрироваться с различными кадровыми и бухгалтерскими системами.

СКУД в варианте Office ориентирована на минимальную конфигурацию СКУД (один контроллер, компьютер-сервер Системы и одна рабочая станция), что, как правило, используется в небольших организациях. СКУД в варианте Profi может являться весьма сложной системой с десятками контроллеров и компьютеров, интегрированной с охранной, пожарной и прочими видами сигнализации. Далее (кроме особо оговоренных случаев) мы не будем различать эти две модификации и будем говорить просто о системе контроля доступа или Системе.

СКУД – это программно-аппаратный комплекс, который включает в себя электронное оборудование и программное обеспечение фирмы-разработчика, и функционирует с использованием персональной вычислительной техники, операционных сред, локальных сетей. Далее остановимся на краткой характеристике всех включаемых в комплекс частей.

1. Оборудование

В общем случае в состав оборудования системы входят:

- Универсальные контроллеры серии TSS: 201, Office, 207, охранный контроллер, релейный контроллер;
- Элементы оборудования проходов (дверей) в контролируемые помещения (электрозащёлки, электромеханические или электромагнитные замки, датчики состояния дверей, кнопки открывания дверей, считыватели ключей и т.п.);
- Компьютеры, объединенные в локальную сеть.

1.1. Контроллеры

1.1.1. Общее описание

Все контроллеры являются устройствами, способными функционировать как в составе сетевой системы контроля и управления доступом (**комплексный режим**), так и автономно, при отсутствии связи с компьютером мониторинга (**автономный режим**). Исключение составляют контроллеры, специально приобретаемые для автономной работы (в них снята микросхема интерфейса с компьютером).

Контроллеры подключаются с помощью общей шины (восьмижильного кабеля типа "витая пара") и модуля согласования интерфейсов BIT-4.3 (RS485 / RS232) к стандартному последовательному порту или нескольким портам (COM-1, COM-2, …) компьютера *Мониторинга.*

Также возможно подключение линии контроллеров по локальной сети посредством интерфейсного модуля *TSSEthernet.*

Общая длина шины контроллеров может достигать 1200 метров[1], а количество контроллеров, подключаемых к одному последовательному порту компьютера, - 254 шт.

Элементы оборудования пунктов прохода с помощью 6- или 8-жильных кабелей подключаются к портам контроллеров. Максимальная длина кабеля соединяющего считыватель пункта прохода и контроллер может достигать 150 метров.

При использовании контроллеров серии 201 (с энергозависимой памятью) необходимо наличие аккумуляторов (поставляются вместе с контроллерами). Свежего аккумулятора хватает примерно на 8 часов автономной работы. При длительном отключении питания контроллера или выключении его из сети необходимо отсоединить клеммы питания с аккумулятора во избежание его разрядки.

Подробнее описание контроллеров приведено в серии документов «Инструкция по монтажу».

Далее будут описаны только те характеристики различных типов контроллеров, которые необходимы для понимания логики работы СКУД.

[1] Без использования репитера.

1.1.2. Контроллеры серии 201

Контроллеры серии 201 являются универсальными устройствами, обладающими:

- Собственной системой стабилизированного штатного и аварийного (на базе аккумулятора) электропитания, обеспечивающей питанием и электронику самого контроллера и подключаемые к нему элементы оборудования;
- Памятью (энергозависимой), в которой хранятся[2]:
- 1984 идентификационных кода (коды ключей);
- данные о событиях, связанных с доступом в контролируемые помещения и работой контроллера (1008 событий);
- время каждого события (в формате чч:мм:сс)[3];
- данные о разрешение или запрете доступа каждого кода (ключа) по каждому порту контроллера (данные о маршрутах);
- Собственным процессором и ПЗУ, в котором находится программа автономной работы контроллера;

К одному порту[4] контроллера серии 201 можно подключить:

- 1 считыватель ключа (устройство ввода кода);
- 1 датчик состояния двери;
- 1 кнопку открывания двери;
- 1 исполнительное устройство.

Буква W в типе контроллера обозначает Weigand интерфейс, буква T – Dallas интерфейс (Touch), буква O – охранный контроллер (Touch).

Количество портов каждого из контроллеров серии зависит от его типа (2 для контроллеров типа 201-2 (W и T), 4 для контроллеров типа 201-4 (W и T) или 8 для контроллеров типа 201-8 (W и T)).

При разряде аккумулятора (ниже 11 В) контроллер генерирует событие *Нет 12 В*. Имеется возможность получить информацию о сбое по питанию 220 В.

1.1.3. Контроллеры Office

Контроллеры типа Office (TA-53 или WA-48[5]) являются двухпортовыми и имеют следующие отличия от контроллеров серии 201:

- хранят 504 или 1008[6] кодов ключей и 7744 событий (для контроллеров с полной памятью – W+ и T+)7,
- хранят время и дату каждого события,

---

[2] Данные, хранящиеся в памяти, обеспечивают работу контроллера в автономном режиме.

[3] Обратите внимание на отсутствие даты.

[4] Порт выполнен в виде клеммной колодки

[5] TA-53 для идентификоров touch memory, WA-48 –для proximity card.

[6] В зависимости от прошивки.

[7] По требованию память ключей может быть расширена до 1000, при одновременном уменьшении памяти событий.

- могут работать в автономном режиме, передавая при этом сообщения о событиях программе мониторинга,
- хранят сведения о расписании проходов (временные зоны), т.е. осуществляют контроль по времени доступа в автономном режиме,
- позволяют изменять время срабатывания реле,
- имеют энергонезависимую память.
- Генерируют события Нет 220 В и Нет 12 В.

1.1.4. Контроллеры 207 серии

Контроллеры 207 серии аналогичны контроллерам серии Office, являются двух-, четырех- или восьмипортовыми и имеют следующие отличия от контроллеров серии Office:

- Хранят 15600 кодов ключей и 150000 событий.
- Имеют встроенные алгоритмы работы с памятью, что увеличивает его быстродействие.

1.1.5. Контроллеры 209 серии

Контроллеры 209 серии аналогичны контроллерам серии 207, но имеют следующие отличия:

- Хранят до 64000 кодов ключей.
- Имеют четное число портов (от двух до восьми).

1.1.6. Релейный контроллер

Релейный контроллер является устройством для дистанционного (в рамках СКУД) управления исполнительными устройствами. В настоящее время выпускается в восьмипортовой реализации.

1.1.7. Особенности описания типа контроллеров

При описании контроллеров в рамках программного комплекса СКУД, установленного на компьютере, следует иметь в виду следующее:

Все параметры контроллера, задаваемые в программе конфигурирования системы, должны точно соответствовать характеристикам контроллера, описанным в его паспорте.

В поле «Тип контроллера» выбирается:

- STN для контроллеров серии 201 и релейных,
- WA48 для контроллеров серий Office и 207,
- ATN для охранных контроллеров 201 (тип 2O, 4O, 8O),
- FIT для охранно-пожарной сигнализации Securiton компании Fittich.

1.2. Требования к компьютерам и ОС

Программное обеспечение СКУД делится на программы ядра Системы и пользовательское ПО. Ядро устанавливается на т.н. Сервер СКУД, требования к кото-

рому тем выше, чем сложнее конфигурация СКУД. Для достаточно развитой Системы можно рекомендовать следующие характеристики компьютера-сервера:

- процессором типа Pentium IV (тактовая частота - не менее 2,4 ГГц).
- оперативной памятью объемом не менее 512 Мб,

Для работы пользовательской части ПО рекомендуется ПК со следующими минимальными параметрами:

- процессором типа Pentium IV (тактовая частота - не менее 1,6 ГГц).
- оперативной памятью объемом не менее 256 Мб,

Чем сложнее конфигурация СКУД, тем выше требования к компьютерам, особенно к серверу, поэтому вопрос об их параметрах в каждом конкретном случае должен обсуждаться с фирмой-производителем или поставщиком СКУД. При жестких требованиях к надежности комплекса рекомендуется устанавливать ядро системы на ПК brand-name в серверной архитектуре. При использование СКУД на объектах с большой интенсивностью проходов (десятки проходов в секунду) и значительным числом персонала (десятки тысяч) рекомендуется выделять отдельный ПК под сервер базы данных.

Компьютер, на котором функционирует ядро СКУД (сервер СКУД) должен быть включен через источник бесперебойного питания.

Программы ядра СКУД работают под управлением только Windows линии NT, а именно Windows 2000 Server или Windows 2003. Допускается установка Windows 2000 Professional.

ОС на всех компьютерах должны быть локализованы (т.е. установлен русский язык). При наличие локализованных версий ОС предпочтительно устанавливать их.

Прочие (клиентские) приложения СКУД работают под управлением любой из вышеперечисленных ОС, а также Windows XP.

На всех компьютерах Системы должна быть установлена сетевая среда с протоколом TCP/IP. При отсутствии сетевой карты эмулируется ее наличие (в NT используется адаптер Loopback). Сетевое имя компьютера должно содержать только цифры и латинские буквы верхнего регистра.

Сервер СКУД необходимо использовать в монопольном режиме (не допускается исполнение на нем программ, не связанных со СКУД). Пользователь данного компьютера должен иметь права администратора. Все остальные программные модули должны быть разнесены по рабочим станциям локальной сети. Администраторские права необходимы только на время установки комплекса.

Минимальная конфигурация Системы – ПК Сервер и ПК рабочая станция. **Еще раз подчеркнем, что мы гарантируем корректную работу СКУД только при выполнении вышеперечисленных условий.**

Примерная схема комплексной системы контроля доступа и охранной сигнализации приведена в конце руководства (схема 1).

В заключении этого раздела хочется напомнить достаточно очевидную вещь. От выбранного компьютера с качественными комплектующими, от грамотно установленной операционной системы и от правильной эксплуатации программного комплекса СКУД зависит надежность его работы. А надежность работы СКУД – это прежде всего гарантированная безопасность на территории Вашего объекта.

2. Программное обеспечение

2.1. Принципы функционирования СКУД

Администратор Системы должен четко представлять себе верхний (системный) уровень работы комплекса, функции ядра СКУД, принципы работы с базами данных, межпрограммное взаимодействие, функционирование прикладных программ комплекса.

2.1.1. Архитектура программного комплекса

Программное обеспечение СКУД построена на модульной основе, т.е. состоит из ряда отдельных программ, каждая из которых решает определенный круг задач.

Функционально ПО делится на программы ядра и пользовательские программные модули. Первые должны работать в связке на Сервере СКУД, вторые могут запускаться по необходимости на рабочих станциях СКУД.

К программам ядра относятся следующие обязательные для работы СКУД модули:

- *Система слежения* – управление работой ядра СКУД.
- *Сервер транспорта* – отвечает за межпрограммное взаимодействие.
- *Сервер контроллеров* - отвечает за связь с контроллерами СКУД.
- *Мониторинг* – система принятия решения.
- *Системный журнал* – программа ведения протокола событий СКУД.

К пользовательским программам относятся следующие модули[8]:

- *Песронал (Бюро пропусков)* – ведение базы данных сотрудников.
- *Проходная* – отображение информации по проходам.
- *Управление объектами* – отображение работы СКУД и управление ею.
- *Дистанционный мониторинг* – отображение событий СКУД.
- *Отчеты* – формирование и печать отчетов о работе Системы.
- *Программы администрирования* – различные программы для администрирования СКУД.

Все программы комплекса связаны в единое целое посредством:

- Использования единой базы данных.
- Обмена сообщениями по сетевому протоколу.

2.1.2. Работа с базами данных

Работа с базами данных осуществляется посредством СУБД Firebird[9]. СУБД устанавливается автоматически при установке СКУД с дистрибутивного диска.

[8] Перечислены только модули, входящие в стандартную поставку.

[9] О СУБД Firebird смотрите на сайте http://www.interbase-world.com/ru/firebird/

Отдельные клиентские приложения также используют СУБД BDE (Borland Database Engine).

2.1.3. Межпрограммное взаимодействие

Связь между приложениями комплекса осуществляется по протоколу TCP/IP. Таким образом, Система изначально настроена на работу в локальной сети.

Перед установкой программного обеспечения комплекса СКУД в операционной системе должна быть выполнена установка сети, с конфигурированием сетевого протокола TCP/IP. Если на компьютере отсутствует сетевая карта, то устанавливается ее эмулятор. Для NT/2000 это MS Loopback Adapter.

Обмен данными между программами комплекса обеспечивает сервис *TSSTransport*. Эта программа, диспетчерирует работу приложений СКУД, запущенных как на сервере Системе, так и на ее рабочих станциях. *Транспорт* является программой ядра СКУД и функционирует на ее сервере.

Для работы всех модулей СКУД, необходимо настроить файлы параметров на работу в конкретной конфигурации (т.е. указать сетевые имена ПК, на которых выполняются программы *Мониторинг* и *Транспорт*), а также указать путь к базе данных Системы (т.н. алиас).

Указанные сервисы и файлы параметров устанавливаются и настраиваются при инсталляции ПО.

2.1.4. Протоколирование событий СКУД

Запись информации в *Системный журнал* производится с помощью сервиса *Системный журнал*. Программа является сервисом и загружается автоматически при старте ОС[10]. При сбоях в записи протокола событий генерируется сообщение о фатальной ошибке, и СКУД переводится в автономный режим работы (т.е. контроллеры начинают работать самостоятельно, сохраняя протокол событий в своем буфере).

2.1.5. Работа с контроллерами

Обмен данными и управление контроллерами реализовано в сервисе *Сервер контроллеров*. Данный сервис может работать как в связке с системой принятия решений СКУД (программа *Мониторинг*), так и самостоятельно. В первом случае он является ретранслятором событий СКУД от контроллеров *Мониторингу* и команд на управление от *Мониторинга* контроллерам. Во втором случае *Сервер контроллеров* самостоятельно принимает решения по правам доступа, руководствуясь данными, хранящимися в системном реестре Windows. Заметьте, что последний режим рекомендуется включать только в особо оговоренных в документации случаях.

2.1.6. Терминология

Далее во всей документации под термином «Сервер системы» будет пониматься ПК, на котором планируется установить ядро системы – сервисы *Транспорт,*

[10] Точнее, ее (как и остальные модули ядра) загружает сервис *Система управления*, который и имеет автоматичаский тип старта.

Системный журнал, Сервер контроллеров[11]*, Мониторинг, Система управления.* Как правило, на этой же машине должна функционировать СУБД.

2.2. Программные модули

В программное обеспечение Системы (стандартная конфигурация) включаются следующие модули:

- «*Транспорт*» (файл transsrv.exe),
- «*Система слежения (Сервер)*» (файл ACSGMSServer.exe),
- «*Система слежения (Клиент)*» (файл ACSGMSClient.exe),
- «*Сервер контроллеров*» (файл ServCont.exe),
- «*Системный журнал*» (файл WriterLog.exe),
- «*Мониторинг*» (файл Monitoring.exe),
- «*Конфигуратор*» (файл Doors.exe),
- «*Персонал*» (файл Person.exe),
- «*Дистанционный мониторинг*» (файл DMon.exe),
- «*Проходная*» (файл MDIMon.exe),
- «*Управление объектами*» (файл PlanBrowser.exe),
- Программы отчетов,
- Сервисные программы.

2.2.1. Программа Система слежения - Сервер

ACSGMSserver [12] (acsgmsserver.exe) – программа, администрирующая работу СКУД в целом на Сервере в частности. Она стартует сервисы и программные модули, следит за их корректной работой, обеспечивает защиту Системы от несанкционированного доступа. Она также проверяет наличие файла лицензии и соответствие параметров лицензии реальной конфигурации системы. В случае несовпадения этих параметров[13] программа отключает нелицензированные приложения.

Является NT сервисом. Устанавливается при инсталляции ПО на Сервер системы.

2.2.2. Программа Система слежения - Клиент

ACSGMClient (acsgmsclient.exe) – программа, администрирующая работу модулей СКУД на рабочих станциях системы. Она стартует сервисы и программные модули, следит за их корректной работой, обеспечивает защиту Системы от несанкционированного доступа. Является NT сервисом. Устанавливается при инсталляции ПО на те рабочие станции системы, где работает программа *Сервер контроллеров*.

---

[11] В конфигурации Мультимониторинг программа *Сервер контроллеров* может функционировать на любой рабочей станции Системы, к которой подключена линия контроллеров.

[12] ACSGMS – Access Control System General Management System.

[13] Подлежит проверке число контроллеров, их адреса, количество записей в базе персонала, количество рабочих станций.

2.2.3. Программа Сервер Контроллеров

ServCont (ServCont.exe) – NT сервис, обеспечивающий работу с контроллерами. Работает либо в режиме ХОСТ (транслирует события и команды между контроллерами и *Мониторингом*), либо в режиме САМ (самостоятельное принятие решений по правам доступа). В режиме САМ использует собственную базу данных, хранящуюся в реестре. Должна быть установлена как NT сервис и сконфигурирована с помощью программы *Редактор настроек*. Может работать как на одном с *Мониторингом* компьютере, так и на рабочих станциях, реализуя т.н. режим *Мультимониторинга* – связи отдельных звеньев контроллеров в единую систему.

Устанавливаются при инсталляции ПО, на тех ПК, к которым подключены линии контроллеров.

При загрузке *Сервер контроллеров* проверяет наличие файла защиты, связь с контроллерами, а также соответствие параметров лицензии реальной конфигурации системы. В случае несовпадения этих параметров[14] программа прекращает работу.

2.2.4. Программа Транспорт

Transport (transsrv.exe) – сервис, обеспечивающий сетевое взаимодействие модулей СКУД. Должен функционировать на Сервере Системы. Имя ПК, на котором работает *Транспорт*, указывается в файле настроек (файлы с расширением *ini*) для каждого модуля.

Устанавливаются при инсталляции ПО. Сервис должен стартовать автоматически при старте ОС.

2.2.5. Программа Системный журнал

WriterLog или *Системный журнал* (WriterLog.exe). Программа, осуществляет запись в Системный журнал СКУД. Именно через нее обращаются к Системному журналу все модули системы. Является сервисом. Устанавливаются при инсталляции ПО на Сервере системы. Помните, что данная программа не предназначена для просмотра и работы с журналом. Для этих целей пользуйтесь программой *Дистанционный мониторинг* и системой отчетов.

2.2.6. Программа Мониторинг

Программа предназначена для выполнения алгоритмов СКУД (принятие решения по правам допуска, реализация различных режимов и функций СКУД, работа с охранной сигнализацией).

Программа функционирует только в связке с *Сервером контроллеров* и *Системным журналом*.

Необходимо понимать, что все остальные модули СКУД (*Персонал, Проходная* и прочие) будут функционировать только при работающем *Мониторинге*.

---

[14] Подлежит проверке число контроллеров, их адреса, количество записей в базе персонала, количество рабочих станций, количество мультимониторингов.

2.2.7. Программа Конфигуратор СКУД

Программа предназначена для описания контроллеров и элементов оборудования (считывателей ключей, кнопок, датчиков) и их привязки к поэтажным планам.

С помощью этой программы также производится описание и настройка различных режимов работы СКУД и охранной сигнализации. Она же используется для создания планов этажей и нанесения на них элементов СКУД.

При необходимости выполнения профилактических и ремонтных работ администратор системы в любой момент может отключить часть оборудования. При этом все остальные подсистемы будут регулировать доступ в обычных режимах.

Следует иметь в виду, что объекты и их характеристики должны точно соответствовать реальной конфигурации конкретной системы контроля доступа: **все необходимые данные о конфигурации Системы (адреса контроллеров, наличие датчиков и кнопок открывания дверей, конкретные места их расположения и т.д.) должны быть получены от представителя монтажной организации после завершения монтажа оборудования.**

2.2.8. Программа Бюро пропусков (Персонал)

Программа предназначена для ввода и редактирования информации о персонале, задания прав доступа, занесения кодов ключей. С помощью этой программы администратор Системы или уполномоченный сотрудник может задавать различные объектные и временные ограничения доступа для отдельных владельцев регистрируемых ключей. На основе установленных ограничений осуществляется автоматическое управление доступом в здания и помещения. Для каждого из зарегистрированных в системе ключей задается срок его действия.

Процесс регистрации человека в системе при выдаче ключа напоминает заполнение определенной формы - персональной "электронной учетной карточки". Помимо различной текстовой информации о человеке, в карточку можно занести фото владельца ключа.

При установке ограничений доступа для владельца ключа можно задать номера зон доступа - так называемых маршрутов, - представляющих собой списки дверей и других пунктов прохода, через которые данный владелец может входить и/или выходить из помещений и здания.

Помимо зон, для каждого конкретного человека можно ввести интервалы времени (по дням недели), в течение которых для него будет заблокирован или разрешен вход/выход в какую-либо из дверей.

Имеется возможность поиска, сортировки и отбора в базе данных "электронных карточек" (записей базы данных) зарегистрированных владельцев ключей. Поиск и отбор "карточек" может осуществляться по самым различным критериям - по названию подразделения, группы, организации, по Ф.И.О., категории (статусу) владельца в организации, по коду ключей, по номеру и серии паспорта, другой дополнительной информации.

Доступ к базе "электронных учетных карточек", содержащих информацию о зарегистрированных владельцах ключей, открыт только для уполномоченных сотрудников - администратора системы, отдельных сотрудников службы безопасности или работников бюро пропусков. Получение доступа к базе и регистрация оператора перед началом сеанса работы (заступлением на пост) осуществляется путем ввода личного пароля.

2.2.9. Программа Дистанционный монитор

Программа “Дистанционный монитор” (DmonM) предназначена для просмотра текущих событий Системы а также списка владельцев ключей.

Пользователь имеет возможность задавать для отображения определенные события и объекты, отбирать события, связанные с конкретными людьми, выводить информацию о месте последнего пребывания данного лица, формировать списки сотрудников, находящихся на объекте или отсутствующих на нем.

2.2.10. Программа Проходная

Программа «Проходная» (MdiMonw) выдает информацию о различных событиях системы. Однако главное ее назначение – отображение на экране сведений о проходящих сотрудниках (фотографию и текстовые данные). Также производится звуковое оповещение об экстренных событиях.

Имеется развитая система управления режимами работы программы.

При соответствующем аппаратном обеспечении программа выводит на экран окно изображения с видеокамеры и осуществляет захват видеоизображения по касанию ключом считывателя.

2.2.11. Программа Управление объектами

Программа «Управление объектами» (PlanBrowser) отображает события системы с помощью поэтажных планов. Позволяет управлять объектами системы (открывать, закрывать, блокировать двери). При наличии охранных контроллеров позволяет ставить и снимать объекты с охраны.

2.2.12. Сервисные программы

Сервисные программы предназначены для администрирования Системы.

- **Архивация и восстановление баз данных (Backup-Restore).**

Позволяет создавать архив баз данных во время работы системы для восстановления Системы после сбоев.

- **Архивация базы системного журнала (ArhSyslog).**

  Позволяет создавать архив базы данных событий системы.

- **Экспорт данных из базы данных (TSSExchange).**

Позволяет экспортировать данные из базы данных во внешние файлы.

- **Редактор установок (ParamsEdit).**

Позволяет изменять различные настройки, необходимые для работы Системы.

2.2.13. Программа отчетов

Программа *Комплексный отчет* позволяет получить и распечатать следующие отчеты:

- **Все события**

Информация о всех или произвольно выбранных событиях.

- **Нарушения**

Информация о нарушениях рабочего графика (опоздания, преждевременный уход).

- **Проходы**

Информация о проходах в помещения всех или выбранных лиц.

- **Рабочее время**

Быстрый отчет по рабочему времени всех или выбранных лиц.

3. Режимы и функции Системы

3.1. Режимы работы Системы

Система может функционировать в двух основных режимах: в **комплексном** (Системой управляет компьютер *Мониторинга*), и в **автономном** (контроллеры работают самостоятельно).

В автономный режим работы система переходит:

- по команде администратора системы (например, в случае необходимости замены или подключения какого-либо элемента, перед проведением профилактики и т.д.),
- автоматически - через 4 секунды после пропадания связи между контроллерами и компьютерами (в результате повреждения линии связи, отключении электричества в здании, при выходе из строя компьютера Мониторинга).

В этом режиме система представляет собой совокупность независимых друг от друга автономных систем контроля и управления доступом, каждая из которых включает в себя контроллер и подключенное к его портам оборудование. Управление доступом в каждой такой системе берет на себя контроллер. При этом он:

- управляет доступом в помещения с учетом запретов на проход (маршрутов) через тот или иной пункт прохода (дверь),
- ограничивает доступ согласно заданным временным интервалам (только для контроллеров серии Office и 207);
- •записывает в свою память информацию о событиях, связанных с доступом в "свои" помещения для последующей перезаписи их в Системный журнал (на жесткий диск компьютера) после перехода в комплексный режим работы;
- управляет доступом в помещения владельцев только тех ключей, коды которых были записаны в память контроллера до момента перехода в автономный режим.

Продолжительность автономной работы системы в случае отсутствия электропитания в сети может достигать 8 часов. Время автономной работы контроллеров зависит от зарядки аккумуляторов, типа исполнительных устройств (защелки, электромагниты), интенсивности их срабатывания. Таким образом, Система способна регулировать доступ в помещения и здания даже при полном отключении электричества, выходе из строя компьютеров, повреждении большей части оборудования и т.д.

Система перестает функционировать лишь при полном обесточивании контроллеров. При этом контроллеры серии 201 сбросят все данные из памяти (коды ключей и события). В контроллерах серии Office и 207, имеющих энергонезависимую память, данные сохранятся.

Охранные контроллеры работают только в комплексном режиме.

Еще раз подчеркнем, что при выходе из строя одного или нескольких контроллеров система будет продолжать штатно функционировать с работоспособными устройствами[15]. Все события об изменении режимов работы или выходе из строя оборудования фиксируются в Системном журнале и сопровождаются текстовыми и звуковыми сообщениями.

Таким образом, выход из строя любого оборудования или элемента не приводит к остановке всей системы, а ремонт или замена могут быть проведены без ее отключения.

3.2. Функции Системы контроля доступа

Основным назначением Системы в комплексном режиме (как, впрочем, и в автономном) является управление доступом в контролируемые здания, зоны и помещения. В ПО реализованы следующие функции СКУД[16].

1. **Разрешение на проход**. Система разрешает проход только по тем ключам, коды которых были занесены в базу владельцев ключей (для комплексного режима) и в память контроллера (для автономного режима работы).
2. **Маршруты**. Назначенные владельцам ключей маршруты проходов позволяют разрешать доступ только в строго определенные помещения (в любой последовательности).
3. **Проходная.** Если в системе действует режим “Проходная” (помещение, имеющее считыватель, как на входе, так и на выходе), то доступ во все внутренние помещения будет запрещен, если ключ не был предъявлен на проходной на вход.
4. **Запрет повторного прохода**. Когда в системе задействовано два режима - “Проходная” и “Запрет на повторный проход” (*Антипасбэк*), владельцу ключа будет запрещен повторный **вход** через проходную, если он не пересек ее на выход и повторный **выход**, если он не пересек ее на вход.
5. **Два ключа**. Режим прохода в помещение только при последовательном касании считывателя двумя ключами.
6. **Шлюз**. Программно организованное помещение между двумя двухридерными дверями (считыватели по обеим сторонам двери). Проход через шлюз блокируется, если какая-либо из его дверей открыта.
7. **Временные зоны**. Задание временных зон дают возможность ограничить время доступа необходимым временным интервалом.
8. **Дисциплина**. Позволяет управлять доступом в отдельные помещения внутри здания, например, запрещать вход в другую комнату, если владелец ключа не покинул данную.
9. **Стоп-гость 1**. Система контроля над временным посетителем: выдача сообщения охране о выходе гостя (с целью забрать ключ), блокировка выхода через проходную, запрет повторного входа.
10. **Стоп-гость 2**. Этот механизм учета одноразовых карточек предусматривает использование специального оборудования, называемого Картоприемник. Картоприемник при выходе проверяет опущенные в него карточки. Постоянные кар-

[15] Если установлен соответствующий режим.

[16] Указаны только основные функции СКУД.

точки (сотрудников) возвращаются обратно, разовые карточки (гостей) остаются в приемной коробке устройства. В обоих случаях Система разрешает проход.

11. **Ключ-кнопка**. Связывание двух событий: запрет прохода по ключу и открытие двери по кнопке RTE. Например, у некоего Сидорова истек срок действия ключа, однако охранник, нажав кнопку, пускает Сидорова. В системном журнале появится сообщение «Проход разрешен по кнопке». Далее можно будет выяснить правомерно был впущен Сидоров, или нет.

12. **Ожидание прохода**. Связывание двух событий: разрешение прохода по ключу и открытие двери (срабатывание датчика двери). Если после прикладывания ключа сработал датчик двери (т.е. дверь открылась) в системный журнал запишется сообщение «Ключ предъявлен, дверь открыта» и владелец ключа будет считаться вошедшим в помещение. В противном случае появится сообщение «Ключ предъявлен» и владелец ключа для СКУД будет отсутствовать.

13. **Хозяева комнаты**. Лица, наделенные особыми правами на пользование помещением. Так, например, только для хозяев комнаты разрешен проход по двум ключам. Любой из хозяев комнаты имеет право ставить комнату на охрану и снимать ее с охраны. Также может быть включен режим запрета доступа в помещение при отсутствии его хозяев.

14. **Взлом двери**. Указанное событие генерируется в том случае, если дверь открывается без предъявления карточки (с разрешенным проходом) или нажатия кнопки.

Также существует ряд функций, доступных при работе с охранной сигнализацией.

Описанные функции системы не являются обязательными и могут быть активизированы или отключены администратором системы.

Все события Системы записываются в *Системный журнал*, в том числе и события, связанные с нарушением прав доступа. При этом в сообщении о событии указывается причина, по которой данному владельцу отказано в доступе, его фамилия, дата и время события.

4. Особенности конфигурирования Системы

Программный комплекс СКУД может приобретаться как в расчете на эксплуатацию в сети, так и для работы на локальной машине[17]. Рассмотрим оба варианта.

4.1. Сеть

Для обеспечения максимальной надежности СКУД настоятельно рекомендуется устанавливать ядро системы (*Сервер контроллеров, Сервер приложений, Системный журнал* и *Мониторинг*), а также базу данных на специально выделенный компьютер, который будем называть сервером СКУД[18].

Оптимальная сетевая конфигурация – отдельная локальная сеть, не связанная с внутренней сетью всего охраняемого объекта. В случае если это невозможно, администратор СКУД должен максимально обезопасить свой сегмент сети от про-

[17] Еще раз подчеркнем, что комплекс СКУД является сетевым, независимо от того работает он на одной или на нескольких машинах. Речь в данном случае идет лишь о лицензионных ограничениях.

[18] Смотрите пункт 1.2.

никновения извне с помощью стандартных средств безопасности Windows NT, а также не допускать исполнения таких сетевых программ, как архивирование дисков, поиск вирусов, синхронизация времени и прочих.

В сети обязательно должен быть установлен протокол TCP/IP. Все компьютеры должны видеть друг друга как по IP адресу, так и по имени ПК[19]. При необходимости[20] имена и соответствующие им IP адреса должны быть прописаны в файле hosts (системный каталог Windows\System32\Drivers\Etc).

4.2. Локальный ПК

Для небольших объектов, с числом контроллеров не более 1-2 и размером базы персонала не более 500 человек допускается работа системы на отдельном ПК[21]. Не рекомендуется запускать более одной-двух прикладных программ СКУД одновременно (в зависимости от мощности ПК).

В случае если данный компьютер планируется использовать для других работ, то оптимальным режимом работы СКУД будет автономный режим. Программа *Мониторинг* при этом может запускаться на короткое время для вычитывания событий из контроллеров и ввода новых ключей.

4.3. Многопроцессорные компьютеры

При работе на многопроцессорных машинах рекомендуется явно задавать номер процессора для исполнения каждого модуля. Особенно это касается программ комплекса, запускаемых на одном ПК.

Наиболее оптимальным является вариант, когда все модули выполняются на одном процессоре, а сервисы СУБД – на втором.

Каждая программа имеет соответствующий ключ в системном реестре (как правило, *OPTIONS\ NUMPROCESSOR*), в котором указывается номер процессора. Указанный параметр можно изменять и в программе *Редактор установок*.

5. Обновление версий ПО

Для перехода на описываемую (6) версию с более ранних версий ПО СКУД (4 и 5) необходимо выполнить процедуру конвертации базы. Необходимые программы-конверторы и описание процедуры преобразования поставляются на дистрибутивном диске.

Обновление ПО в рамках 6-ой версии осуществляется автоматически при установке новых релизов. Последние доступны на сайте фирмы-разработчика www.sevenseals.ru.

6. Обязанности администратора СКУД

Система контроля доступа представляет собой совокупность сложного электронного оборудования (контроллеры, компьютеры), линий связи (межконтрол-

[19] Т.е. выполняться команда ping.

[20] Только при явном задании IP адресов!

[21] Подобный режим работы должен быть учтен при покупке ПК – системные требования к нему должны быть увеличены.

лерные линии, локальная сеть) и программного обеспечения. Для правильной и бесперебойной работы Системы необходима ее грамотная эксплуатация, которая должна быть возложена на ответственное лицо – главного администратора СКУД.

Администратором Системы контроля доступа может быть любой опытный пользователь персонального компьютера. Для сложных конфигураций Системы (большое количество контроллеров и ПК) им должен являться системный программист или сетевой администратор.

Администратор СКУД должен:

- Тщательно изучить документацию на Систему.
- Понимать общие принципы работы оборудования (контроллеров, интерфейсного устройства Бит, взаимодействие с программным обеспечением). Хорошо представлять работу программного обеспечения.
- Участвовать в планировании Системы (количество и расположение пунктов прохода, их оснащение устройствами контроля доступа, расположение контроллеров, питание электромагнитных замков и пр.).
- Принять от монтажной организации установленное оборудование, потребовать проверку его работоспособности (запуском тестовой программы).
- Подготовить компьютеры для установки программного обеспечения СКУД согласно приведенным выше рекомендациям.
- Вместе с представителем монтажной организации или фирмой производителем программного обеспечения установить пакет программ, сконфигурировать Систему, настроить и запустить программное обеспечение, проверить работу всех модулей Системы. При необходимости установить программные модули на рабочих станциях и проверить их работоспособность.
- Создавать инструкции персоналу по работе с различными модулями.
- Обучить администраторов программы Персонал (Бюро пропусков) работе по вводу и корректировке карточек сотрудников, заданию им прав доступа, присвоению кодов ключей.
- При необходимости формировать отчеты о событиях Системы, статистике проходов, учете рабочего времени (или обучить этому ответственных лиц).
- Своевременно осуществлять резервное копирование базы данных.
- Непосредственно контактировать с монтажной организацией и фирмой производителем оборудования и программного обеспечения в случае возникновения проблем в работе Системы.

7. Изучение документации

Администратор СКУД до начала работы однозначно должен изучить документацию на Систему, поставляемую на дистрибутивном компакт диске.

Описание ПО соответствует модульному принципу построения самой Системы. Т.е. каждая программа описывается либо в отдельном документе, либо в отдельном разделе. Рекомендуется следующая последовательность чтения документации:

- Общее описание
- Программы ядра

- Установка
- Конфигурирование
- Администрирование Системы
- Документация на пользовательские модули.

8. Лицензионные соглашения

Права и обязанности правообладателя и покупателя программно-аппаратного комплекса TSS2000 изложены в Лицензионном соглашении.

Лицензии на использование СУБД *Firebird* не требуется. Подробности смотрите на:

http://www.interbase-world.com/ru/firebird/

или

http://www.ibase.ru/ibfaq.htm#freepay

Лицензии на использование мощной утилиты *IBExpert* для работы с Firebird базами данных также не требуется.

Ряд параметров конфигурации СКУД проверяется во время ее работы. Контролю с целью предотвращения несанционированого использования комплекса в целом или его отдельных компонентов подлежат, например, число и адреса контроллеров, размер базы сотрудников, число клиентских мест, использование ряда модулей, не входящих в стандартную поставку. Мы заранее приносим свои извинения за некоторые неудобства, связанные с политикой защиты, однако подобная защита является общемировой практикой. Если у вас возникли проблемы с работой комплекса из-за несоответствия лицензионных параметров срочно связывайтесь со своими поставщиками или с фирмой разработчиком ПО (http://www.sevenseals.ru/contacts/index.html).

9. Решение проблем

По всем вопросам функционирования СКУД (работа контролеров, исполнительных устройств, датчиков, считывателей, программного обеспечения) следует обращаться к представителю организации, осуществлявшей монтаж и настройку Вашего оборудования.

Если Вы приобретали оборудование и ПО непосредственно у фирмы-разработчика и состоите на гарантийном или послегарантийном обслуживании, то имеете право обращаться непосредственно на фирму по указанным на титульном листе телефонам или по электронной почте.

Все переговоры по вопросам функционирования оборудования и программного обеспечения ведутся только с главным администратором[22] СКУД.

Перед звонком необходимо:

- подготовить информацию о характеристиках компьютера (компьютеров), операционной системе, локальной сети, количестве и типе установленных контроллеров, конфигурации Системы,
- четко сформулировать проблему,

[22] Требования к администратору указаны в п.6 данного руководства.

- расположиться перед компьютером, на котором установлено ядро Системы.

В случае нарушения требований данного документа по установке и эксплуатации комплекса Вы лишаетесь права на гарантийное обслуживание.

Схема №1: "Классическая" схема комплексной системы безопасности на основе оборудования "Семь Печатей ТСС"