

**Инструкция по монтажу
Система контроля и управления доступа
ForSec.
часть I [из 3-х]**

Содержание.

- 1 Введение.**
 - 1.1 Управление доступом.**
 - 1.2 Контроль обратного прохода.**
 - 1.3 Контроль повторного прохода.**
 - 1.4 Зона доступа.**
 - 1.5 Временные зоны.**
 - 1.6 Уровень доступа.**
- 2 Обзор системы управления доступа ForSec.**
 - 2.1 Назначение системы.**
 - 2.2 Основные возможности системы.**
 - 2.2.1 Применяемые идентификаторы и считыватели.**
 - 2.2.2 Управление доступом.**
 - 2.2.3 Картотека владельцев ключей идентификаторов.**
 - 2.2.4 Ограничение доступа операторов к приложениям ПО.**
 - 2.2.5 Мониторинг объектов. поэтажные планы.**
 - 2.2.6 Охранно-пожарная сигнализация.**
 - 2.2.7 Сохранение, просмотр и архивация информации о событиях**
 - 2.2.8 Отчеты.**
 - 2.2.9 Конфигурирование системы**
 - 2.2.10 Программное обеспечение**
- 3 Состав системы ForSec.**
 - 3.1 Контроллер доступа (панель).**
 - 3.1.2 Основные характеристики контроллеров доступа.**
 - 3.1.3 Контроллер доступа FS-2-W, FS-2WT.**
 - 3.1.4 Контроллер доступа FS-4W, FS-4WT.**
 - 3.1.5 Установка DIP переключателей контролера.**
 - 3.1.6 Подключение к сети интерфейса RS485.**
 - 3.1.7 Подключение считывателя и датчиков к контроллерам системы.**
 - 3.1.8 Типовые структурные схемы подключения исполнительных устройств.**
 - 3.1.9 Правила заземления контроллеров.**
 - 3.1.10 Рекомендации по использованию проводов.**
 - 3.1.11 Зависание контроллеров.**
 - 3.2 Сетевые контроллеры FS-CT, FS-Eth. Требования к сети интерфейса RS-485.**
 - 3.2.1 Сетевой контролер FS-CT.**
 - 3.2.2 Сетевой контролер FS-Eth.**
 - 3.2.3 Репитер интерфейса RS-485 FS-P-485.**
 - 3.2.4 Правила соединения устройств системы ForSec по сети интерфейса RS-485.**
 - 3.3 Модемы в системе ForSec.**
 - 3.4 Интерфейсные модули.**
 - 3.4.1 Интерфейсный модуль входов FS-I-08**
 - 3.4.2 Интерфейсный модуль реле FS-R-07**
 - 3.4.3 Интерфейсные модули охранно-пожарные**
- 4. Инсталляция системы ForSec на объекте.**
 - 4.1 Подключение считывателей и исполнительных устройств.**
 - 4.2 Правила создания сети контроллеров доступа.**

1 Введение.

Доступ — перемещение людей, транспорта и других объектов в (из) помещения, здания, зоны и территории.

Управление доступом — это автоматизированное управление входом в любую область (помещение), который может быть закрыт при помощи замка (преграды) и ключа (идентификатора). Вход разрешается только уполномоченному персоналу в разрешенное время. Т.е. когда осуществляется санкционированный доступ.

Идентификация — процесс опознавания субъекта или объекта по присущему ему или присвоенному ему идентификационному признаку.

В отличие от простейших систем ограничения доступа (любое запирающее устройство), электронные системы управления доступом позволяют решать задачи запрещения использования утерянного ключа идентификатора, назначения гибкого времени разрешения прохода, ведение мониторинга событий, поиска персонала по помещениям (областям) объектам и т.д.

Принцип функционирования системы контроля и управления доступом следующий: Каждый сотрудник, клиент, посетитель фирмы получает идентификатор (электронный ключ) - пластиковую карточку или брелок с содержащимся в ней индивидуальным кодом. "Электронные ключи" выдаются в результате регистрации перечисленных лиц с помощью средств системы. Паспортные данные, фото (видеоизображение) и другие сведения о владельце "электронного ключа" заносятся в персональную "электронную карточку". Персональная "электронная карточка" владельца и код его "электронного ключа" связываются друг с другом и заносятся в специально организованные компьютерные базы данных. У входа в здание или в подлежащее контролю помещение устанавливаются считыватели, считывающие с карточек их код и информацию о правах доступа владельца карты и передающие эту информацию в контроллер системы.

В системе каждому коду поставлена в соответствие информация о правах владельца карточки. На основе сопоставления этой информации и ситуации, при которой была предъявлена карточка, система принимает решение: контроллер открывает или блокирует двери (замки, турникеты), переводит помещение в режим охраны, включает сигнал тревоги и т.д.

Все факты предъявления карточек и связанные с ними действия (проходы, тревоги и т.д.) фиксируются в контроллере и сохраняются в компьютере. Информация о событиях, вызванных предъявлением карточек, может быть использована в дальнейшем для получения отчетов по учету рабочего времени, нарушениям трудовой дисциплины и др.

1.1 Управление доступом.

В простейшем случае система управления доступом блокирует одну точку доступа (прохода).

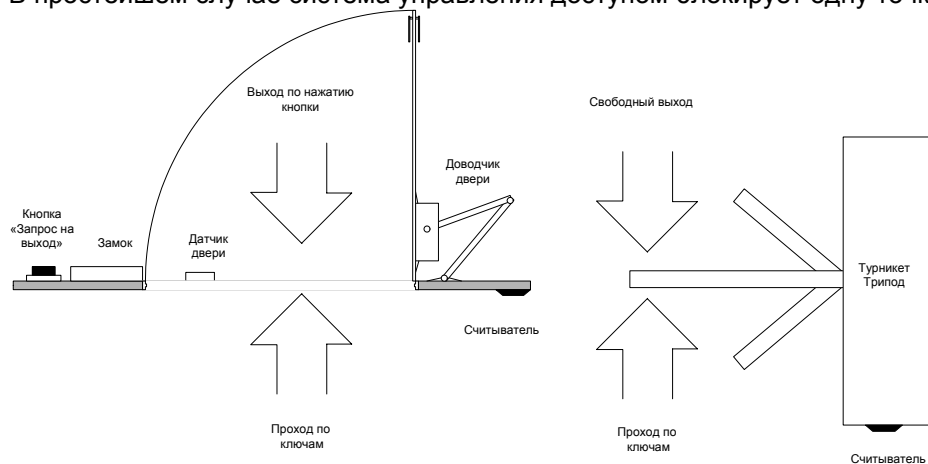


Рис. Блокирование одной точки доступа.

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

В общем случае точка доступа оборудуется устройством, обеспечивающим физическое препятствие доступу людей, транспорта и других объектов и оборудованные исполнительными устройствами для управления их состоянием (двери, ворота, турникеты, шлюзы, проходные кабины и т. п. конструкции).

Данная схема проверяет полномочия сотрудника при входе в помещение и имеет свободный проход в обратную сторону, т.е. выход сотрудников в обратную сторону осуществляется без проверки их полномочий. В качестве исполнительных устройств ограничения доступа в настоящее время используются электромеханические замки, электромеханические защелки, электромагнитные замки, турникеты различных конструкций, шлагбаумы, шлюзовые кабины.

1.2 Контроль обратного прохода.

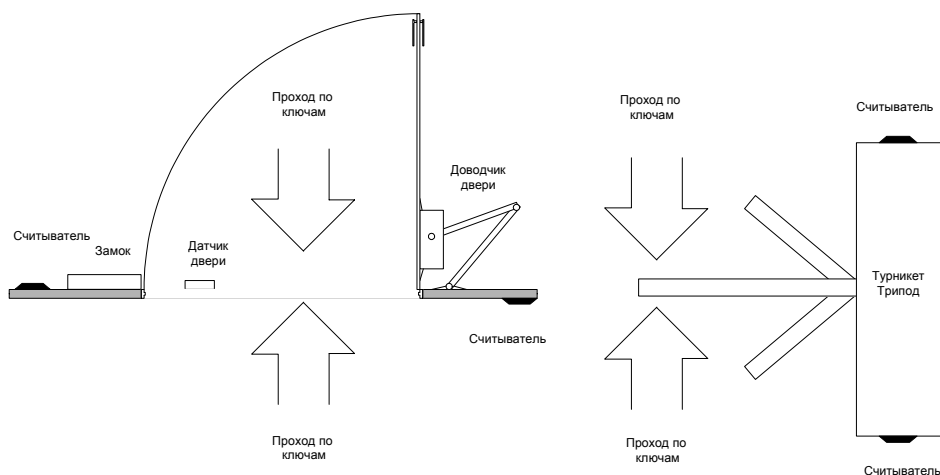


Рис. Организация функции контроль обратного прохода.
Данная схема проверяет полномочия сотрудника как при входе, так и при выходе из помещения.

1.3 Контроль повторного прохода «antipassback».

Запрет повторного прохода «antipassback» - это запрет на пропуск через одну и ту же точку прохода пользователя, не вышедшего из помещения. Естественно, эта возможность существует только для полностью контролируемой точки прохода, так как понять, что человек вошел, но не вышел, можно только на проходе, оборудованном двумя считывателями на вход и на выход. Функция запрета двойного прохода введена для того, чтобы затруднить передачу идентификатора другому лицу. Логично использовании данной функции при использовании устройств разделяющих поток людей по одному (турникеты, шлюзы) а также на объектах все входы на которые оборудованы СКУД. Система ForSec позволяет организовать данную функцию на аппаратном уровне (в пределах одного контроллера доступа) «жестко», карта «вторично» не активирует исполнительное устройство, «мягко» т.е. проход разрешается, но охрана предупреждается о факте «повторного входа». При этом следует учитывать, что для системы при «аппаратном» КПВ повторное поднесение карты является повторным проходом, независимо от того был проход совершен или нет.

В пределах крупного объекта возникает необходимость в организации функции КПВ программными методами, т.е. в тех случаях, когда есть возможность покинуть объект через другой выход. Также «программный» КПВ рекомендуется применять при включении функции «подтверждение прохода». При этом система ForSec игнорирует поднесение карты (проход не регистрируется), если в течение установленного времени не происходит подтверждение прохода.

1.4 Зона доступа.

Часть территории объекта, вход/выход на которую осуществляется под контролем СКУД.

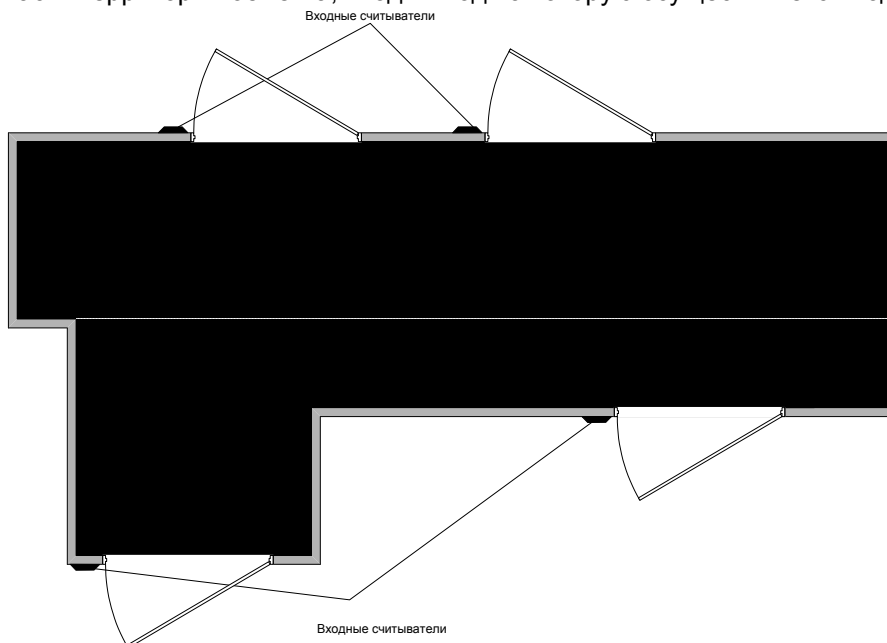


Рис. Организация СКУД в помещении с несколькими точками прохода.

Введение понятия зона доступа позволяет решать задачу контроля повторного входа сотрудника в помещение (и повторного выхода из него) при нескольких точках прохода. Также разбивка объекта на зоны доступа позволяет ввести поиск (мониторинг) нахождения сотрудника в пределах объекта. Необходимым условием создания зон доступа являются считыватели, установленные с обеих сторон точек прохода. Точка прохода с кнопкой выхода не может разделять две зоны.

Зона доступа описывается входными и выходными считывателями. При описании зон доступа необходимо учитывать, что считыватель может быть входным в одну зону доступа и выходным в одну зону доступа. Вложенные друг в друга зоны доступа являются ошибочным описанием объекта и не имеют смысла.

На объекте необходимо четко описывать зоны доступа, учитывая такую зону как внешнее пространство. Т.е. сотрудник покинувший объект находится, к примеру, в зоне доступа "Улица".

1.5 Временные зоны.

Введение понятия «временные зоны» позволяет решать задачи реализации запрета и разрешения доступа сотрудников в помещения, зоны в зависимости от времени суток и календарных дат. В простейшем случае разрешение доступа на объект в рабочее время и запрет в нерабочее время, в т.ч. в зависимости от дня недели.

Система ForSec по умолчанию имеет временные зоны Всегда и Никогда.

Аппаратура, применяемая в системе ForSec, поддерживает 64 временные зоны, каждая до 8 временных интервалов, и до 256 праздников в год (тип 1, тип 2). Это позволяет организовать на объекте доступ сотрудников по сменам и перенос рабочих дней на выходные.

1.6 Уровень доступа.

Уровень доступа – параметр, описываемый временной зоной и считывателями через которые разрешен проход. Уровень доступа является основным при назначении карт идентификаторов конкретным владельцам. Именно этот параметр ограничивает возможности владельца карты по доступу в различные помещения. Система ForSec по умолчанию имеет два случая НИГДЕ и ВЕЗДЕ. Пользователь (администратор) системы может назначать любые уровни доступа: «Гостевой», «Временный» и т.д.

2 Обзор системы управления доступа ForSec.

2.1 Назначение системы.

Интегрированная система контроля и управления доступа ForSec (далее система или СКУД) предназначена для осуществления автоматического и/или автоматизированного контроля и управления доступом на объектах различного масштаба – от небольшого офиса до групп объектов разнесенных территориально.

Помимо управления доступом, система способна контролировать различные датчики устройств автоматики здания, охранно-пожарной сигнализации по средствам входящих в номенклатуру различных интерфейсных модулей, что позволяет обеспечить комплексную автоматизацию и защиту объекта. Информация о состоянии датчиков постоянно выводится на компьютеры мониторинга, заносится в архив событий и может быть использована для управления исполнительными устройствами от средств сигнализации до устройств автоматики и установок пожаротушения.

2.2 Основные возможности системы.

2.2.1 Применяемые идентификаторы и считыватели.

В качестве "электронных ключей", выдаваемых сотрудникам и посетителям организации для прохода в защищаемые помещения, в системе ForSec могут использоваться идентификаторы самых различных типов - Touch Memory (iButton), Proximity-карты, Wiegand-карты и т.д. Контактные ключи Touch Memory (iButton) или считыватели с данным выходным форматом подключаются к некоторым моделям контроллеров доступа системы ForSec.

Для считывания и ввода кода идентификаторов в составе системы могут применяться считыватели отечественного производства, а также устройства известных фирм: Motorola, HID и т.д. Для повышения уровня секретности применяются считыватели совмещенные с клавиатурой.

Ряд считывателей в системе может использоваться для постановки/снятия с охраны шлейфов сигнализации интерфейсных модулей. В этом случае считыватели с клавиатурой используются как для доступа, так и для управления охранно-пожарной сигнализацией.

Главным параметром при выборе модели считывателей является выходной стандарт данных Wiegand 26, Wiegand 34 или Wiegand 44. При использовании идентификаторов формата Touch Memory (iButton) на аппаратном уровне происходит преобразование этого формата данных в формат данных Wiegand.

2.2.2 Управление доступом.

Автоматическое управление доступом в помещения и здания, контролируемые системой, осуществляется на основе уровня доступа владельца ключа идентификатора, задаваемого администратором системы, уполномоченными сотрудниками службы безопасности, сотрудником отдела кадров и т.д. Ограничения могут задаваться как для отдельных владельцев ключей, так и для групп владельцев, выделенных по какому-либо признаку. Для каждого из зарегистрированных в системе ключей можно определить срок его действия. Информация об уровне доступа ключей идентификаторов хранится в контроллерах доступа, где и происходит сверка параметров ключа с разрешенными полномочиями. Функционирование СКУД не зависит от работоспособности компьютеров входящих в систему. В простейшем случае компьютер служит только для задания структуры конфигурации аппаратуры, регистрации карт, назначения карт уровня доступа.

2.2.3 Картотека владельцев ключей идентификаторов.

Программное обеспечение системы позволяет устанавливать ограничения доступа, регистрировать постоянных сотрудников, клиентов, гостей и посетителей объекта и сохранять сведения о них в базах данных.

Регистрации человека в системе при выдаче идентификатора – это создание персональной учетной карточки. Помимо различной текстовой информации о владельце, в "электронной карточке" можно вставить изображение владельца идентификатора, полученное с помощью электронного фотоаппарата или из файла изображения.

Быстрота и эффективность регистрации позволяет выдавать идентификаторы не только постоянному персоналу, но и организовать в Бюро пропусков выдачу идентификаторов посетителям и гостям в качестве временных или разовых пропусков.

При большом количестве выданных идентификаторов возникает необходимость быстрого поиска информации в базе данных их владельцев. Программное обеспечение ForSec позволяет производить поиск и отбор "карточек" по самым различным критериям и в общем случае оказывает неоценимую помощь службе кадров.

2.2.4 Ограничение доступа операторов к приложениям ПО.

Администратор системы может самостоятельно задавать к каким именно приложениям ПО ForSec имеет доступ каждый из операторов, и в каком режиме (в режиме пользования или в режиме полного доступа). Т.е. изменения баз данных возможно только уполномоченными представителями.

2.2.5 Мониторинг объектов. поэтажные планы.

Информация о событиях, связанных с доступом в контролируемые помещения и работой оборудования, отображается в реальном масштабе времени на экранах ПК на которых установлено программное приложение «монитор».

Текстовые сообщения о событиях (входах, выходах конкретных лиц, взломах дверей, предъявлении незарегистрированных идентификаторов, срабатываниях датчиков и т.д.) могут дублироваться речевыми сообщениями и показом фотографии владельца предъявленного идентификатора.

В случае предъявления идентификатора в момент, когда для его владельца действует какое-либо из ограничений доступа, истек срок действия идентификатора или при предъявлении незарегистрированного идентификатора, в сообщении о событии указывается причина, по которой данному владельцу отказано в доступе.

При необходимости проводить визуальный мониторинг объектов, - отслеживать события и управлять доступом, - можно также и в режиме отображения поэтажных планов, на которых наглядно отображается ситуация в здании. Только не в версии ForSec-Lite.

Контролируемые объекты (датчики, считыватели и т.д.) обозначаются на планах пиктограммами или значками, вид или цвет которых может меняться в зависимости от состояния соответствующего объекта.

В момент возникновения нештатного события, на экране компьютера, автоматически или по команде пользователя, разворачивается план нужного этажа, на котором указывается место или объект, с которым связано тревожное событие.

После принятия решения, оператор системы с помощью клавиатуры компьютера, мыши или выносного пульта исполнительного устройства, может дистанционно открыть или заблокировать какую-либо отдельную дверь, открыть все двери в случае пожара или заблокировать их в момент нападения, активизировать системы пожаротушения, включить сирену и т.д.

Если система имеет достаточно сложную структуру и контролирует большое количество объектов, расположенных в многоэтажном здании или нескольких отдельных зданиях, планы этажей имеют иерархическую структуру типа "Общий - Подробный". В этом случае ситуация в здании или зданиях отображается на общем, схематичном плане, а при возникновении экстренного события раскрывается подробный план соответствующего этажа или помещения.

2.2.6 Охранно-пожарная сигнализация.

Система ForSec способна контролировать самые различные охранные и пожарные извещатели. Срабатывание какого-либо датчика, какой-либо зоны, вызывает появление текстового и речевого сообщения и фиксируется в журнале событий.

В момент срабатывания датчика, система автоматически, в соответствии с заранее заданной реакцией системы, может включить или выключить то или иное устройство (например, сирену, насосы пожаротушения, разблокировать двери, и т.п.)

Информация о факте и месте срабатывания датчиков выводится на поэтажных планах здания а также заносится в журнал событий. Дежурный сотрудник охраны может самостоятельно отдать команду исполнительным устройствам системы.

Интерфейсные модули охранно-пожарные могут подключаться к любому контроллеру доступа (панели), т.е. располагаться в любой точке объекта. Что сокращает число проводных линии (шлейфов сигнализации).

Централизованная постановка и снятие с охраны осуществляется с рабочего места (компьютера) дежурного оператора. Кроме этого, отдельные помещения или этажи могут ставиться и сниматься с охраны уполномоченными сотрудниками организации. В последнем случае, постановка и снятие может осуществляться, например, после предъявления персонального идентификатора и/или набора кода с помощью клавиатуры. Например, при использовании считывателей, совмещенных с клавиатурами, сотрудник должен сначала набрать код, а затем предъявить считывателю свой идентификатор. Либо в системе выделяется специальный считыватель (без клавиатуры) на управления системой ОПС.

Информация о том, какие помещения и проходы находятся под охраной или сняты с охраны наглядно отображается на поэтажных планах здания.

2.2.7 Сохранение, просмотр и архивация информации о событиях

В процессе мониторинга контролируемых объектов, информация обо всех событиях, связанных с доступом в контролируемые помещения, датчиками сигнализации и работой системы, а также связанные с действиями операторов, фиксируется в базе данных, хранящейся на жестком диске компьютера-сервера.

В любой момент времени информацию об этих событиях можно просмотреть на экране компьютера и распечатать в виде отчетов.

В любой момент времени база данных может быть заархивирована. Благодаря этому, в системе может сохраняться информация о событиях за длительные периоды времени.

2.2.8 Отчеты.

На основе баз данных с помощью специальных программных модулей, входящих в состав программного обеспечения системы, можно легко сформировать различные отчеты о событиях доступа и работе оборудования. В частности: отчеты об экстренных или всех событиях за какой-либо период времени; о событиях связанных с каким-либо конкретным человеком или помещением; о рабочем времени персонала; о времени прихода сотрудников на работу, отчеты дежурной смены службы безопасности и т.д.

Полученные отчеты можно тут же просмотреть на экране компьютера, использовать в других приложениях (например, в MS Excel) и распечатать на принтере для дальнейшего анализа.

2.2.9 Конфигурирование системы

С помощью программного обеспечения системы можно самостоятельно задать схему подключения элементов, установки и режимы работы системы в целом и ее отдельных подсистем, изменять заданные параметры при изменении конфигурации и расширении состава оборудования системы, создавать различные виды реакции системы на события и т.д.

Благодаря универсальности основного оборудования, система легко расширяется, позволяет подключать новые устройства.

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

2.2.10 Программное обеспечение

В зависимости от требований пользователя поставляется или однопользовательская версия для работы на одном компьютере, или же многопользовательская версия (на несколько рабочих станций в сети, объединенных единой базой данных), а также наличием или отсутствием функциональных возможностей (полная версия и версия Lite) и дополнительных приложений («Учет рабочего времени»). В случае многопользовательской версии в сети компьютеров

выделяется «сервер» для хранения баз данных. Остальные ПК являются рабочими станциями. Все функции по управлению и настройке системы доступны с любой рабочей станции и сервера. Максимальное количество одновременно работающих ПК в системе ForSec определяется при заказе системы. Однако ПО ForSec может быть установлено на большее количество ПК. Ограничение действует на одновременную работу ПК в системе.

Программный комплекс системы состоит из 6-ти основных приложений:

«Администратор» - предназначен для регистрации комплекса, работы со списком пользователей программного комплекса, задания для каждого из них прав доступа к возможностям программирования параметров системы. Также данное приложение позволяет настроить общие параметры работы с базами данных всех приложений, а также проводить архивирование и разархивирование данных, перерегистрацию комплекса.

«Сервер» - это единственное приложение в составе пакета, которое непосредственно работает с аппаратурой. Оно осуществляет обработку входных событий системы, помещая их в журнал событий и входных событий, посылая их контроллерам доступа через сетевой контроллер непосредственно подключенного к COM порту компьютера. Все взаимодействия других приложений с устройствами системы осуществляется через «Сервер». Т.е. после регистрации комплекса, необходимым условием работы системы является постоянная работа приложения «Сервер». Чаще всего через меню Автозапуск операционной системы.

«Конфигуратор» - используется для полного описания всей системы с указанием аппаратуры, обучения системы картам индентификаторам, визуальной разработки схемы мониторинга, задания временных зон, уровней доступа, зон доступа, групп охранных зон, праздников, планов помещения.

«Картотека» - предназначена для работы с информацией о сотрудниках предприятия имеющих карты индентификаторы и других владельцах карт. Здесь осуществляется выдача и возврат карт, назначается уровень доступа карт. «Картотека» включает графический редактор для разработки внешнего вида карт (бэджинг) и модуль работы с цифровой камерой.

«Монитор» - обеспечивает наглядный и удобный мониторинг событий с возможностью видеоиндентификации и просмотра событий системы в реальном времени, регистрируя тревожные события. Программа предоставляет возможность непосредственного управления и получения подробной информации о состоянии объектов системы, таких как панели, считыватели, зоны доступа и др.

«Генератор отчета» - предназначен для просмотра и вывода на печать событий системы. Все события можно разделить на две категории: программные события – сообщения при работе с аппаратурой. Пользователь может получать отчеты как по сообщениям одного типа, так и по комбинации различных типов, одновременно устанавливая отбор по времени, карте, объекту системы, владельцу карт и др. параметрам.

3 Состав системы ForSec.

Система ForSec представляет объединение аппаратных и программных средств. Основой аппаратной части системы являются контроллеры доступа (панели). К панелям подключаются дополнительное оборудование – считыватели, исполнительные устройства, устройства управления, интерфейсные модули. Аппаратная конфигурация, логика работы, уровни пользователей, уровень доступа посетителей задаются программным обеспечением с ПК. Для связи сети контроллеров доступа (панелей) с ПК служат сетевые контроллеры, преобразующие интерфейс RS-485 сети панелей в интерфейс обмена данными с ПК. Также в процессе функционирования системы через сетевые контроллеры осуществляется постоянный обмен служебной и пользовательской информацией между ПК и сетью контроллеров доступа при развитой СКУД. Для увеличения длины линии связи панелей, гальванической развязки сегментов линии, создания сложной структуры служат репиторы интерфейса RS-485. В случае необходимости организации удаленных объектов в систему включаются модемы под различные линии связи. Для интеграции с системами охранно-пожарной сигнализации и автоматики служат интерфейсные модули различного назначения.

Состав системы ForSec.

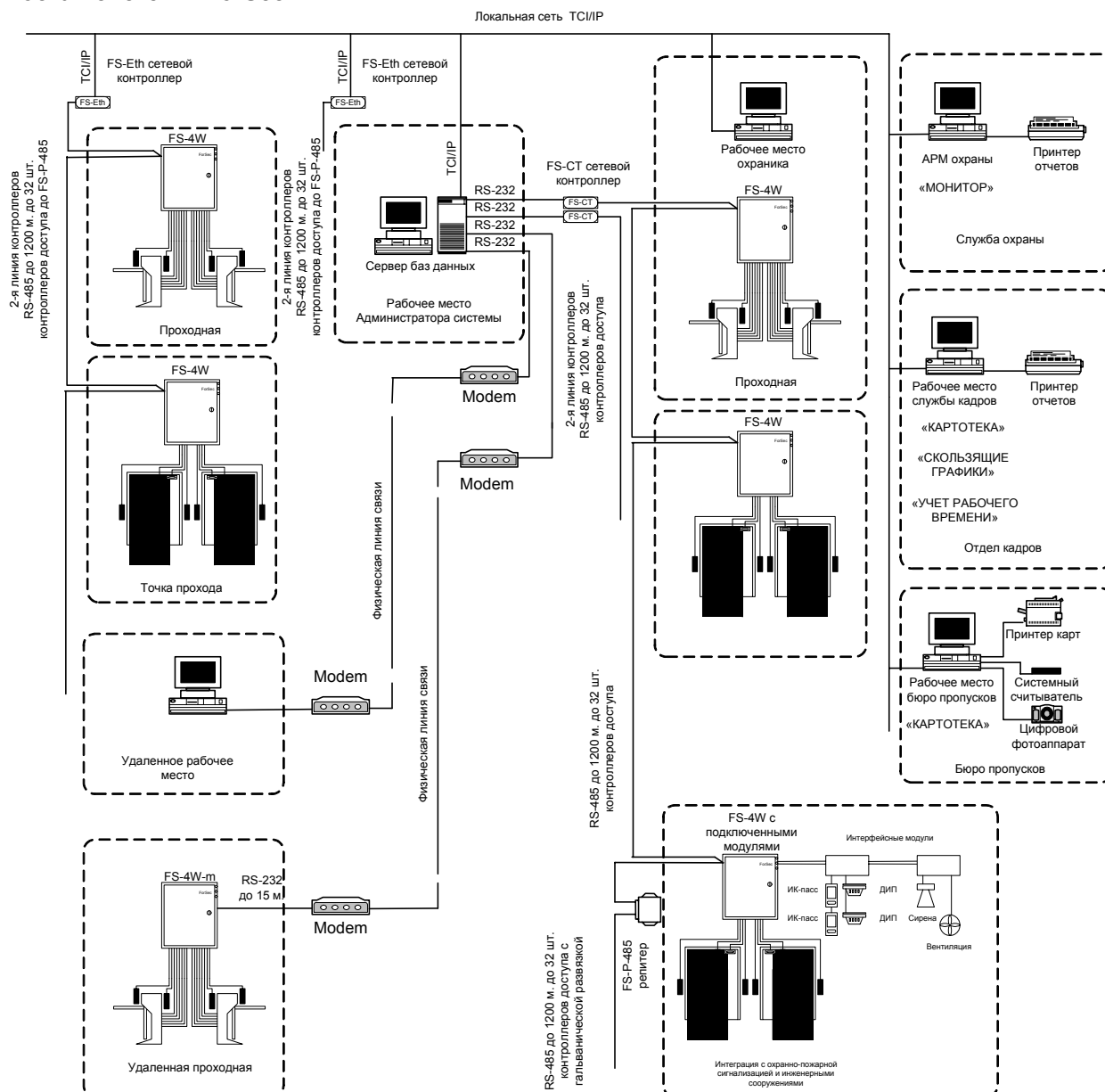


Рис. Пример построения системы контроля доступа на оборудовании ForSec.

Основная аппаратура системы ForSec.

Контроллеры доступа (панели) FS-2..., FS-4W..., FS-8W.

Назначение:

- Получение информации от считывателей
- Принятие решение о разрешении доступа
- Управление исполнительными устройствами
- Сбор информации от интерфейсных модулей
- Управление интерфейсными модулями
- Обмен информацией (при наличии связи) с сетью контроллеров доступа и ПК

Номенклатурный ряд на настоящий момент содержит контроллеры на 2/4/8 считывателя.

Сетевой контроллер FS-CT.

Назначение: организация интерфейса между сетью контроллеров работающих по интерфейсу RS485 и ПК с входом интерфейса RS232 для контроллера FS-CT, или подключения сети контроллеров работающих по интерфейсу RS-485 в локальную сеть Ethernet компьютеров для сетевого контроллера FS-Eth. При использовании контроллера FS-CT, из-за ограничения длины линии интерфейса RS-232, контроллер подключается к компьютеру баз данных системы.

Сетевой контроллер FS-Eth.

Назначение: организация интерфейса между сетью контроллеров работающих по интерфейсу RS485 и сетью по протоколу TCP/IP (локальную сеть Ethernet компьютеров и другого оборудования). IP адрес контроллера FS-Eth присваивается через прилагаемое ПО. Таким

образом снимается ограничение по максимальной удаленности сервера баз данных от сети контроллеров доступа. Сеть контроллеров доступа может быть удаленна от сервера баз данных, и для связи с ним использовать доступные каналы связи.

Считыватели.

Назначение: преобразование кода ключей идентификаторов в стандартные форматы входных данных контроллеров доступа (Wiegand 26, Wiegand 34, Wiegand 44).

Репитеры интерфейса RS-485 FS-P-485.

Ограничение нагрузочной характеристики сети RS-485 ограничивают длину линии до 1200м, а также накладывают ограничения на количество абонентов сети интерфейса RS-485. Репитеры интерфейса RS-485 позволяют наращивать линию связи, либо вводить ответвления а также обеспечивают гальваническую развязку между сегментам линии интерфейса RS-485.

Интерфейсные модули FS-I-08, FS-R-07, FS-S-04, FS-S-08.

В общем случае получение информации о состоянии извещателей охранно-пожарной сигнализации, датчиков систем автоматизации и а также управление исполнительными устройствами.

Исполнительные устройства.

Устройства блокирования точек прохода, а также устройства автоматики и сигнализации.

Модемы.

Связь с удаленными средствами СКД ForSec.

Дополнительная аппаратура для применения с системой ForSec.

Принтер карт.

В соответствии с типом приобретенных карт может быть осуществлена непосредственная печать на тонкие карты (толщиной от 0,25 до 1,5 мм) или на наклейки для последующего крепления на толстых картах (толщиной более 1,2 мм).

Любая информации по желанию заказчика может быть нанесена на карты идентификаторы. Карты будут содержать всю необходимую информацию: фото сотрудника, ФИО, фирма, отдел, табельный номер, уровень полномочий, уровень доступа и т.д. Карты идентификаторы заменяют собой ранее применявшиеся на объекте бумажные пропуска. В ПО ForSec встроен модуль разработки макетов и печати на пластиковых картах.

Цифровой фотоаппарат.

Автоматизация создания базы данных по сотрудникам. Далее фото сотрудников применяются для печати пропусков и процесса фотоидентификации на проходных.

ПО ForSec имеет встроенный модуль работы с цифровым фотоаппаратом, который позволяет редактировать файлы с целью оптимизации изображений. Следует понимать, что база данных будет медленно работать с файлами больших размеров. Поэтому выбирайте компромисс между размером файла и требуемым качеством изображений.

3.1 Контроллер доступа (панель).

Основой системы ForSec является контроллер (панель) управления доступом. В зависимости от модификации контроллер осуществляет полный мониторинг от 2 до 8 точек прохода и принимает решение о разрешении на проход. Контроллер накапливает информацию о точках прохода и по средством сети RS-485 передает информацию на объектовый уровень.

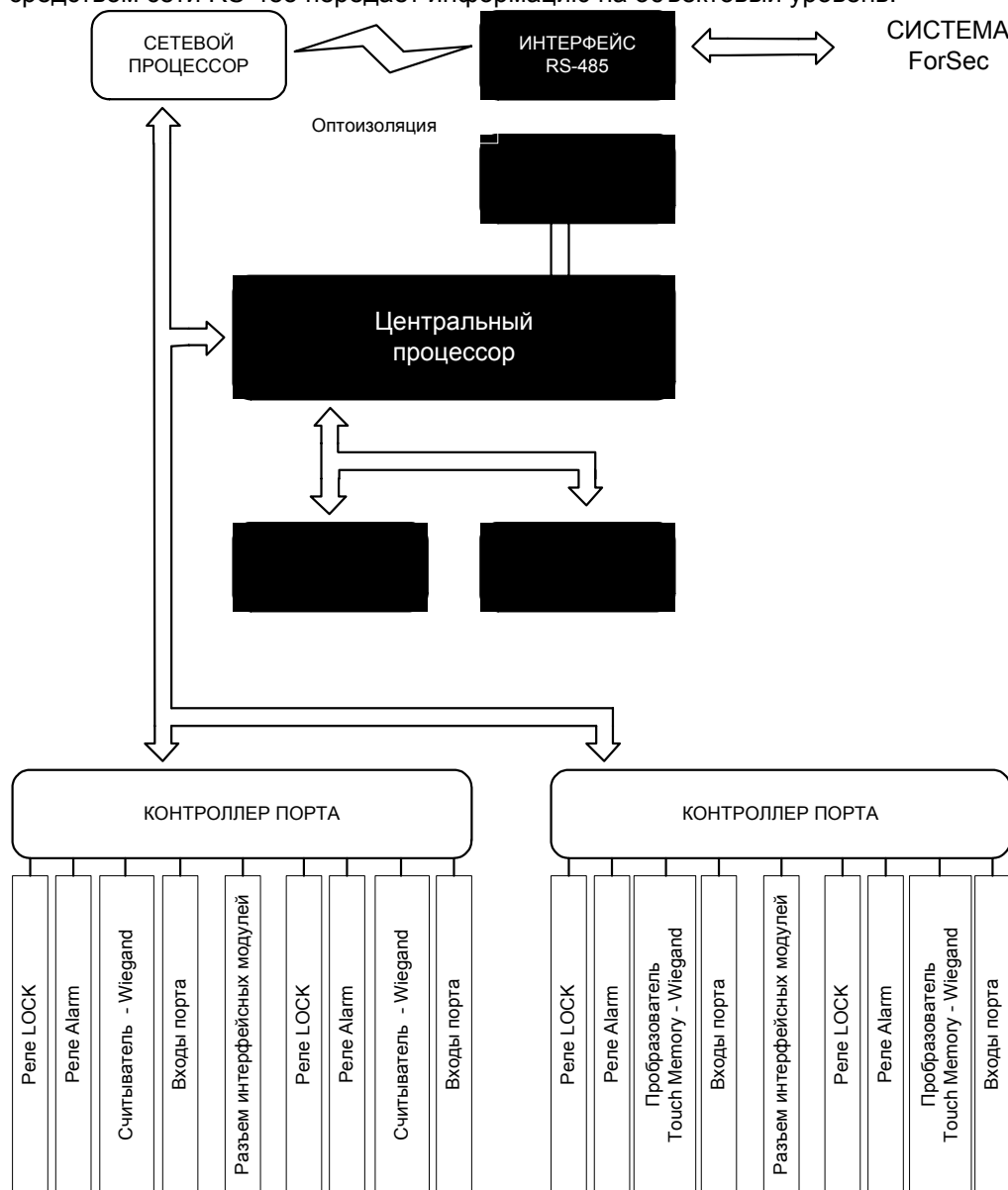


Рис. Структура контроллера доступа.FS-4W.

Каждый контроллер содержит следующие функциональные модули:

- Центральный процессор (Мастер процессор)
- Память карт (Flash-память)
- Память событий (Энергонезависимая ОЗУ)
- Часы реального времени
- Сетевой процессор
- Контроллер порта
- Преобразователь интерфейса TM –Wiegand модели контроллеров с индексом WT

Центральный процессор (ЦП)

Ядро панели, осуществляющее управление всеми периферийными устройствами. ЦП выдает санкцию на проход. Получив код из порта, центральный процессор анализирует состояние памяти карт и принимает решение о разрешении на проход. Обнаружив код карты, ЦП проводит проверку дополнительных ограничений (уровень доступа, временные зоны, активность карты). Если нет условий для запрещения прохода, центральный процессор выдает команду активизации исполнительного устройства соответствующей двери. ЦП контролирует состояние входов панели. При активизации входов панель включает необходимые исполнительные устройства. Решение об

активизации выходов также принимает центральный процессор. Любое изменение в состоянии панели фиксируется в буфере событий.

FLASH-память.

Наиболее ценная информация базы данных панели хранится в энергонезависимой памяти, которая построена на компонентах типа "Disk On Chip". В этом разделе памяти помещены данные о картах и временных зонах. Отключение питания не оказывает губительного действия на содержимое Flash-памяти. Гарантированная сохранность данных составляет несколько десятков лет.

Память событий.

Оперативная обстановка в точках прохода фиксируется в фискальной памяти. Любое изменение состояния панели заносится в буфер событий. Содержимое памяти событий периодически транслируется на более высокий иерархический уровень управления. Получателем информации о состоянии панели является компьютер. Даже, если связь с РС потеряна, все фискальные данные накапливаются в энергонезависимом буфере. Благодаря большой емкости памяти событий (5000) панель ForSec может находиться в режиме "Off LINE" продолжительное время.

Часы реального времени.

Для обеспечения функционирования временных зон и привязки событий к реальному времени в панели использован специальный чип RTC. Часы питаются от отдельного литиевого источника питания. Специализированная микросхема имеет эффективную защиту от сбоев и функционирует даже, когда остальные модули системы отключены и обесточены.

Сетевой процессор.

Дополнительный коммуникационный микроконтроллер обеспечивает сервис сети PROFIBUS. Сетевой процессор обеспечивает гибкий интерфейс между физической средой сети и центральным процессором. Пакеты информации, получаемые по сети, декодируются и обрабатываются без участия центрального

Процессора. Стандарт RS485 позволяет удалять устройства на значительные расстояния друг от друга (1 200 м на сегменте). Разность потенциалов земли таких устройств может достигать сотен вольт. При разработке панели ForSec учтены реальные условия российских объектов. Поэтому для эффективной защиты от перечисленных выше ситуаций в сетевом контроллере использована полная гальваническая развязка (2500 В) электроники от физической среды сети RS485. Выпускается вариант контроллера доступа для работы с модемом или непосредственного подключения к персональному компьютеру через интерфейс RS232

Контроллер порта.

Для обслуживания портов используется контроллер порта. Контроллер порта рассчитан на обслуживание двух считывателей. Микропроцессор преобразует информацию, поступающую из интерфейса Wiegand, к виду удобному для обработки центральным процессором. Кроме того контроллер порта осуществляет мониторинг и защиту от помех всех входов. Выходы панели также обслуживаются этим микроконтроллером. Подобная архитектура позволяет легко адаптировать систему к новым протоколам и интерфейсам. В настоящее время контроллер порта поддерживает следующие стандарты и протоколы: Wiegand26(HID, Motorola), Wiegand34(HID34). Клавиатуры совмещенные со считывателями в стандартах HID и Motorola.

Преобразователь интерфейса TM -Wiegand.

Дополнительная плата устанавливается только в панелях с индексом WT. Ведение в модельный ряд панелей с индексом WT связано с большой популярностью в России электронных идентификаторов TouchMemory (в настоящее время торговая марка заменена на iButton). При всех положительных качествах, интерфейс TM имеет один серьезный недостаток – считыватель идентификаторов TouchMemory имеет электрический контакт с идентификатором. Разность потенциалов статических зарядов, возникающих при трении синтетических материалов одежды человека, могут достигать десятков киловольт. При контакте идентификатора со считывателем весь заряд, накопленный человеком, стекает в электронику панели ограничения доступа. Для защиты от статических зарядов входные цепи интерфейса TM панели ForSec имеют сложные цепи защиты и полную гальваническую развязку входных цепей интерфейса TM. Длина шлейфа от считывателя до панели может достигать расстояния более 100 метров.

3.1.2 Основные характеристики контроллеров доступа.

Исполнение	Количество Считывателей	Входы	Выходы реле	Интерфейс Wiegand	Интерфейс Touch Memory	Карт	Буфер
FS-2W	2 Prox Card	4	3	Есть	Нет	2000	5000
FS-2WT	2 Touch-Memory	4	3	Есть	Есть	2000	5000
FS-4W	4 Prox Card	12	8	Есть	Нет	10500	10800
FS-4W-x	4 Prox Card	12	8	Есть	Нет	25000	10800
FS-4WT	4 Touch-Memory	12	8	Есть	Есть	10500	10800

FS-4WT-x	4 Touch-Memory	12	8	Есть	Есть	25000	10800
FS-4W-xx	4 Prox Card	12	8	Есть	Нет	50000	10800
Входной формат данных от считывателей			Wiegand26 (HID, Motorola) Wiegand34 (HID34), Wiegand44 (HID44), Touch-Memory				
Количество временных зон			64 зоны по 8 интервалов каждая				
Количество праздников			256 праздников тип 1, тип 2				
Интерфейс для связи с компьютером			RS-485: FS-2W, FS-4W, FS-4WT RS-232: FS-4W-m, FS-4WT-m				
Поддержка интерфейсных модулей			FS-R-07 – модуль расширения на 7 реле FS-I-08 – модуль расширения входов на 8 FS-S-04 – охранно-пожарный модуль на 4 ШС FS-S-08 - охранно-пожарный модуль на 8 ШС				
Количество модулей на 1 панель доступа			FS-2W... – до 2 шт. FS-4W... – до 8 шт.				
Функции организованные на аппаратном уровне			Antipassback Доступ по двум картам Проверка кода организации «facility code» Режим работы выходов панели (импульс, инверсия, включение, выключение). Длительность импульса Время шунтирования датчиков Режим «вход под принуждением» Режим «ночной обход»				
Контакты реле управления замка LOCK			NO/NC, переменное 250В/7А, постоянное 30В/7А				
Контакты реле ALARM			NO/NC, переменное 250В/7А, постоянное 30В/7А				
Напряжение первичного питания			220 (+/-10%) 50 Гц				
Напряжение вторичного бесперебойного питания/ максимальный ток			12 В/ 2 А				
Потребляемый ток панели, без учета дополнительных потребителей по цепи питания 12В не более			FS-2W - 250 мА FS-4W - 500 мА				
Рекомендуемая емкость аккумулятора			7А/ч				
Рабочая температура			От 0 до +50С				
Влажность			95% без конденсата				
Режим работы			Круглосуточный				
Внешние габариты металлического кожуха			FS-2W 270x310x120 мм FS-4W 400x310x120 мм				

3.1.3 Контроллер доступа FS-2-W, FS-2WT.

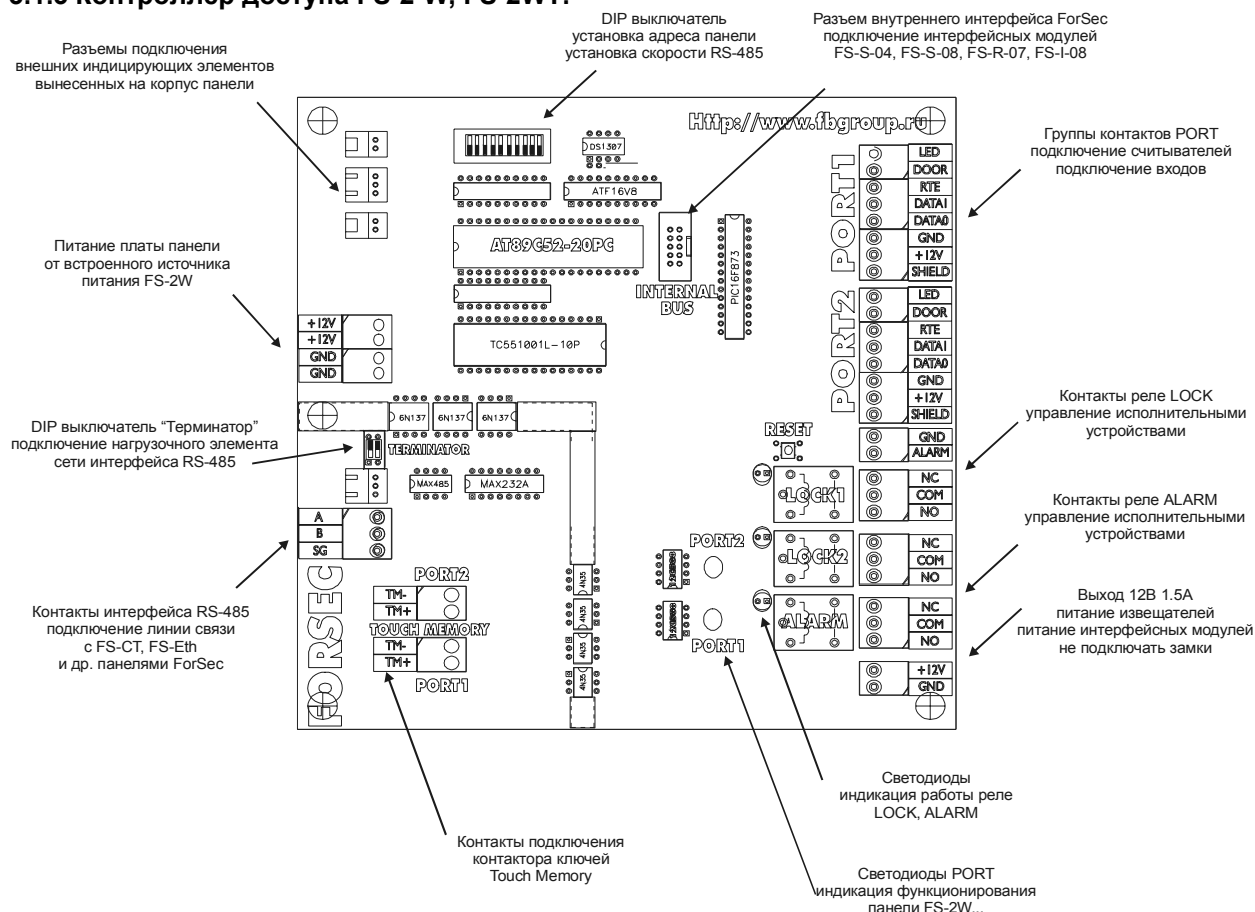


Рис. Расположение коммутационных и индицирующих элементов на плате контроллера FS-2WT.

Коммутационные разъемы и индицирующие элементы.

В правой части панели расположены 2 блока портов считывателей PORT. Ниже 2 группы контактов LOCK для подключения исполнительных устройств (замок) и тревожный выход ALARM. Конфигурирование выходов обеспечивается программным обеспечением. Работоспособность панели можно оценить с помощью светодиодных индикаторов платы. Если процессоры портов работают нормально, светодиоды PORT1, PORT2 мигают. Для удобства эксплуатации все выходы реле имеют светодиодную индикацию. Кроме перечисленных выше, на металлическом корпусе панели расположены 3 светодиода (220, 12, Mode). Редкое мигание MODE - панель в режиме автономна, частое мигание MODE панель в режиме опроса компьютером, постоянно горит MODE - разряд аккумулятора (истощение рабочего ресурса аккумулятора).

На плате расположены следующие DIP переключатели:

Адрес панели (двоичный код),
Скорость интерфейса RS485,
Терминатор интерфейса RS485, двойной.

Правила установки переключателей описаны далее. Правила создания сети интерфейса RS485 в инструкции по установке сетевого контроллера.

Модификация панели FS-2WT

Для использования в системе ключей контакторов Touch Memory на плате контроллера с индексом WT устанавливается интерфейсная плата Touch-Wiegand (представлена выше).

Контакты ключей TM подключаются к клеммам «TM - », «TM + ». Информация о состоянии платы отображается светодиодами Status. Если микропроцессоры модуля работают, светодиоды мигают. При касании идентификатора (Touch Memory) читается код, который транслируется в стандарт Wiegand 26 и передаются контроллеру.

3.1.4 Контроллер доступа FS-4W, FS-4WT.

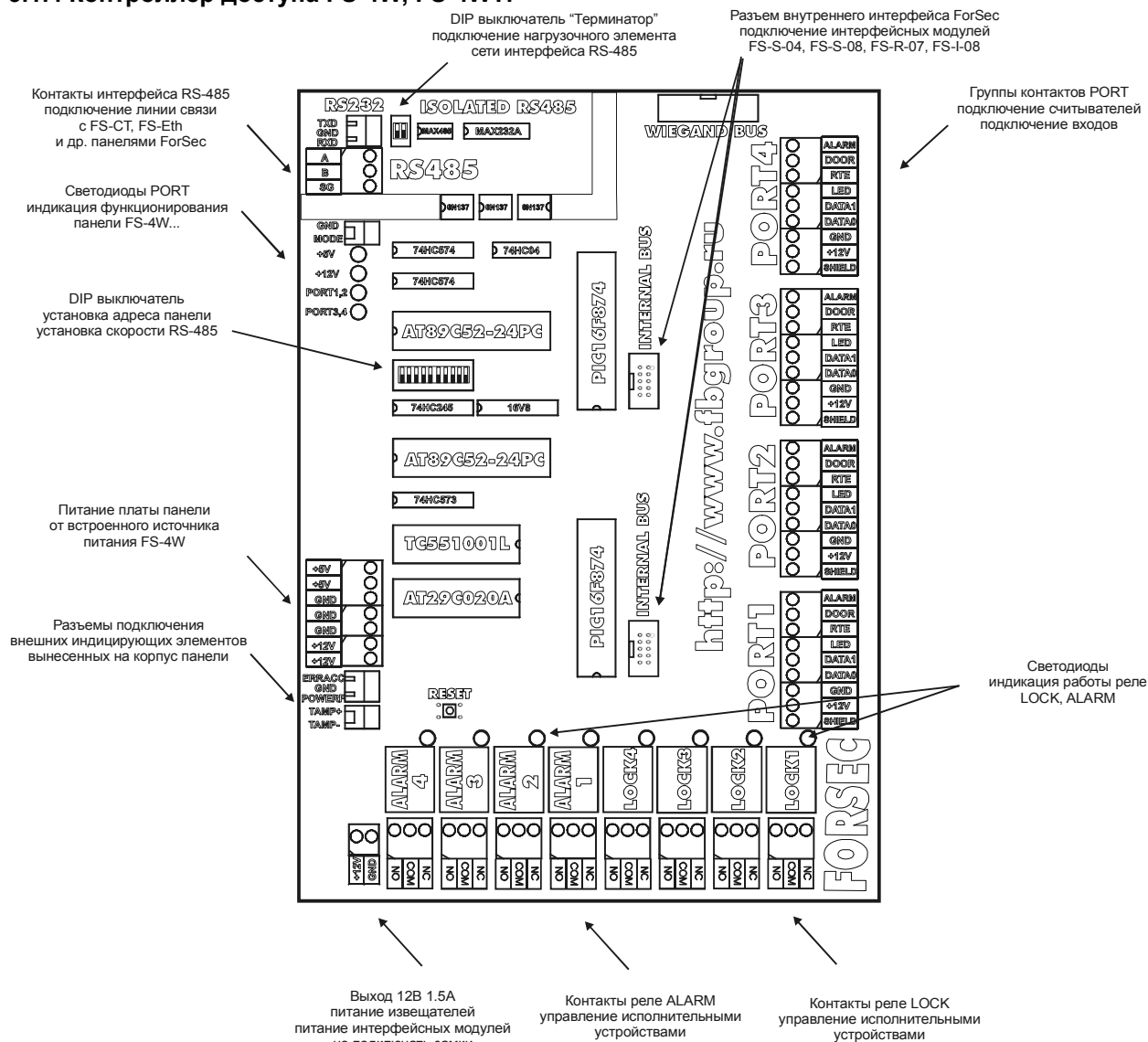


Рис Печатная плата FS-4W

Коммутационные разъемы и индицирующие элементы.

В правой части панели расположены терминальные блоки 4 портов считывателей PORT. В нижней части панели расположены 4 группы контактов LOCK для подключения исполнительных устройств 4 группы контактов ALARM. Конфигурирование выходов обеспечивается программным обеспечением. Работоспособность панели можно оценить с помощью светодиодных индикаторов. В левой верхней части панели расположены индикаторы напряжения +5V, +12V. Ниже установлены диагностические светодиоды портов PORT1,2, PORT3,4. Если процессоры портов работают нормально, светодиоды мигают.

Для удобства эксплуатации все выходы реле имеют светодиодную индикацию. Кроме перечисленных выше на корпусе панели расположены 3 светодиода (220 , 1 2 , Mode). Редкое мигание MODE - панель в режиме автоном, частое мигание MODE панель в режиме опроса компьютером, постоянно горит MODE-разряд аккумулятора (истощение рабочего ресурса аккумулятора).

На плате расположены следующие DIP переключатели:

Адрес панели (двоичный код),
Скорость интерфейса RS485,
Терминатор интерфейса RS485, двойной.

Модификация панели FS-4WT

Для использования в системе ключей контакторов Touch Memory на плате контролера с индексом WT устанавливается интерфейсная плата Touch-Wiegand Соединение платы преобразователя с панелью производится через шину Wiegand Bus.

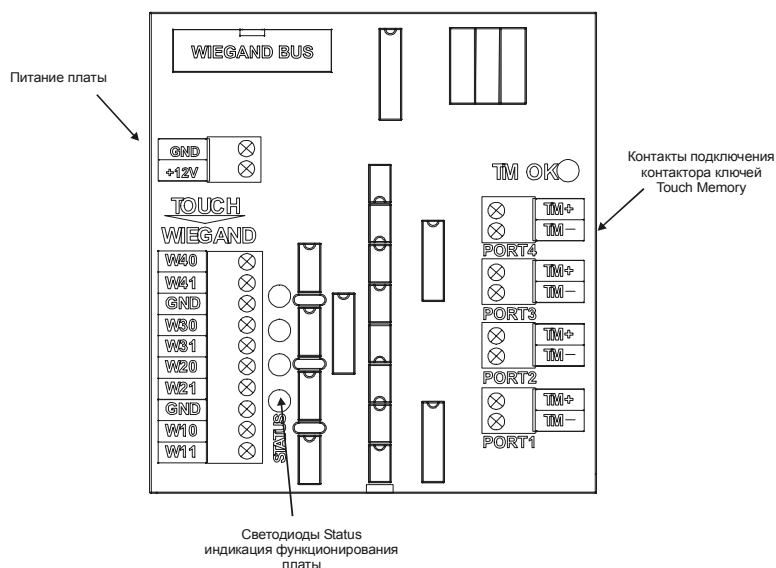


Рис плата WT панели FS-4WT.

Контакторы ключей TM подключаются к клеммам «TM - », «TM + ». Информация о состоянии платы отображается светодиодами Status. Если микропроцессоры модуля работают, светодиоды мигают. При касание идентификатора (Touch Memory) читается код, который транслируется в стандарт Wiegand 26 и передаются контролеру.

3.1.5 Установка DIP переключателей контролера.

Для функционирования системы ForSec каждому контроллеру доступа (панели) присваивается свой **физический адрес**. В сети контроллеров доступа не может быть двух с одинаковым адресом. Порядок подключения контроллеров доступа к физической линии никак не связан с адресом в системе.

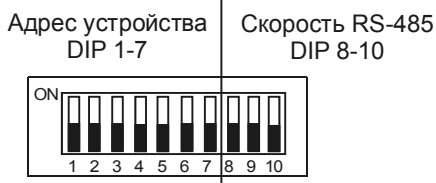


Рис. Переключатель адреса контроллера и скорости сети RS485.

Физический адрес контроллера в системе ForSec задается в двоичном коде в соответствии с таблицей.

Таблица переключателя адреса панели.

1	2	3	4	5	6	7	Адрес
ON	ON	ON	ON	ON	ON	ON	Недопустимо
OFF	ON	ON	ON	ON	ON	ON	1
ON	OFF	ON	ON	ON	ON	ON	2
OFF	OFF	ON	ON	ON	ON	ON	3
ON	ON	OFF	ON	ON	ON	ON	4
OFF	ON	OFF	ON	ON	ON	ON	5
ON	OFF	OFF	ON	ON	ON	ON	6
OFF	OFF	OFF	OFF	ON	ON	ON	7
ON	ON	ON	OFF	ON	ON	ON	8
OFF	ON	ON	OFF	ON	ON	ON	9
ON	OFF	ON	OFF	ON	ON	ON	10
OFF	OFF	ON	OFF	ON	ON	ON	11
ON	ON	OFF	OFF	ON	ON	ON	12
OFF	ON	OFF	OFF	ON	ON	ON	13
ON	OFF	OFF	OFF	ON	ON	ON	14
OFF	OFF	OFF	OFF	ON	ON	ON	15
-	-	-	-	-	-	-	-
ON	OFF	OFF	OFF	OFF	OFF	OFF	126
OFF	OFF	OFF	OFF	OFF	OFF	OFF	127

Скорость интерфейса RS-485 зависит от длины линии интерфейса и помех в линии. Рекомендуемая скорость 115200 бод и меньше. Скорость интерфейса на всех устройствах

системы должна быть одинаковой. Т.е. скорость на контроллере соответствует скорости установленной на сетевом контроллере, репитере и других панелей.

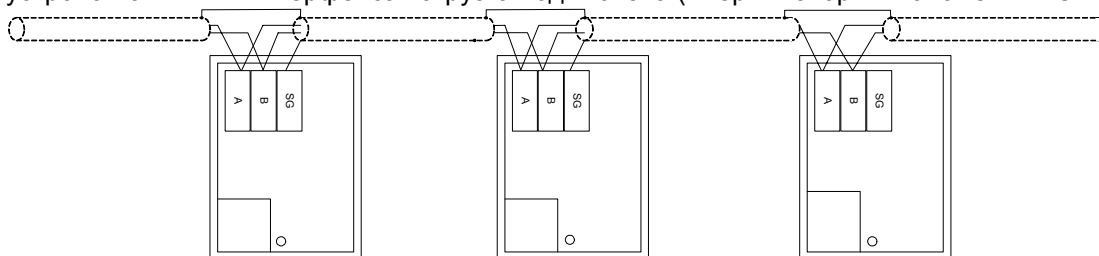
Таблица переключателя скорости интерфейса RS485.

Скорость	8	9	10
172800	ON	ON	ON
115200	ON	ON	OFF
57600	ON	OFF	ON
38400	ON	OFF	OFF
19200	OFF	ON	ON
9600	OFF	ON	OFF
4800	OFF	OFF	ON
2400	OFF	OFF	OFF

DIP переключатель «Терминатор» служит для подключения нагрузочных элементов линии связи по интерфейсу RS-485. Имеет два положения «ON» нагрузка подключена, «OFF» нагрузка интерфейса отключена. Сегмент сети интерфейса RS-485 представляет собой моноканал без ответвлений. На оконечных устройствах линии интерфейса нагрузка подключена: DIP-переключатель «Терминатор» в положении «ON».

3.1.6 Подключение к сети интерфейса RS485.

Сеть интерфейса RS-485 прокладывается кабелем типа экранированная витая пара. Контакты «A», «B», «SG» одной панели подключаются к соответствующим контактам другой панели и т.д. Сегмент сети интерфейса RS-485 представляет собой моноканал без ответвлений. На оконечных устройствах линии интерфейса нагрузка подключена («Терминатор» в положении «ON»).



3.1.7 Подключение считывателя и датчиков к контроллерам системы.

Считыватели подключаются через группы контактов PORT контроллеров доступа.

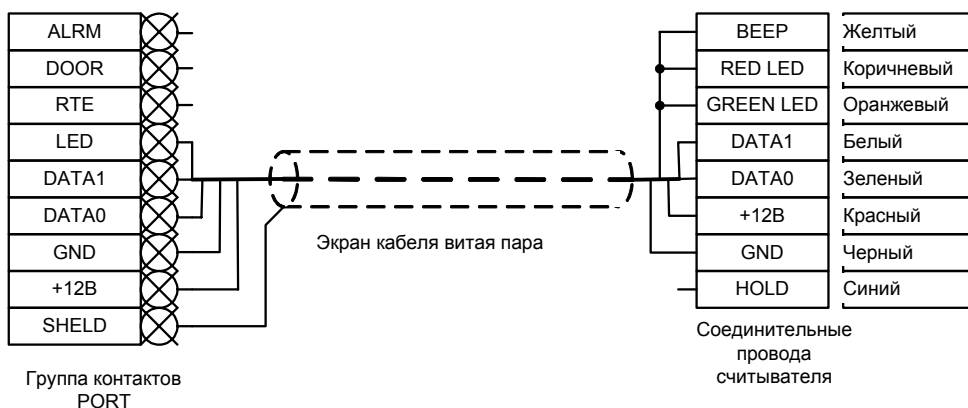


Рис. Схема подключения считывателя.

Назначение контактов группы PORT.

ALRM	вход подключения охранного датчика
DOOR	вход подключения датчика состояния двери
RTE	вход подключения кнопки выхода (нормально разомкнутое положение)
LED	Разъем подключения индикатора считывателя
DATA1	вход данные 1
DATA2	вход данные 2
GND	Разъем общий провод питания считывателя и входов порта
12V	Разъем питания считывателя 12В
SIELD	Разъем подключения экрана кабеля

Считыватели карт имеют собственную схему управления. При подаче напряжения питания на считыватель активен зеленый светодиод. Считывание кода карты индицируется короткой активностью красного светодиода и звукового сигнала. Управление внешними сигналами не блокирует собственную схему управления.

Назначение соединительных проводов считывателя:

Желтый	Звуковой сигнал	Замыкание на общий провод приводит к активности звукового сигнала (зумера)
Коричневый	Красный светодиод	Замыкание на общий провод приводит к активности красного светодиода
Оранжевый	Зеленый светодиод	Замыкание на общий провод приводит к активности зеленого светодиода
Белый	DATA 1	Выход данные 1
Зеленый	DATA 0	Выход данные 0
Красный	+12В	Питание подается постоянно
Черный	Общий провод питания (отрицательный провод)	Не связан с экраном кабеля, не связан с экраном считывателя
Синий	Блокировка считывания	Замыкание на общий провод приводит к разрыву линии передачи данных, считыватель остается активным по отношению к своей схеме управления

Таким образом, для подключения именно считывателя достаточно 5 проводов линии связи и экран кабеля. Рекомендуется при монтаже системы протягивать вывод HOLD (блокировка считывателя). Данный вывод может быть успешно использован для реализации разных алгоритмов СКУД. (Шлюз, блокировка зоны доступа и т.д.).

При указанной схеме алгоритм работы считывателя следующий: в дежурном режиме индикация считывателя зеленая, при разрешении на проход индикация красная и длинный звуковой сигнал, при правильном считывании кода карты, но запрете доступа короткий звуковой сигнал (карта не прописана в аппаратуру, либо доступ запрещен). Программным обеспечением задается режим управления выходом контроллера LED (время импульса, конфигурация).

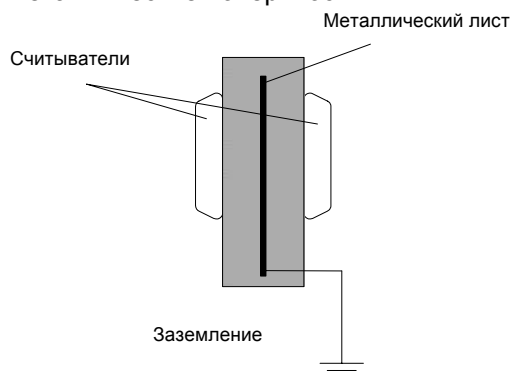
Соответственно можно отказаться, например, от звукового сигнала не используя желтый провод считывателя.

При использовании кабеля типа экранированная витая пара возможная дальность до 150 м от контроллера до считывателя. Рекомендуется использовать кабеля типа FTP5.

Важное замечание: Контроллеры доступа (панели) конструктивно выполнены так, что плата гальванически развязана от корпуса прибора (металлического шкафа). Это позволяет эффективно экранировать контроллер доступа от внешнего электромагнитного излучения. Контакт SHELД связан именно с экраном контроллера и гальванически развязан с контактами GND (общий питания). Экран кабеля подключается к контакту SHELД. Недопустимо экран кабеля использовать для подключения общего провода питания. Со стороны считывателя экран кабеля остается не подключенным, если конструкция считывателя не предусматривает подключение экрана.

Установка считывателей. При разработке структурной схеме следует учитывать правила установки считывателей проксимити карт. Уточняется по техническому описанию считывателей, но стандартным является установка считывателей не ближе 50 см. друг от друга, т.к. считыватели являются излучателями электромагнитного поля. Стандартным является установка считывателей на разных сторонах дверного проема на высоте удобной для применения, обычно немного выше установки ручки двери.

При невозможности удаления считывателей, в строительной конструкции закладывается ЭКРАН, с обязательным заземлением, для исключения взаимного влияния считывателей. При этом дальность считывания карт снижается, то же распространяется при установке считывателей на металлические поверхности.



Контакты ключей Touch Memory (iButton) возможны различных типов по вандальности, методам установки, наличия индикации. Главная задача контактора - просто обеспечить электрический контакт с ключом. Здесь нет требований по установке контакторов. В частности понятно, что параллельно может быть включено несколько контакторов Touch Memory (iButton).

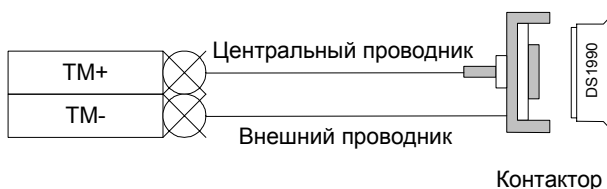


Рис. Подключение контакторов Touch Memory (iButton) к панелям ForSec.

Также по этому стандарту возможно подключение считывателей (к примеру уже установленных на объекте) с эмуляцией формата Touch Memory (iButton). При использовании кабеля типа экранированная витая пара возможна дальность до 100 м от контроллера до считывателя.

Подключение датчиков.

Контроллер доступа ForSec отслеживает состояние контактов ALRM, DOOR, RTE. Состояние контактов оценивается относительно клеммы GND группы контактов PORT.

Каждый считыватель может работать с любым входом, кроме RTE.

Кнопка выхода (RTE) имеет жесткую связь с соответствующим считывателем и не может быть шунтирована. Кнопка RTE всегда нормально разомкнута. Действие кнопки выхода аналогично действию соответствующего считывателя: включается выход и шунтируются входы.

Считыватель может шунтировать любой из 8 оставшихся входов

Входы (кроме RTE) панели защищены от случайных помех и имеют время интегрирования около 300 мс. С помощью программного обеспечения они могут быть определены как нормально замкнутые или нормально разомкнутые. Вход может быть подключен к любому выходу. Входы могут шунтироваться на определенное время. Время шунтирования задается ПО.

Входы могут быть удалены от панели на значительные расстояния – сотни метров. При значительном удалении рекомендуется использовать экранированную витую пару.

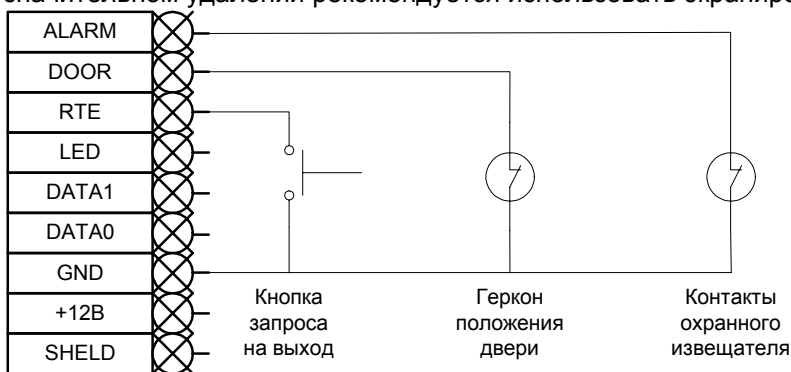


Рис. Подключение датчиков к панелям (контроллерам доступа) системы ForSec.

3.1.8 Типовые структурные схемы подключения исполнительных устройств.

Каждый контроллер доступа имеет достаточное количество реле управления исполнительными устройствами. Каждое реле имеет полную группу контактов NO/NC с токовой нагрузкой:

Постоянное напряжение – 30В 7А;

Переменное напряжение – 250В 7А.

Режим функционирования задается ПО. Любое реле панели может быть: выключено/включено/импульс (от 0,5 сек.)/инверсия. Любое реле может быть связано с любым считывателем, с любым входом. Режим «включено» соответствует подачи напряжения на реле. Каждое реле имеет светодиод функционирования. Режим «импульс» соответствует включению реле на время длительности импульса.

Перечисленные параметрами позволяют подключать практически любые исполнительные устройства к контроллерам доступа системы ForSec.

В качестве исполнительных устройств ограничения доступа в настоящее время используются электромеханические замки, электромеханические защелки, электромагнитные замки, турникеты различных конструкций, шлюзовые кабины.

Электромеханические защелки и замки в нормальном запертом положении двери не потребляют электрический ток и обеспечивают блокировку двери за счет механических частей запирающего устройства. Потребление тока возникает с случае открытия замка. Т.е. командой для этого вида исполнительных устройств является подача напряжения.

Электромагнитные замки обеспечивают запираение двери за счет магнитного эффекта между электромагнитом замка и ответной частью. Соответственно к открытию двери приводит снятие напряжение с обмотки электромагнита. В плане надежности электромагнитные замки не имеют механически изнашивающихся частей запорного механизма. При использовании на объекте данного типа замков следует продумывать тип электромагнитного замка с платой управления и без. От типа замка зависит что будет являться сигналом на открытие замка либо снятие напряжения с замка, либо импульс напряжения на плату управления замка.

Турникеты в большинстве случаев блокируются электромеханическим запором. Открытие запора происходит при подаче напряжения на исполнительное устройство, хотя большинство турникетов имеют собственные платы управления и сигналом на разблокировку на ВХОД/ВЫХОД могут являться любые сигналы (сухое замыкание, импульс напряжения) на два разных входа.

Важное замечание: При разработке схемы системы следует четко выполнять требование по гальванической развязке контроллеров доступа и исполнительных устройств. Не используйте для питания замков выход 12В панели. Требуется дополнительный источник питания.

Не соединяйте общие провода питания контроллеров и исполнительных устройств, во избежание попадания на плату панели электромагнитных наводок и импульсов помех.

При непосредственном управлении индуктивных нагрузок (обмотки электромеханических замков, электромагнитных замков без плат управления) необходимо шунтирование обмоток защитными диодами. В противном случае из-за индуктивных токов, имеющих достаточно высокое значение, возможно обгорание или спайка контактов реле контроллера доступа (панели).

При работе с исполнительными устройствами питаемыми от переменного тока, диод заменяется на варистор.

Структурная схема подключения электромеханических замков, защелок.

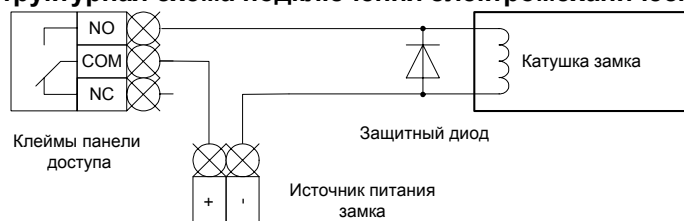


Рис. Управление электромеханическими замками, защелками.

Открытие подачей напряжения.

Реле в режиме импульс (достаточно 0,5 сек.). Для взведения замка в рабочее состояние требуется отработка цикла двери ОТКРЫТЬ/ЗАКРЫТЬ.

Структурная схема подключения электромагнитных замков.

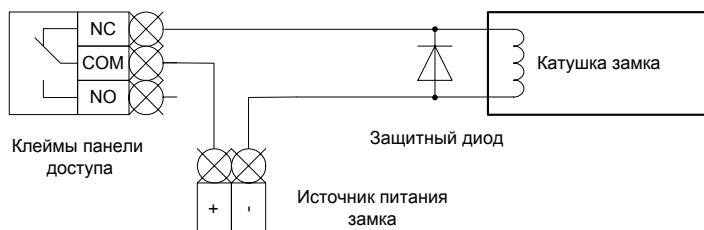


Рис. Управление электромеханическими защелками, электромагнитными замками.

Открытие по снятию напряжения.

Реле в режиме импульс (достаточно от 3сек. и выше). Для взведения замка в рабочее состояние требуется отработка цикла двери.

Структурная схема подключения электромагнитных замков с платой управления.

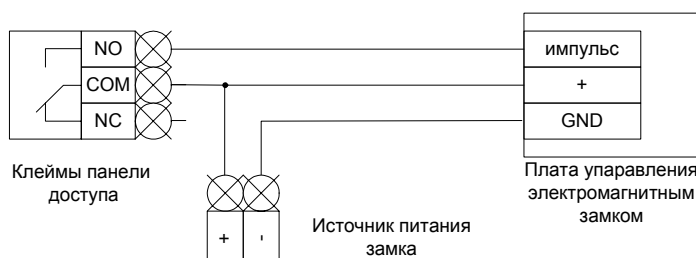


Рис. Управление электромагнитным замком с платой управления.

Открытие по управляющему импульсу напряжения.

Реле в режиме импульс (достаточно 0,5 сек.). Время открытия двери устанавливается на плате управления замка.

Работа системы ForSec с турникетами.

Особенностью работы с турникетом является необходимость управления двумя направлениями прохода и необходимость в ряде случаев получать сигнал о провороте турникета, т.о. турникет может быть расценен как два исполнительных устройства. Заметим, что в большинстве случаев достаточно одного сигнала проворота штанг, вне зависимости от направления прохода. Сигнал

поворота формируется не всеми моделями турникетов и при необходимости может быть получен от охранного извещателя, зоной обнаружения перекрывающего зону прохода. Конкретная схема зависит от модели турникета. Приведена структурная схема управления турникетом по трем сигналам (замыканием входных цепей платы управления турникета на землю) и наличием сухих контактов поворота турникета.

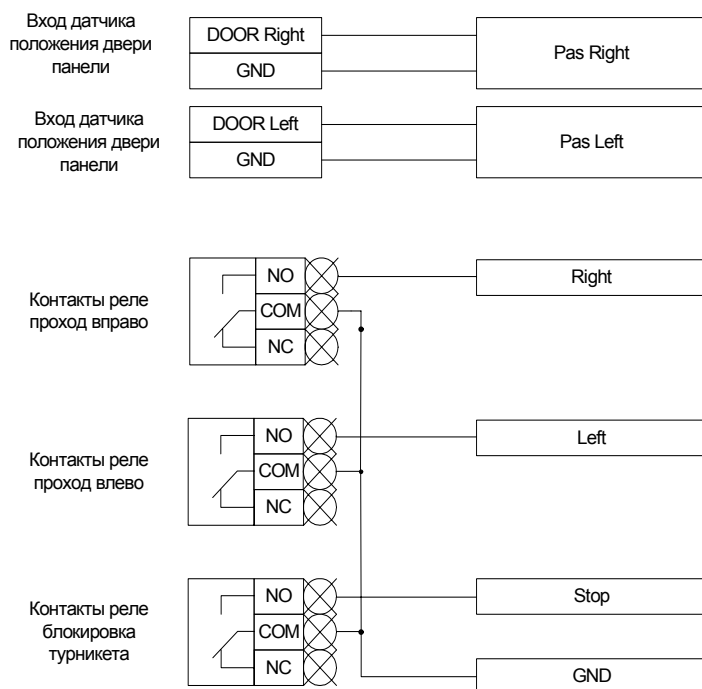


Рис. Схема подключения турникета к панели системы ForSec.

Данная схема позволяет производить безусловную блокировку турникета, используя любое свободное реле. Т.е. в отличие от двух исполнительных устройств, турникет может занимать три реле.

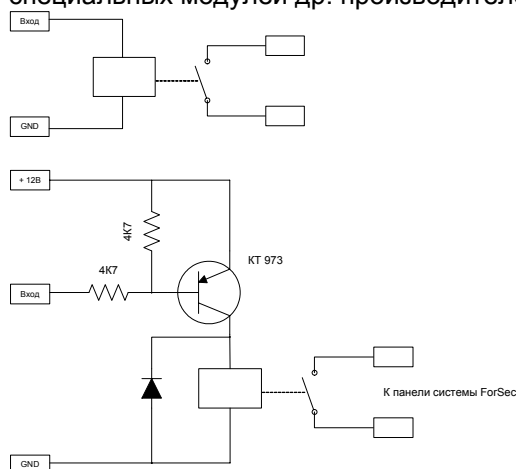
Реле в импульсном режиме на время от 3 сек и выше (время достаточное для совершения прохода). Для корректной работы СКУД, используется функции «подтверждение прохода», устанавливается при конфигурировании системы через ПО ForSec. Сброс реле (выключение) осуществляется по сигналу от датчика поворота турникета, что также задается через ПО ForSec.

Оптические турникеты

Отдельный класс исполнительных устройств – оптические турникеты. Идея турникета при несанкционированном проходе через зону охраны выдается сигнал тревоги (звук, свет или приведение в действие устройства типа преграды и т.д.). При санкционированном проходе система охраны шунтируется на время прохода. Для получения сигнала о проходе может быть использован охранный извещатель любого принципа (напоминаем, что большинство извещателей имеет инерционность по выходным сигналам). По сигналу считывателя шунтируется охранный извещатель перекрывающий проход. В случае несанкционированного прохода выдается сигнал на реле, управляющее сиреной, лампой и т.д.

Важная информация: Недопускается гальваническая связь между турникетом и контроллером доступа. При необходимости устанавливайте устройства гальванической развязки по цепям датчика проворота турникета.

Для гальванической развязки исполнительных устройств и панелей системы ForSec рекомендуем применять слаботочные реле (характеристика срабатывания от вида и характеристик сигнала устройств), вариант использования 12В реле приведен ниже, также возможно применение специальных модулей др. производителей.



3.1.9 Правила заземления контроллеров.

Как уже отмечалось, система ForSec устанавливается на объектах любой степени сложности, в том числе, и в условиях сложной электромагнитной обстановки.

Для отсутствия влияния внешних наводок и импульсов по цепям питания контроллеры выпускаются в виде законченных устройств с бесперебойным источником питания с отсеком для установки аккумулятора 12В 7А/ч. Корпус контроллера доступа (панели) не имеет гальванической связи с цепями питания панели.

Чтобы защитные цепи работали эффективно необходимо заземлить корпус панели. В нижней части панели имеется специальная точка заземления. Не допускается занулять панель (использовать нулевой провод цепи питания), использовать земли с большим сопротивлением, контуры заземления промышленного оборудования. Каждая панель должна иметь радиальное подключение к земле. В связи с отсутствием гальванической связи между панелями, общая шина заземления не является обязательной с условием заземления корпусов каждой панели.

Обратите внимание, что экран сети интерфейса RS 485 подключается к колодке на каждой панели, но заземляется на шину только в одной точке системы. На реальных объектах возможна разность потенциалов между панелями в разных точках объекта.

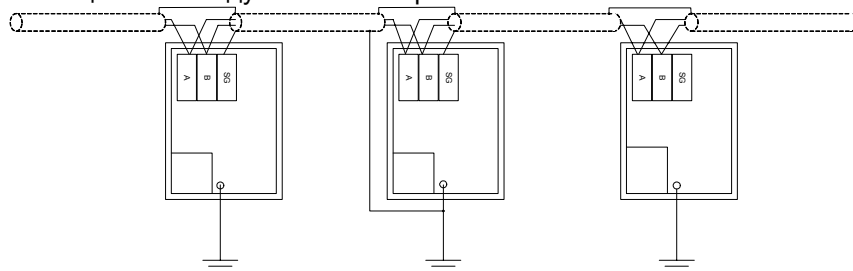


Рис. Радиальное заземление каждой панели.

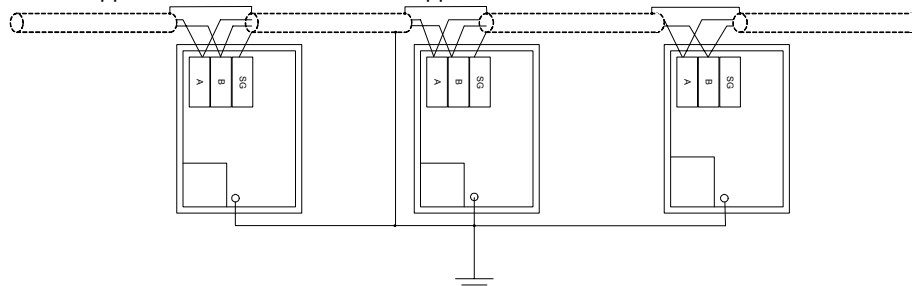


Рис. Заземление панелей на общую шину.

Прокладка отдельной шины заземления для сети контроллеров системы ForSec является предпочтительным вариантом. В этом случае система ForSec максимально устойчива к действию электромагнитных импульсов.

Для обеспечения устойчивой работы системы рекомендуется выполнять следующие требования:

1. Выполнять монтаж провод силовых цепей (замки, защелки, сеть 220) в отдельных экранированных профилях (трубах). Запрещается располагать слаботочные цепи (счетчиков, проводов входов, RS485) ближе чем 50 см от силовых линий.
2. Для уменьшения электромагнитных излучений рекомендуется использовать экранированные кабели или экранированные профили (трубы).
3. Запрещается располагать внутри корпуса панели устройства, не предусмотренные конструкцией.
4. Не рекомендуется питать исполнительные устройства (замки, защелки, сирены) от внутреннего источника панели. Необходимо использовать внешние источники питания.
5. Запрещается монтировать панели вблизи источников электрических помех (электрические двигатели большой мощности, мощные трансформаторы, инверторы и т.д.).

3.1.10 Рекомендации по использованию проводов.

Применение	Сечение минимальное мм.	Описание	Максимальная дальность
Считыватель интерфейс Wiegand	0,22	Экранированная витая пара Level 5 маркировка FTP-5cat	150 м
Контакты Touch Memory	0,22	Витая пара маркировка UTP...	100 м
Входы	0,22	Витая пара маркировка UTP...	500 м
Выход реле	0,5	Желателен экран	500 м
Интерфейс RS485	0.22	Экранированная витая пара Level 5 маркировка FTP-5cat	1200 м

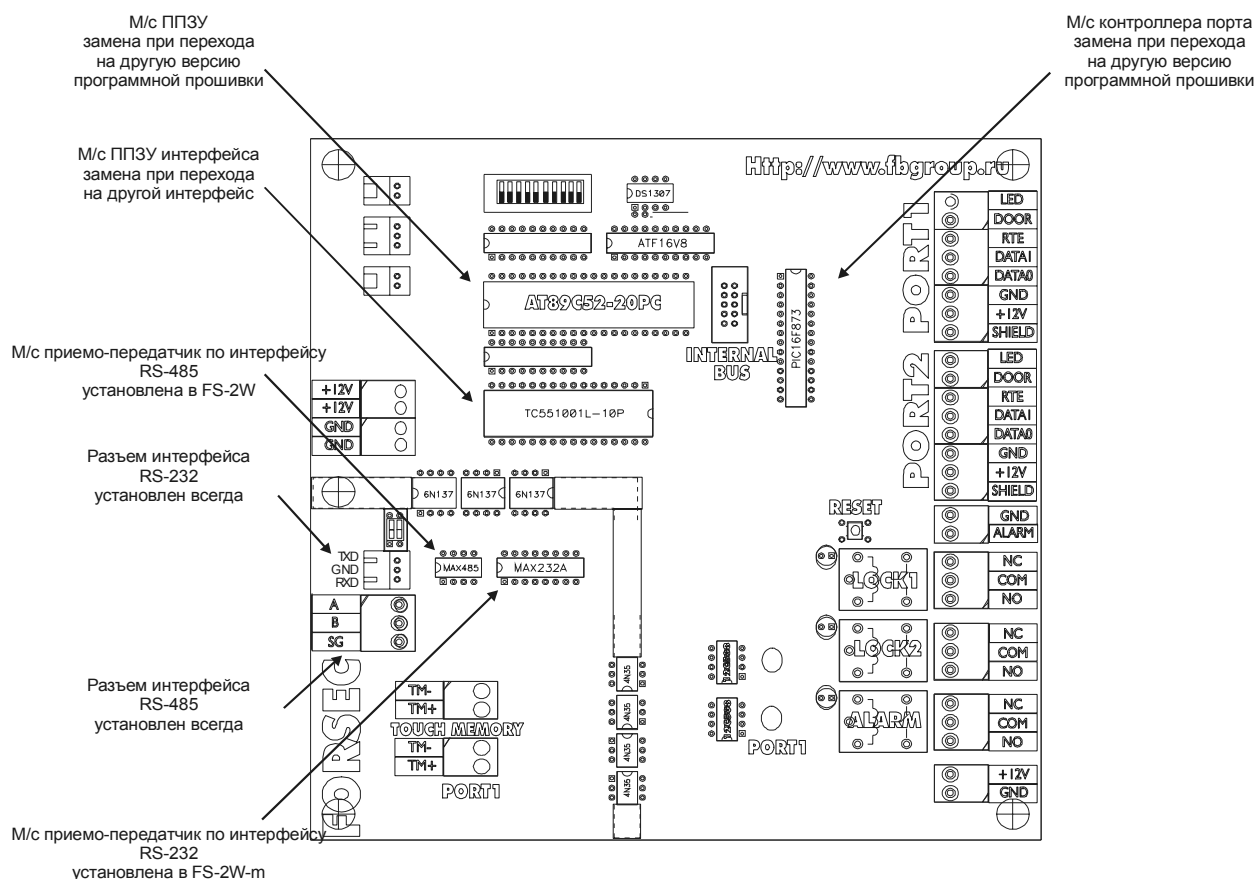
3.1.11 Зависание контроллеров.

Панель имеет защиту от зависания процессоров. Однако всегда существуют исключительные ситуации. Для сброса панели предусмотрена кнопка RESET в нижнем левом углу платы. Если по каким-либо причинам работоспособность панели не восстановилась, рекомендуется полное отключение питания. Нужно снять со штырей терминальный блок питания (+5V, +5V, GND, GND, GND, +12V, +12V). Подождать около 10 секунд и установить терминальный блок в прежнюю позицию. При установке блока на место остерегайтесь сдвигов контактов.

3.1.12 Модернизация контроллеров доступа (панелей).

В связи с постоянной модернизацией аппаратуры, входящей в систему ForSec а так же, возможными переходами на более совершенное ПО иногда встает вопрос о замене программной прошивки аппаратуры при расширении систем на ранее оборудованных объектах. Также возможна ситуация перехода с интерфейса RS-232 на интерфейс RS-485 (или наоборот).

В указанных случаях по требованию заказчика может быть поставлен комплект микросхем для замены непосредственно на объекте заказчика. Все микросхемы подлежащие модернизации установлены на разъемах и их замена не представляет труда.



Вторую часть инструкции по монтажу системы контроля доступа ForSec можно скачать на сайте компании Формула Безопасности: <http://www.fbgroup.ru/>