Интегрированная система безопасности

«ФОРТЕЦЯ»

ОБЩЕЕ ОПИСАНИЕ

Содержание

1. Назначение

Интегрированная система безопасности «Фортеця» предназначена для решения задач по обеспечению комплексной безопасности объекта, в частности: ограничению доступа, организации охраны объекта, управления различными техническими и вспомогательными системами.

2. Структура построения системы

Структуру построения интегрированной системы условно можно разбить на три уровня:

- аппаратный уровень;
- транспортный уровень;
- программный уровень.

Графическое изображение уровней системы представлено на рисунке 1.

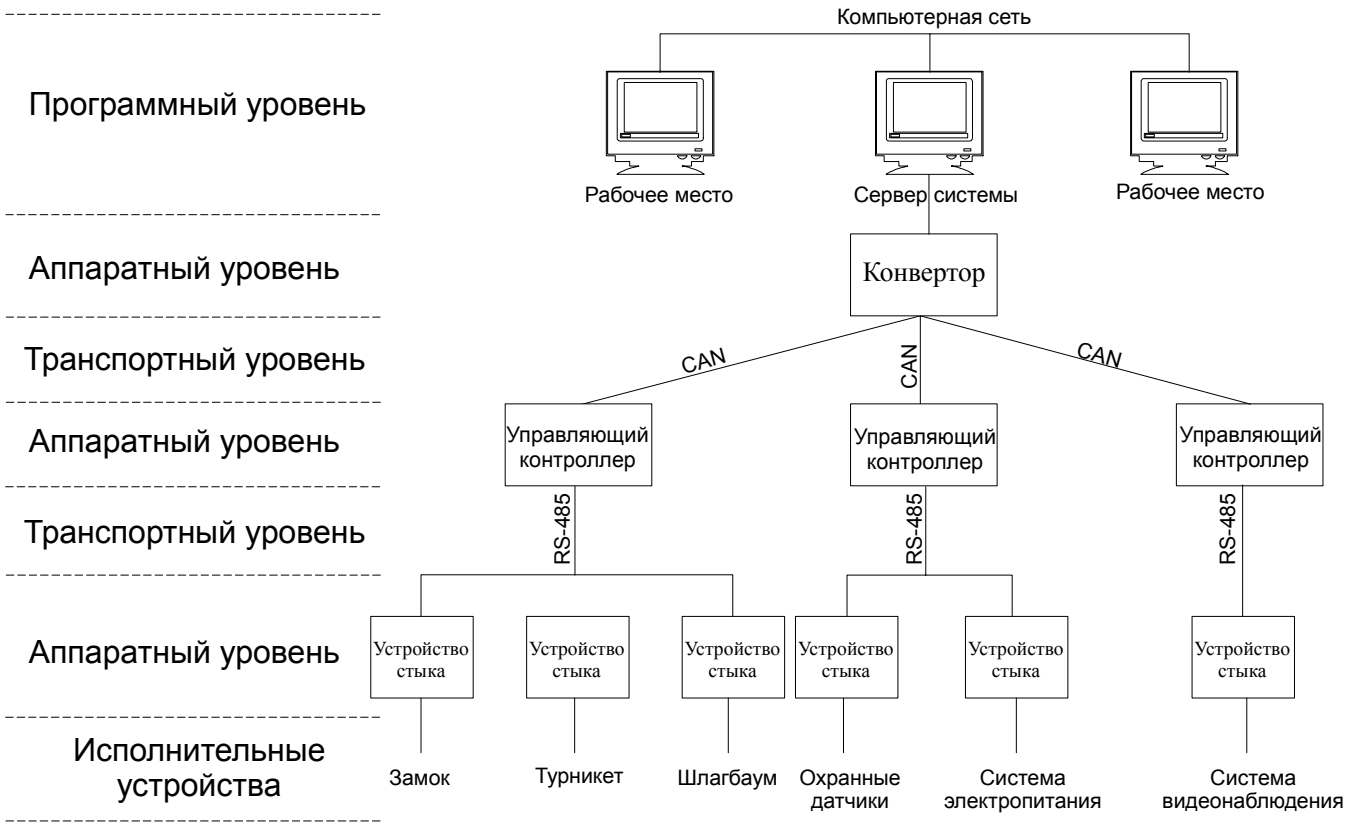


рисунок 1.

- Исполнительными устройствами для системы могут служить самые разнообразные устройства. Например, электрозамок, шлагбаум, турникет, коммутатор видеокамер, система видеозаписи, система электроснабжения и т.д.

- Устройства обеспечения стыка с исполняющими устройствами представляют собой семейство различных устройств сориентированных строго для работы с конкретным исполнительным механизмом. Пример: модуль, управляющий работой электрозамка, не позволяет работать со шлагбаумом. Детальное назначение каждого семейства модулей будет изложено далее.

- Управляющий контроллер производит синхронизацию работы и управление всеми локальными устройствами, подключенными к своей локальной шине.

- Конвертор связи обеспечивает решение задач по организации обмена данными между сервером системы и управляющими контроллерами.

- Сервер системы обеспечивает решение задач ввода, вывода различных данных в систему, наглядного графического интерфейса управления системой и обеспечивает организацию рабочих мест операторов и возможность управления системой через локальную сеть компьютера.

2.1 Аппаратный уровень

Аппаратный уровень представляет собой совокупность всех аппаратных устройств системы, выполняющих задачи: по управлению различными исполнительными устройствами и механизмами; устройств обеспечения стыка с данными устройствами; а так же совокупность управляющих центров (узлов), обеспечивающих синхронизацию и обобщенное управление всеми этими устройствами.

2.1.1. Децентрализация управления

Аппаратный уровень системы можно разбить на отдельные ячейки или соты. Условное графическое изображение уровня представлено на рисунке 2.

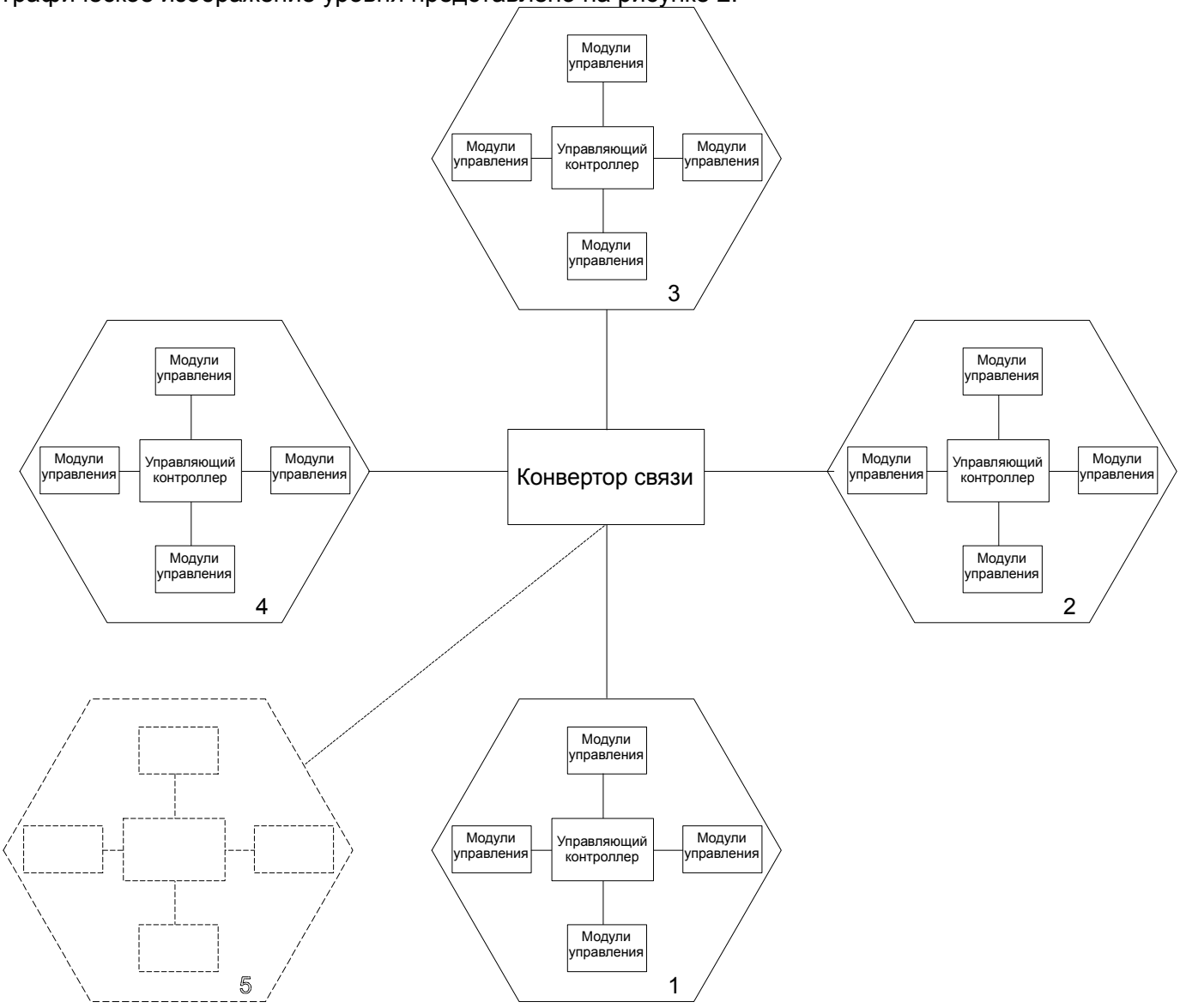


рисунок 2.

Каждая ячейка работает под управлением своего контроллера – управляющего узла. Данный принцип построения можно назвать частичной децентрализацией управления. Для децентрализованной системы присущи следующие отличительные черты:

- *Живучесть системы.* Система, построенная по принципу децентрализованного управления, обладает лучшими показателями по живучести. Так как отдельные соты не связаны между собой, то выход их из строя или нарушение работоспособности не приводит к нарушению работы остальных частей системы.

Рассмотрим рисунок 2. На рисунке изображен один из вариантов построения интегрированной системы на большом объекте. Допустим, что каждой отдельной соте соответствует свой этаж в здании. Предположим, что произошла нештатная ситуация, вызвавшая полное или частичное нарушение работоспособности системы на втором этаже. В результате вышла из строя часть системы относящейся ко второй ячейки системы. Однако остальные части (соты) системы продолжают функционировать в нормальном режиме.

- *Наращиваемость системы.* Система позволяет гибко наращивать дополнительные соты системы, не вызывая при этом нарушение работоспособности других локальных ячеек.

Рассмотрим рисунок 2. Каждому локальному сегменту соответствует отдельное здание. Первоначально интегрированной системой на объекте были оснащены только четыре здания. В дальнейшем возникла потребность в дополнительном оснащении пятого здания. Каждое из зданий представляет собой локальный фрагмент сети, поэтому дополнительный ввод в систему здания не потребует остановки работы четырех первых сегментов системы безопасности и не вызовет нарушения в их работе.

- *Предел ресурса одного сегмента*. Фактор, отражающий вероятность нехватки какого-либо ресурса системы в пределах одного сегмента. Пример: необходимо объединить в одну группу охраны 200 охранных зон одновременно. Так как данное требование не соответствует техническим возможностям системы, то в данном случае оно не выполнимо. Смотри пункт 6.«Элементы охраны » настоящего руководства.

Однако вероятность появления данных требований достаточно мала и на практике, как правило, исключена.

Для преодоления данного ограничения ресурс одного сегмента сети должен удовлетворять практические потребности в 90 % случаях.

2.2 Транспортный уровень

Транспортный уровень представляет собой совокупность каналов сбора информации от управляющих контролеров и локальных устройств, подключенных к нему. Физический уровень между управляющими контролерами – канал CAN. Физический уровень между управляющими контролерами и локальными устройствами – канал RS485. Подробное описание реализации каналов связи указано в разделе 8 «Каналы связи» настоящего руководства.

2.3 Программный уровень

Программный уровень представляет собой: управляющий компьютер с установленным программным обеспечением «Фортеця», обеспечивающий ввод\вывод необходимых данных в систему; соединения между компьютерами, объединенными в единую сеть; и сами компьютеры выполняющие роль удаленных рабочих мест.

Принципы построения компьютерных сетей и организация взаимодействия компьютеров между собой не входят в данное руководство и далее не рассматриваются.

Краткое описание программного уровня указано в разделе «Программное обеспечение» данного руководства.

3. Состав системы

Интегрированная система «Фортеця» включает в себя следующие основные части:

- Верхнее программное обеспечение:
  - «Фортеця».
- Конверторы связи:
  - CCG-4;
  - CCG.
- Управляющие контролеры:
  - VNC;
  - ANC.
- Модули удаленного управления точкой прохода:
  - RCP10;
  - RCP20;
  - RCP20м;
  - RCP30.
- Модуль подключения клавиатуры:
  - RKB10.
- Модуль охранных шлейфов:
  - RAM-8.
- Модуль релейных выходов:
  - RM-8.

Примечание. *В состав системы могут входить дополнительные модули, выходящие за рамки данного списка.*

Функциональное назначение отдельных частей системы указано в разделе 7 настоящего руководства, а также в соответствующих технических описаниях.

4. Возможности системы

4.1. Общие возможности системы

Интегрированная система в полном объеме позволяет подключить до 2176 считывателей, до 8567 шлейфов охраны, до 8384 исполнительных выходов. Пример расчета указан в таблице 1.

Табл.1

Наименование	На базе VNC	Локальных сегментов	Итого	На базе ANC	Локальных сегментов	Итого	Общий итог
Считывателей	32	x 64	2048	2	x 64	128 *	2 176
Охранных зон	128	x 64	8192	6	x 64	384 *	8 567
Исполнительных выходов	128	x 64	8192	3	x 64	192 *	8 384

*** Примечание.** Для контроллера ANC расчет взят из условия обслуживания одной двусторонней точки прохода. Остальные ресурсы контроллера могут использоваться в зависимости от задачи. (См. п. 7.2.2.Функциональное назначение контроллера ANC).

5. Элементы разграничения доступа

5.1. Общее описание

Элементами разграничения доступа называется совокупность технических и организационных мероприятий, позволяющих разграничить доступ на определенные территории, как физических лиц, так и технических средств. Одним из элементов системы разграничения доступа является точка прохода.

Точкой прохода является место, оснащенное элементами идентификации физического лица (технического средства) и оборудованное механизмом ограничения свободного прохода через него.

Элементами идентификации являются любые технические средства, обеспечивающие достаточно достоверное распознавание физических лиц по определенным идентификационным критериям. В качестве идентификационных критериев могут применяться самые разнообразные методы, например, биометрические или с помощью дополнительных технических средств - идентификаторов.

Биометрические системы производят распознание по каким-либо физическим параметрам человека, например, отпечаткам пальцев, руки, визуально по изображению, по голосу и т.д. Биометрические системы не требуют дополнительных внешних носителей информации. Процесс идентификации личности биометрическими системами может быть достаточно продолжительным по времени и занимать до нескольких минут.

Внешний идентификатор представляет собой носитель информации, который содержит некую уникальную информацию, подтверждающую персону человека. Это может быть карта с магнитной полосой, со штрих кодом, бесконтактная радиочастотная карта, чип-карта и т.д. Устройство считывания производит съем информации с носителя и сверяет с информацией, хранящейся в своей памяти.

Внешний идентификатор позволяет достаточно быстро, как правило, не больше нескольких секунд, подтверждать персону человека. Основным его недостатком является необходимость иметь его при себе.

Под механизмом ограничения свободного прохода предполагается любое техническое средство, исключающее или затрудняющее свободный проход без разрешения. Например, дверь с электрозамком, турникет, калитка, тамбур-шлюз и т.д. В частном случае точка прохода может не иметь механических препятствий, а быть оборудована только системами контроля прохода, например, оптическим лучом. Разрешение на проход выдается системой контроля доступа после идентификации человека и подтверждения его права доступа на данную территорию.

5.2. Организация точки прохода в системе « Фортеця»

Организация точки прохода в интегрированной системе “Фортеця” производится на базе семейства модулей RCP. Функциональное описание каждого модуля указано в разделе 7 настоящего руководства.

Модуль RCP обеспечивает решение следующих задач:

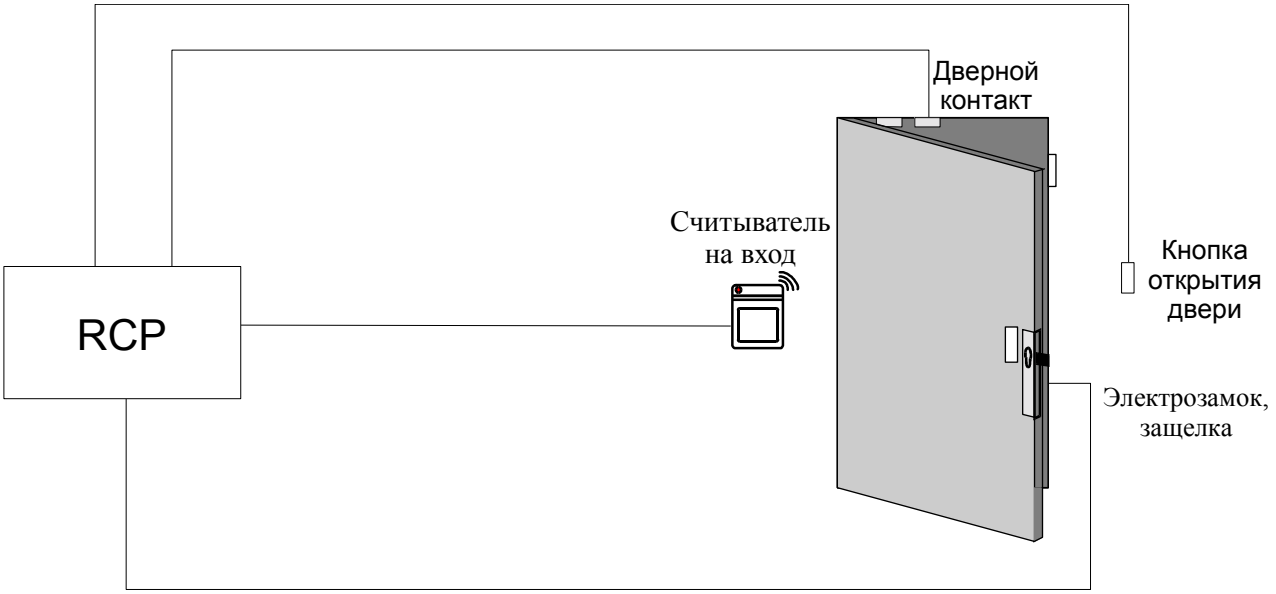
- прием данных с устройств идентификации (считыватели);
- управление исполнительным устройством (замок, защелка и т.д.);
- контроль состояния механизма для ограничения прохода (дверь, турникет, шлюз, и т.д.)
- выдача сигналов индикации о разблокировке или отказа в допуске;
- контроль факта прохода через «препятствие».

Организация точки прохода может осуществляться двумя вариантами:

1) Односторонний вариант;
2) Двусторонний вариант.

5.2.1. Организация односторонней точки прохода

Вариант организации односторонней точки прохода изображен на следующем рисунке. В целях упрощения на функциональной схеме не отражены элементы питания электрозамка и модуля RCP.



На данном рисунке отображены следующие элементы:

- Устройство идентификации – проксимити-считыватель;
- Механизм ограничения свободного прохода - дверь;
- Исполнительное устройство – электрозамок;
- Устройство разблокировки исполнительного устройства - кнопка;
- Датчик состояния двери – дверной контакт;
- Модуль управления точкой прохода – контроллер RCP.

Рассмотрим вариант прохождения через точку прохода.

В качестве варианта взята точка прохода на базе одностворчатой двери, оборудованной механизмом запора – электромеханическим замком.

!!! В качестве устройства идентификации здесь и далее будут рассматриваться бесконтактные проксимити-считыватели.

Нормальное состояние для точки прохода: механизм удержания двери заблокирован, дверь закрыта. Физическое лицо, оснащенное бесконтактным идентификатором – проксимити-картой, находится вне помещения. Задача: необходимо попасть внутрь помещения.

Для решения данной задачи необходимо кратковременно поднести проксимити-карту к устройству идентификации - считывателю. Считыватель произведет «съем» кода с проксимити-карты и транспортирует данный код в устройство обработки – модуль RCP. Модуль произведет анализ полученного кода и, если данное физическое лицо обладает правом доступа на данную территорию, выдаст команду разблокировки на механизм удержания двери – электромеханический замок. Считыватель произведет индикацию разрешения доступа в данное помещение. Если права доступа нет, то производится индикация об отказе в доступе.

Если факт прохода состоялся (была открыта дверь), то датчик состояния двери сформирует сигнал, который поступит в модуль RCP. Система « считает», что человек прошел.

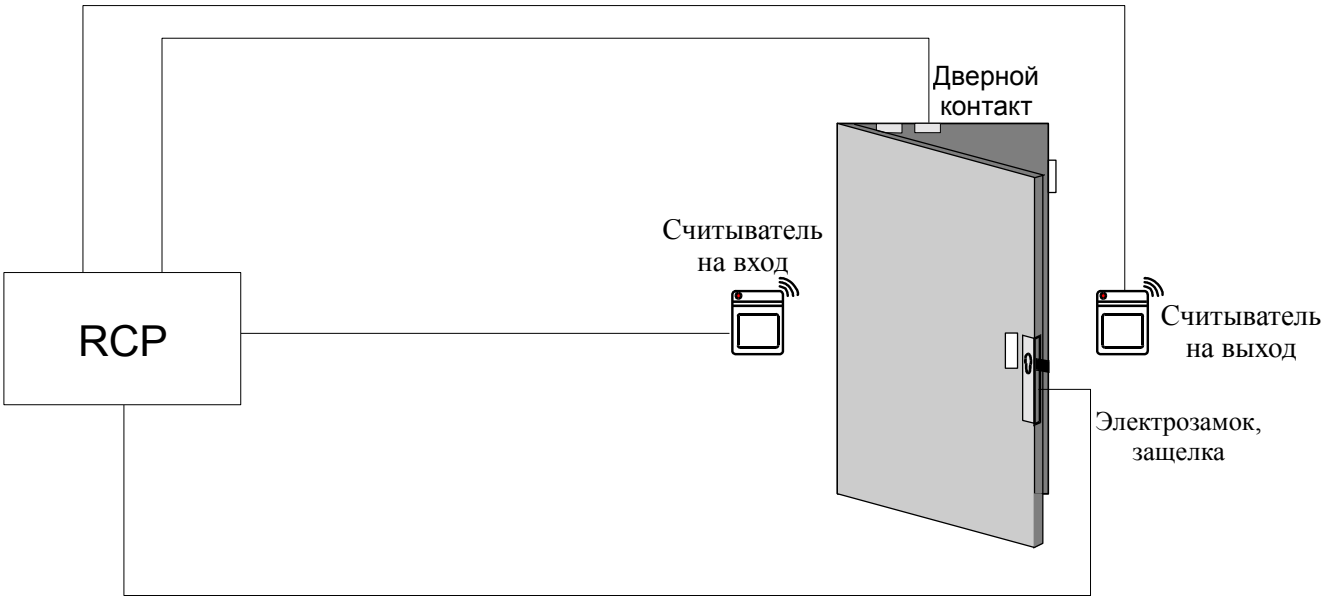
Для выхода из помещения достаточно кратковременно нажать на кнопку открытия двери. Модуль RCP произведет при этом разблокировку замка.

При данном методе построения контролируется только вход в помещение. Выход из помещения производится без контроля. Для разблокировки механизма удержания двери используется кнопка. Недостатком данного метода является:

- отсутствие возможности проконтролировать нахождение физических лиц в помещении;
- производить учет рабочего времени по временным критериям.

5.2.2. Организация двусторонней точки прохода

Вариант организации двусторонней точки прохода изображен на следующем рисунке. В целях упрощения на функциональной схеме не отражены элементы питания электрозамка и модуля RCP.



На данном рисунке отображены следующие элементы:

- Устройство идентификации – проксимити-считыватели;
- Механизм ограничения свободного прохода - дверь;
- Исполнительное устройство – электрозамок;
- Датчик состояния двери – дверной контакт;
- Модуль управления точкой прохода – контроллер RCP.

Процесс взаимодействия элементов разграничения доступа аналогичен тому, что описан в пункте 5.2.1. Для точки прохода оборудованной элементами считывания с двух сторон, выход из помещения производится аналогично входу.

При данном методе построения точки прохода контролируется вход и выход в помещение. Данная схема построения позволяет полноценно решать задачи:

- поиска сотрудников на территории предприятия;
- контроля персонала в помещении;
- учета рабочего времени.

Данная схема не исключает возможности подключения кнопки открытия двери.

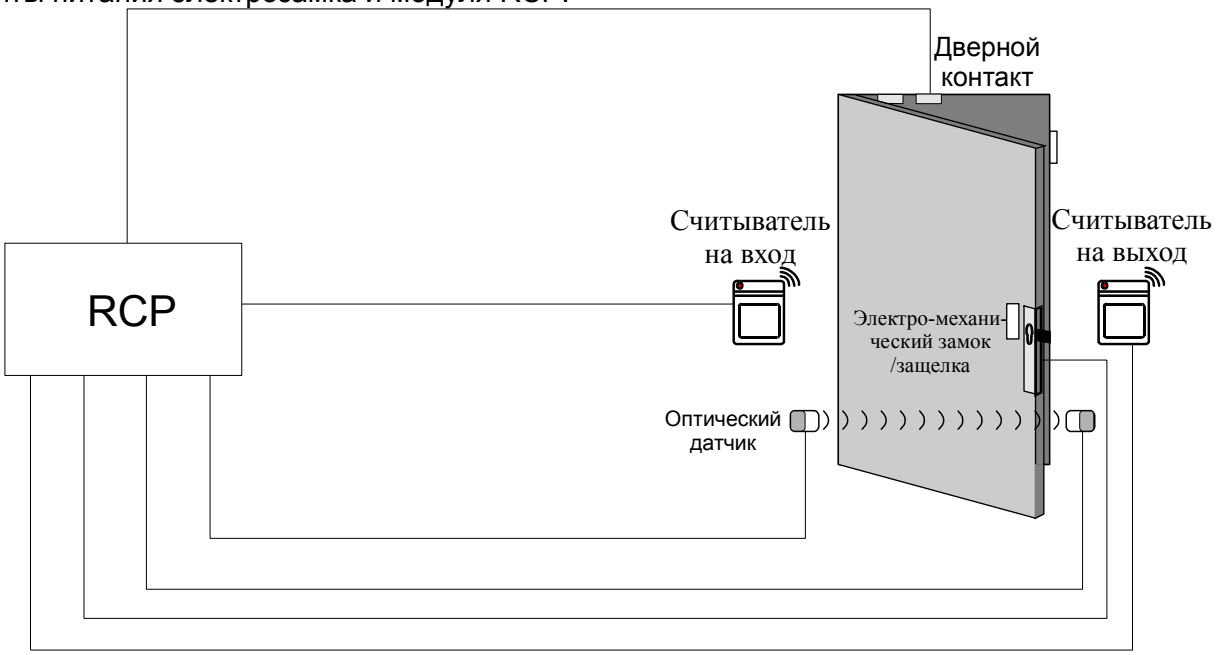
5.2.3. Повышение достоверности факта прохода

В процессе пересечения точки прохода (см. пункт 5.2.1) зачастую возникают нештатные ситуации, вызванные «человеческим фактором». Наиболее распространенной проблемой является ситуация, когда пользователь приложил идентификатор к считывателю, получил разрешение на

проход, приоткрыл дверь, но по каким-то причинам передумал и не пошел далее. Система считает, что был факт пересечения точки прохода, так как датчик открытия двери выдал соответствующий сигнал. Если на данную точку прохода дополнительно распространяется функция «контроль повторного прохода» (см. пункт 5.7), то данный пользователь не сможет произвести повторное открытие двери. Данная ситуация может повлечь за собой некорректный учет рабочего времени пользователей.

!!! Интегрированная система «Фортеця» позволяет организовать построение односторонних и двусторонних точек прохода с повышенной достоверностью факта пересечения. Для повышения достоверности могут применяться оптические датчики типа ИК-барьер.

Вариант организации двусторонней точки прохода с дополнительным оптическим датчиком изображен на следующем рисунке. В целях упрощения на функциональной схеме не отражены элементы питания электрозамка и модуля RCP.



Дополнительный оптический датчик позволяет устранить проблемы, вызванные «человеческим фактором». С момента, когда система получила сигнал от датчика открытия двери - дверного контакта производится анализ состояния оптического датчика. Если пересечения оптического луча не было, то система выдаст соответствующую информацию оператору системы. Например: «Доступ разрешен, человек не прошел».

Если пересечение луча произошло, будет сформировано сообщение об успешном пересечении данной точки прохода.

!!! Данная схема организации точки прохода рекомендуется на объектах:

- с повышенными требованиями по высокой достоверности нахождения персонала в данном помещении (территории);
- в системах с точным учетом времени нахождения персонала в определенных зонах.

5.3. Количество пользователей

Количество пользователей системы – параметр, определяющий максимальное количество пользователей системы, которые могут иметь право доступа в одну точку прохода. Интегрированная система «Фортеця» поддерживает (для одного сегмента) - 14 336 пользователей.

При использовании много сегментной схемы построения, в которой пользователь имеет доступ только в пределах одного сегмента (одного управляющего контроллера), количество пользователей увеличивается до 64 x 14 336 = 917 504.

5.3.1. Статус пользователя (идентификатора)

Под статусом пользователя понимается состояние идентификатора, хранящегося в энергонезависимой памяти управляющего контролера. Статус пользователя имеет два состояния:

- Активен;
- Неактивен.

Под состоянием «активен» предполагается, что данный идентификатор (проксимити - карточка) находится в памяти контроллера и позволяет пользователю иметь право доступа в определенные точки прохода.

Под состоянием «неактивен» предполагается, что данный идентификатор (проксимити - карточка) находится в памяти контроллера, но не позволяет пользователю иметь право доступа ни в какие точки прохода.

!!! Интегрированная система «Фортеця» позволяет реализовать изменение статуса пользователя без прекращения работоспособности системы разграничения доступа.

Данная функция применяется на объектах, где помимо постоянных пользователей активно присутствуют временные пользователи системы. Изменение статуса карточки позволяет быстро ее активизировать при выдаче посетителю и делать её неактивной по истечению времени пребывания на данном объекте.

5.4. Список событий

Список событий – параметр, определяющий максимальное количество событий, хранящихся в памяти одного управляющего контроллера. Интегрированная система «Фортеця» поддерживает (для одного сегмента) - 10 752 записей.

При использовании много сегментной схемы построения список событий всей системы будет равен 64 х 10 752 = 688 128.

Событием в системе является любое изменение, вызванное как внешним воздействием на систему, так и внутренним – по встроенным временным часам. Например, событием, вызванным внешним воздействием является: факт прохода через любую точку прохода, нарушение охранной зоны, попытка несанкционированного прохода, и т.д.

Внутренним событием является факт автоматической постановки под охрану группы в определенное время. Например, в 20.00 по команде внутренних часов и т.д.

!!! Интегрированная система ”Фортеця» обеспечивает хранение списка событий в своей энергонезависимой памяти. Сбой системы электропитания или персонального компьютера не приведет к потере списка событий.

5.5. Уровень доступа

Под уровнем доступа понимается список пользователей, которым разрешено проходить через данную точку прохода. В данный список вносятся все точки прохода, через которые данному пользователю разрешен проход. Как правило, в данном списке дополнительно присутствуют данные о временных зонах (см. пункт 5.6). Интегрированная система «Фортеця» поддерживает 64 уровня доступа. Это означает, что можно сформировать 64 списка, в каждом из которых, ограничить возможность в доступе конкретных физических лиц по определенным точкам прохода.

Пример. Система доступа имеет четыре точки прохода. Количество физических лиц – 10. необходимо организовать три уровня доступа.

Уровень доступа №1

Физическое лицо	Точки прохода
1. Иванов	№ 2, 3
2. Сидоров	
3. Петров	
4. Дубинин	

Уровень доступа №2

Физическое лицо	Точки прохода
1. Пупкин	№ 1, 3
2. Заморин	
3. Травкин	
4. Волкова	

Уровень доступа №3

Физическое лицо	Точки прохода
1. Зябликов	№ 4
2. Заболотный	

5.6. Временная зона

Под временной зоной понимается график интервалов времени, в течение которых данному пользователю в данной точке прохода, разрешен доступ. Например, временной зоной для физического лица – Иванова, будет являться следующий график:

разрешение входа с 8.45 до 9.15;
разрешение входа\выхода с 12.45 до 13.45;
разрешение выхода с 18.00 до 18.30;
запрет входа\выхода с 18.30 до 8.45.

Примечание. В *системе указывается только интервалы времени, в течение которых, доступ разрешен, соответственно в остальное время доступ будет запрещен*.

!!! Интегрированная система ”Фортеця» допускает сформировать в пределах одних суток четыре временных интервала с разрешенным доступом, что позволяет гибко формировать рабочий график для разных групп пользователей.

Временная зона позволяет указать интервалы доступа не только в течение одних суток, но и сделать распределение по:

- Рабочим дням;
- Выходным дням;
- Любой выбранной дате.

5.6.1. Периодичность временной зоны

Понятие временной зоны предполагает взаимосвязь с параметром периодичности или кратности временной зоны.

Под периодичностью временной зоны понимается максимальная продолжительность временной зоны с какими-либо параметрами, выраженная в количестве дней недели, после которого происходит повторение параметров по данной временной зоне.

Пример. Необходимо сформировать временную зону с 7 дневной кратностью для некоего списка сотрудников. Точка прохода - «Проходная».

Дни недели							
Функция	Понед.	Вторник	Среда	Четверг	Пятница	Суббота	Воскр.
Разрешить доступ	8.45-18.30	8.45-18.30	8.45-18.30	8.45-18.30	8.45-18.30	X	X

Для списка сотрудников сформирована временная зона, по которой они в течение 5-ти рабочих дней могут проходить через «проходную» завода, а в субботу и воскресенье доступ им запрещен. На следующей рабочей неделе данный список повторяется. Следовательно, периодичность временной зоны составляет 7 дней.

!!! Интегрированная система ”Фортеця» поддерживает периодичность временных зон с периодом от 1-х до 7-ми дней, что позволяет гибко формировать уровни доступа сотрудников на предприятиях, использующих посменный график работы.

Пример. Необходимо сформировать временную зону с 3-х дневной периодичностью для некоего списка сотрудников. Точка прохода - «Проходная».

Дни недели							
Функция	Понед.	Вторник	Среда	Четверг	Пятница	Суббота	Воскр.
Разрешить доступ	8.45-18.30	8.45-18.30	14.00-15.00	8.45-18.30	8.45-18.30	14.00-15.00	8.45-18.30
	Кратность 3 дня			Кратность 3 дня			

Для списка сотрудников сформирована временная зона, по которой они в течение 2-х дней могут проходить через «проходную» завода, а на третий - имеют доступ только в ограниченное время. Через каждые три дня данный список повторяется. Следовательно, периодичность временной зоны составляет 3 дня.

5.7. Контроль повторного прохода – « AntiPass Back»

Функция « AntiPass Back» (контроль повторного прохода) – определяет возможность прохода дважды по одному и тому же идентификатору через одну и ту же точку прохода.

Если данная функция на конкретной точке прохода включена, то пользователь, пройдя через эту точку внутрь помещения и передав кому–либо свой пропуск-идентификатор, не сможет добиться повторного разрешения для входа через данную точку прохода. Система выдаст предупредительное сообщение оператору системы: «Доступ запрещен. Контроль повторного входа».

Если помещение имеет несколько точек прохода, то есть в одно помещение можно войти\выйти через несколько дверей, то эти точки прохода определяются в так называемую «зону доступа».

Если пользователь покинул территорию данной зоны, не отметившись, система, при его попытке вновь попасть внутрь, выдаст предупредительное сообщение оператору и заблокирует проход.

6. Элементы охраны

6.1. Общее описание

Охраной называется комплекс технических и организационных мероприятий, позволяющих обеспечить сохранность материального и нематериального имущества на охраняемой территории.

В качестве охраняемого объекта могут выступать как материальные, так и нематериальные ценности.

В данном разделе, будут рассмотрены только методы организации охраны материальных объектов техническими средствами интегрированной системы «Фортеця».

Одним из элементов охраняемого объекта является охраняемое помещение (территория).

Охраняемым помещением (территорией) является место, оснащенное элементами технической средствами охраны.

Под техническими средствами охраны подразумеваются средства, обеспечивающие достоверный контроль помещения по каким-либо физическим параметрам (например, тепловым(инфракрасным), объемным, на разрушение физической цепи, и т. д.).

Приборы, реализующие конкретные методы контроля, называются датчиками. Например, прибор, позволяющий контролировать помещение по тепловому излучению, является инфракрасным датчиком.

Описание принципов работы различных датчиков не входит в данное руководство, и далее не рассматривается.

Сигналы, формируемые различными датчиками, поступают на охранные шлейфы.

Охранный шлейф позволяет контролировать сигналы от одного или нескольких датчиков одновременно. Основными сигналами, которые формируются охранным шлейфом, являются:

- «норма» - нет нарушения охранного шлейфа;
- «тревога» - есть нарушение шлейфа.

Охранный шлейф может формировать ряд дополнительных сигналов, позволяющих контролировать свою работоспособность (исправное состояние).

6.1.1. Понятие охранной зоны

Под охранной зоной понимается охранный шлейф, сигналы состояния которого были обработаны по специальным алгоритмам.

6.1.2. Понятие охранной группы

Охранной группой называется от одной до нескольких охранных зон, объединенных в одну условную группу с целью удобства постановки\снятия их под охрану.

6.1.3. Понятие постановки\снятия под охрану

Под постановкой системы под охрану понимается комплекс мероприятий, после выполнения которых, система производит выработку сигналов тревоги при нарушении какой-либо из зон.

Под снятием системы с охраны понимается комплекс мероприятий, после выполнения которых, система игнорирует выработку сигналов тревоги даже при нарушении какой-либо из зон.

6.1.4. Задержка времени на вход\выход

Под задержкой времени понимается интервал времени, в течение которого не производится формирование сигналов «Тревога» в процессе постановки\снятия объекта под охрану. Как правило, на объекте выделяются специальные зоны – «зоны с задержкой».

Время задержки на вход - это время, на которое задерживается выработка сигнала тревоги при нарушении «зоны с задержкой» при снаряженной системе.

Время задержки на выход - время, в течение которого можно выйти из охраняемого помещения после постановки системы под охрану, не вызывая тревоги.

6.1.5. Реакция системы - формирование сигналов тревоги

Реакцией системы является совокупность действий, производимых системой охраны на наличие сигнала «тревога» с какой-либо из охранных зон. В простейшем варианте это может быть включение сирены при нарушении охранной зоны.

6.2. Организация охранных зон в системе « Фортеця»

Организация охранных зон в интегрированной системе “Фортеця” производится на базе модуля RAM-8. Функциональное описание модуля указано в “Руководстве пользователя. Модуль RAM-8”.

Программное обеспечение позволяет группировать зоны в группы. Минимальное количество зон входящих в одну группу – 1. Максимальное количество зон входящих в одну группу – 128. В одну и ту же группу могут входить охранные шлейфы, физически расположенные на разных модулях RAM-8, но принадлежащих к одному управляющему контролеру.

Одна и та же зона не может входить одновременно в две группы сразу, поэтому максимальное количество групп, для одного управляющего контроллера – 128.

Модуль RAM-8 обеспечивает решение следующих задач:

- прием данных с различных датчиков охраны;
- анализ состояния охранного шлейфа;
- формирование сигналов «тревога», «норма»;
- формирование сигналов «короткое замыкание», «обрыв»;
- диагностический контроль состояния охранного шлейфа;
- управление процессом постановки\снятия зоны под охрану;
- управление релейным модулем.

Аппаратный контроль состояния охранного шлейфа модуля RAM-8 подразделяется на два основных типа:

- «сухой» контакт;
- с контролем целостности.

6.2.1. Охранный шлейф типа «сухой» контакт

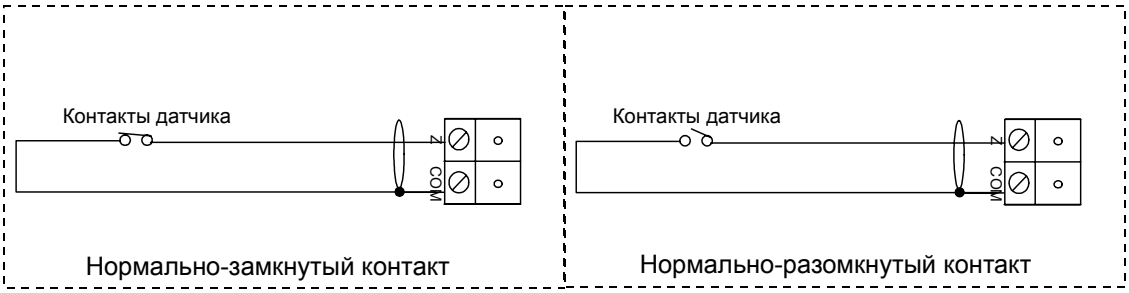
Модуль RAM-8 способен работать с двумя вариантами охранного шлейфа типа «сухой контакт»:

a) нормально-замкнутый;
b) нормально-разомкнутый.

Для шлейфа типа «сухой контакт» модуль отслеживает только два состояния шлейфа:

1. короткое замыкание шлейфа
2. обрыв шлейфа

Принципиальная схема подключения охранного шлейфа изображена на следующем рисунке. Физически данный тип шлейфа представляет собой провод, оканчивающийся контактами охранного датчика.



Подключение шлейфа охраны
без оконечного сопротивления -
“сухой контакт”

Для нормально-замкнутого шлейфа состоянию “Норма” соответствует - “КЗ”, состоянию “Не норма” соответствует - “Обрыв”.

Для нормально-разомкнутого шлейфа состоянию “Норма” соответствует - “Обрыв”, состоянию “Не норма” соответствует - “КЗ”.

6.2.2. Организация охранного шлейфа с контролем «целостности»

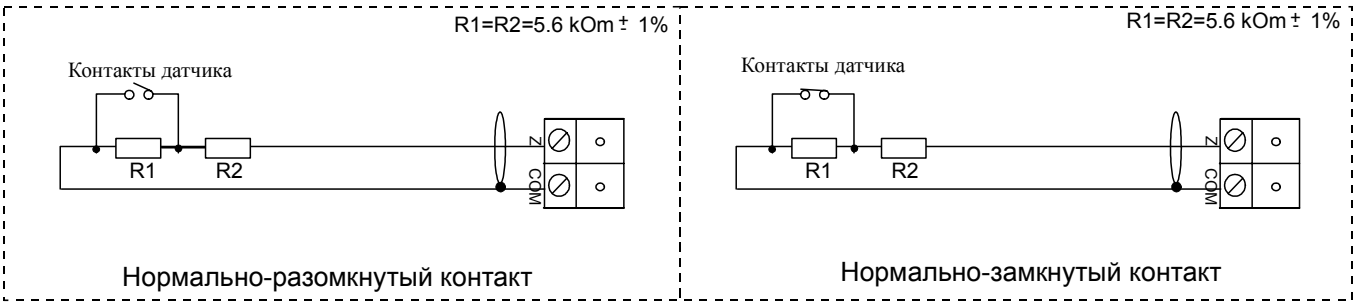
Модуль RAM-8 поддерживает следующие варианты охранного шлейфа «с контролем целостности»:

a) нормально-замкнутый;
b) нормально-разомкнутый.

Для шлейфа «с контролем целостности» модуль отслеживает четыре состояния:

1. “КЗ”- короткое замыкание шлейфа;
2. “Обрыв”- обрыв шлейфа;
3. “Норма” (R1) – нормальное состояние шлейфа;
4. “Тревога” (R1+R2) – наличие сигнала тревоги.

Принципиальная схема подключения охранного шлейфа изображена на следующем рисунке.



Подключение шлейфа охраны с двойным оконечным сопротивлением

Физически данный тип шлейфа представляет собой провод, оканчивающийся контактами охранного датчика с подключенными оконечными сопротивлениями.

Для нормально-замкнутого шлейфа состоянию “Норма” соответствует - R1, состоянию “Тревога» - R1+R2.

Для нормально-разомкнутого шлейфа состоянию “Норма” соответствует - R1, состоянию “Тревога» - R1+R2.

Детальное описание технических параметров шлейфа с двойным оконечным сопротивлением смотрите: «Руководство пользователя. Модуль RAM-8».

!!! Интегрированная система «Фортеця» позволяет гибко определять тип охранного шлейфа. Модуль RAM-8 позволяет работать с различными вариантами охранного шлейфа одновременно, как «сухой контакт», так и с «контролем целостности», а также произвольно определять их количество на своем борту.

6.2.3. Дистанционный контроль состояния охранного шлейфа

Для диагностики состояния любого из 128 охранных шлейфов достаточно дать команду посредством верхнего программного обеспечения. Оператор системы может производить контроль сопротивления шлейфа, переведя данный охранный шлейф в режим «тест».

!!! Интегрированная система «Фортеця» позволяет дистанционно производить измерение сопротивления охранного шлейфа, что существенно упрощает процесс инсталляции и диагностики системы.

6.3. Тип охранной зоны

Данные, приходящие с охранного шлейфа, математически могут быть обработаны различными алгоритмами. В зависимости от алгоритма обработки интегрированная система позволяет сформировать четыре основных типа охранных зон:

1. Зона с задержкой;
2. Внутренняя зона;
3. Мгновенная зона;
4. 24-х часовая зона.

6.3.1. Зона с задержкой

При постановке\снятии под охрану группы, куда входят зоны с задержкой, происходит задержка выработки сигнала «тревога» на установленный интервал. Интервал задержки может колебаться от 0 до 255 секунд. По истечению данного интервала, если не поступила команда снятия с охраны, производится выработка сигнала «тревога».

Интервал задержки распространяется на все зоны в пределах данной группы, которые определены как зоны с задержкой.

Зона с задержкой используется для возможности покинуть охраняемое помещение при: постановке под охрану, снятии с охраны без формирования сигнала «тревога».

6.3.2. Внутренняя зона

Внутренняя зона – зона, входящая в группу и логически связанная с зоной с задержкой. При постановке под охрану на данную зону распространяется задержка по входу \ выходу, если сначала происходит нарушение зоны с задержкой, а потом внутренней зоны.

Если нарушение происходит в обратном порядке, то сигнал «тревога» формируется мгновенно.

При постановке под охрану периметра группы, в случаях нарушения данной зоны, сигнал «тревога» не формируется.

6.3.3. Мгновенная зона

Мгновенная зона – зона, входящая в группу. При постановке под охрану, на данную зону задержка не распространяется.

Если происходит нарушение, то сигнал «тревога» формируется мгновенно.

При постановке под охрану периметра группы, в случаях нарушения данной зоны сигнал «тревога» формируется мгновенно.

6.3.4. 24-х часовая зона

24-х часовая зона – зона, входящая в группу. 24-х часовая зона не может быть снята с охраны. Под охрану зона становится с момента загрузки конфигурации в управляющий контроллер.

Если происходит нарушение, то сигнал «тревога» формируется мгновенно.

6.4. Постановка\снятие групп под охрану

Постановка\снятие групп может производиться пользователем одним из трех способов:

- с помощью клавиатуры;
- с помощью верхнего программного обеспечения;
- с помощью системы реакций.

!!! Интегрированная система ”Фортеця» позволяет производить постановку под охрану, снятие с охраны любой из 128 групп с позонной постановкой.

Посредством клавиатуры или верхнего программного обеспечения «Фортеця» пользователь может производить следующие действия:

- Производить выбор необходимой группы;

- Осуществлять контроль состояния выбранной группы:
  - группа поставлена под охрану;
  - группа под охраной, было нарушение в группе;
  - группа с охраны снята и готова к постановке;
  - группа с охраны снята и не готова к постановке под охрану.
- Производить постановку \ снятие с охраны выбранной группы.

6.4.1. Постановка\снятие под охрану посредством клавиатуры

Постановка\снятие осуществляется посредством клавиатуры совмещенной с проксимити-считывателем. Для постановки\снятия конкретной группы идентификатор пользователя должен иметь разрешение для постановки соответствующей группы под охрану. За идентификатором пользователя программным путем можно закрепить любую из 128 групп охраны.

За каждым пользователем можно закрепить от 1-й до 128–ми групп охраны. Каждому пользователю, имеющему право постановки\снятия под охрану, формируется индивидуальный 4-х значный номер – ПИН код пользователя.

Для постановки\снятия под охрану может использоваться любая из клавиатур в пределах одного управляющего контролера.

6.4.1.1. Выбор группы

Выбор группы осуществляется посредством считывания идентификатора пользователя. Для считывания необходимо кратковременно поднести проксимити-карту к клавиатуре. Клавиатура, считав код карточки, выдаст короткий звуковой сигнал и переведет светодиодный индикатор в режим индикации выбора группы.

Клавиатура не перейдет в режим выбора группы, если за данной проксимити-картой не закреплена ни одна из групп.

После ввода проксимити-карты пользователю необходимо набрать номер группы. Устройство воспринимает номер группы и подтверждает это длинным звуковым сигналом. Пользователь получает отказ если:

- неправильно введен номер группы или такого номера не существует;
- данному пользователю не разрешена постановка под охрану данной группы.

6.4.1.2. Индикация состояния группы.

Режим индикации состояния группы позволяет определить, в каком состоянии находится данная группа.

Индикация производится с момента ввода номера группы. На светодиодном индикаторе клавиатуры отображается один из статусов состояния данной группы:

1) группа поставлена под охрану;
2) группа под охраной, было нарушение в группе;
3) группа с охраны снята и готова к постановке;
4) группа с охраны снята и не готова к постановке под охрану.

6.4.1.3. Команды постановки\снятия под охрану.

Командный режим предназначен для перевода группы из состояния – «под охраной», в состояние – «с охраны снято» и обратно.

Ввод команды осуществляется в формате [1] [3456] *, где [1] –тип команды, 3456 – индивидуальный ПИН код пользователя, * - признак окончания ввода.

Перечень команд системы:

0 -команда снятия с охраны
1- команда постановки под охрану
3 - команда постановки под охрану группы принудительно (неготовность группы)
6 - команда снятия с охраны под принуждением (в случае угрозы)

8 - команда постановки под охрану периметра

Если постановка под охрану прошла успешно на светодиодном индикаторе отображается новый статус данной группы.

6.5. Реакция системы

При нарушении охранной зоны система формирует ряд последовательных действий, определяемых заранее с помощью программного обеспечения «Фортеця». Под последовательностью действий подразумевается управление теми или иными исполнительными устройствами, подключенными к интегрированной системе посредством модулей релейных выходов. См. «Руководство пользователя. Модуль RAM-8. Модуль RM8».

В качестве исполнительных устройств могут выступать: сирены, системы тревожного оповещения, системы видео наблюдения, системы видеозаписи и т.д.

Систему реакций условно можно разбить на два уровня:

- Аппаратный уровень, в пределах одного модуля RAM-8;
- Программный уровень, в пределах одного управляющего контроллера.

6.5.1. Аппаратный уровень

Под аппаратным уровнем реакции подразумевается возможность модуля охранных шлейфов RAM-8 производить непосредственное управление дополнительным модулем релейных выходов RM8, в зависимости от состояния охранных шлейфов. См. «Руководство пользователя. Модуль RAM-8. Модуль RM8».

Каждое из восьми реле модуля RM8 жестко закреплено за одной из охранных зон модуля RAM-8. Включение соответствующего реле будет производиться, если охранный шлейф находится в одном из состояний:

- короткое замыкание;
- обрыв;
- тревога;
- норма;
- на охране;
- с охраны снято.

Выбор состояния охранного шлейфа производится аппаратно на модуле RAM-8 путем установки соответствующих микропереключателей.

6.5.2. Программный уровень

В режиме «Программный» функциональное назначение каждого из реле, подключенного к управляющему контроллеру, будет определяться программным обеспечением «Фортеця». Последовательность действий системы формируется так называемой системой реакций.

Система реакций – порядок взаимодействия отдельных частей системы, определяемый оператором системы посредством верхнего программного обеспечения.

!!! Интегрированная система ”Фортеця» позволяет производить функциональное назначение любого из 128 реле программным путем.

7. Функциональное назначение отдельных частей системы

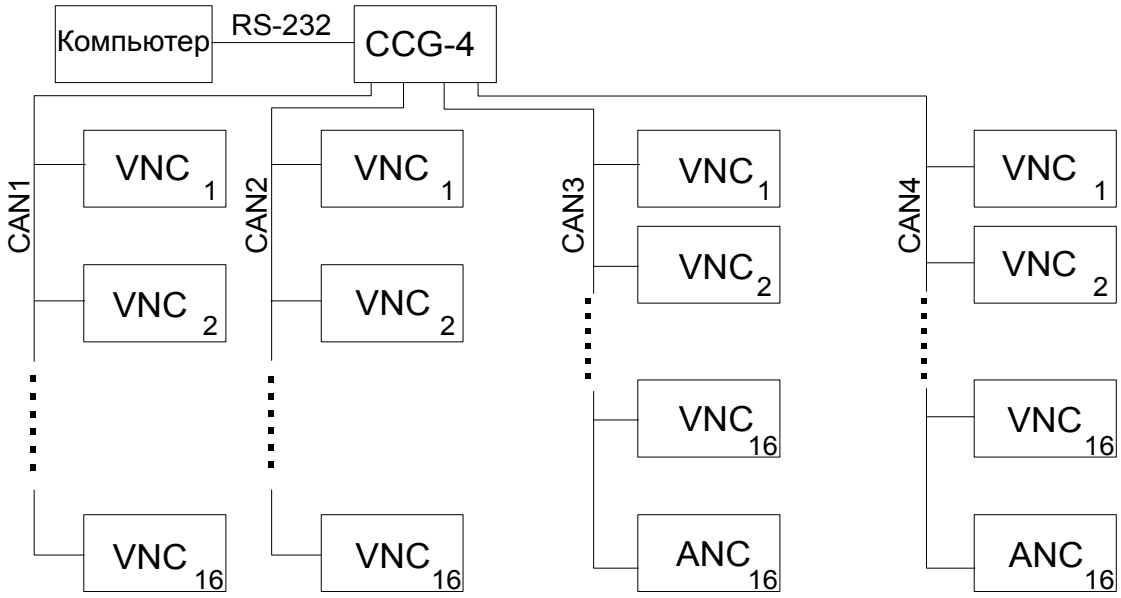
7.1. Конверторы связи

Конверторы связи предназначены для объединения управляющих контроллеров в единую систему, преобразования форматов данных с одного интерфейса в другой и их последующей передачи на персональный компьютер. Конверторы связи обеспечивают гальванически развязанный канал связи между управляющими контроллерами и персональным компьютером.

7.1.1. Конвертор CCG-4

Конвертор связи CCG-4 предназначен для объединения контроллеров VNC, ANC в систему связи до 64-х контроллеров (для каждого типа контролера), а так же для стыка системы с персональным компьютером. Конвертор обеспечивает подключение до 16-ти контроллеров VNC,ANC на один CAN канал, а также позволяет расширить количество CAN каналов до 4-х посредством установки модуля расширения CAN канала - CA-16. Конвертор позволяет установить дополнительно до 3-х модулей расширения CA-16.

Функциональное назначение контролера изображено на рисунке.



К каждому каналу допускается подключение произвольного количества контроллеров ANC и VNC, но не более 16-ти каждого типа. Пример: на рисунке изображено подключение 16-ти контролеров VNC на первом и втором каналах связи. К третьему и четвертому, помимо контролеров VNC, дополнительно подключено 32 контролера ANC, по 16 на каждый канал.

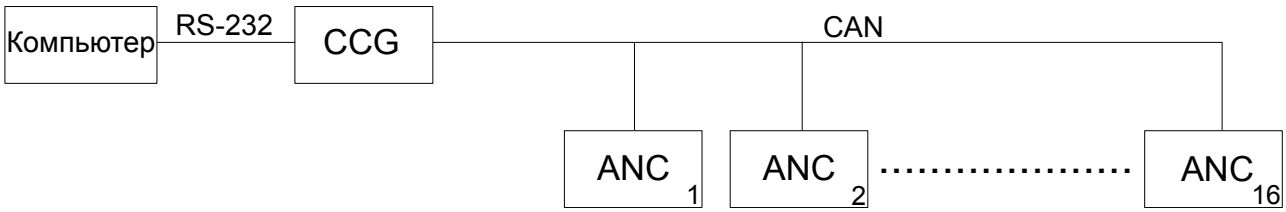
!!! Конвертор святи CCG-4 обеспечивает гальваническую развязку всех четырех каналов связи между собой, а также позволяет индивидуально установить скорость обмена с управляющими контроллерами по каждому из каналов связи.

Конвертор CCG-4 обеспечивает дополнительно контроль параметров питающего напряжения и целостность датчика вскрытия корпуса.

7.1.2. Конвертор CCG

Контроллер связи CCG предназначен для объединения контроллеров ANC в систему связи, а так же для стыка системы с персональным компьютером. Обеспечивает подключение до 16-ти контроллеров ANC на один CAN канал.

Контроллер связи CCG не позволяет объединять контроллеры VNC. Функциональное назначение контролера изображено на рисунке.



Конвертор CCG обеспечивает дополнительно контроль параметров питающего напряжения и целостность датчика вскрытия корпуса.

7.2. Функциональное назначение управляющих контроллеров

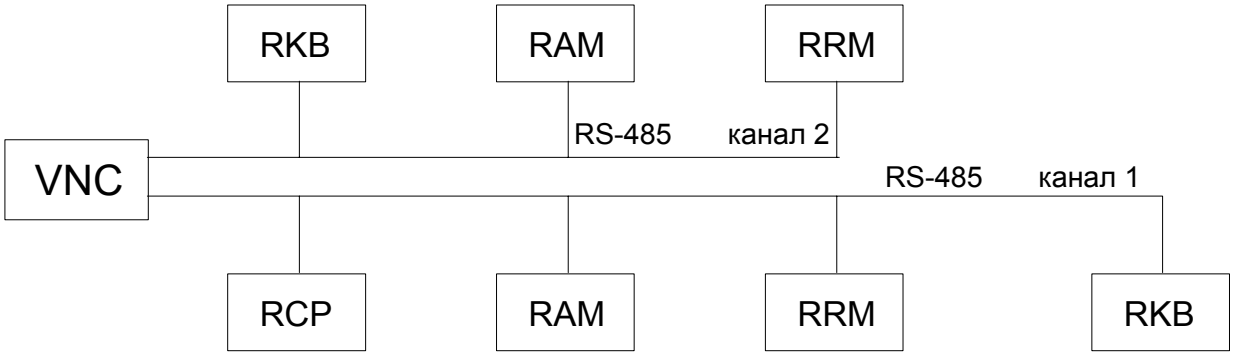
7.2.1. Контроллер VNC

Универсальный контроллер VNC предназначен для систем управления доступом и охранной сигнализацией. Энергонезависимая память на 14336 номеров идентификаторов, 10752 событий, 64 временные зоны, 64 уровня доступа. Контроллер обеспечивает подключение посредством дополнительных модулей до 128-ми охранных зон, до 128-ми релейных выходов, до 32-х считывателей.

Управляющий контроллер VNC обеспечивает решение следующих основных задач:

- работа в автономном режиме (без участия компьютера);
- организация систем разграничения доступа до 32-х считывателей;
- поддержка функции замкнутых зон для 16-ти двусторонних точек прохода;
- организация охраны объекта (до 128-ми охранных групп);
- обеспечение по зонной постановки любой из групп охраны;
- управление до 128-ми релейными выходами;
- реализация системы реакций;
- накопление базы данных событий в энергонезависимой памяти.

Функциональное назначение контролера изображено на рисунке.



Управляющий контролер VNC обеспечивает дополнительно контроль параметров питающего напряжения и целостность датчика вскрытия корпуса.

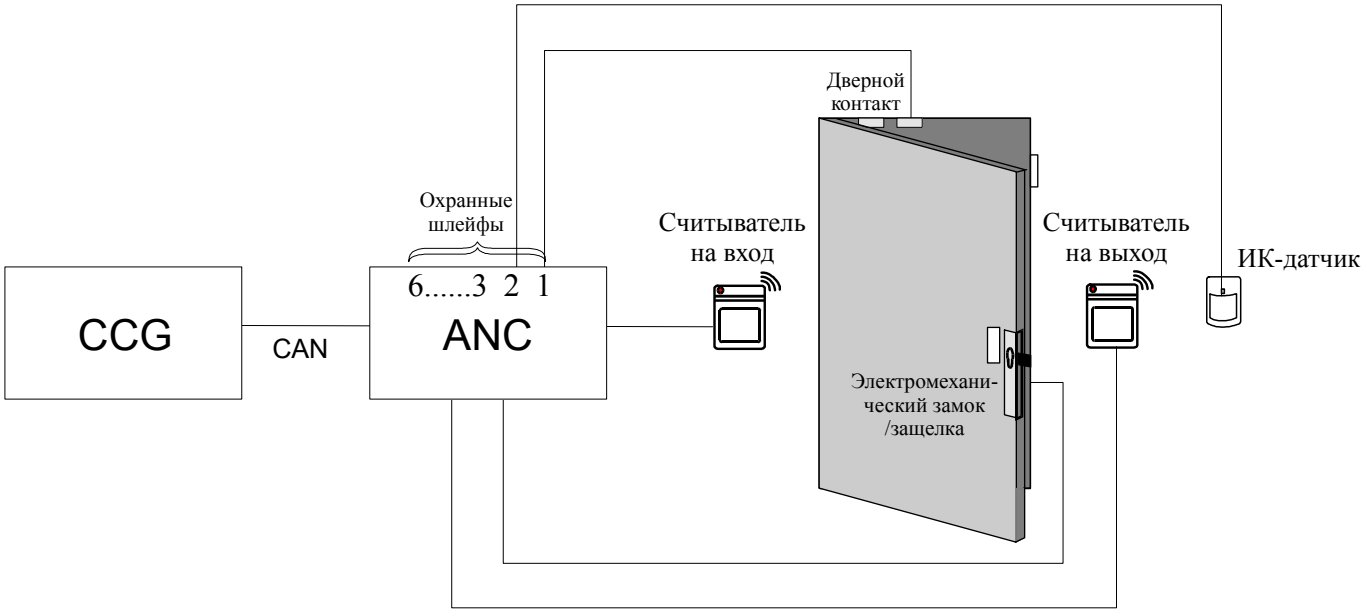
7.2.2. Контроллер ANC

Контроллер ANC предназначен для реализации систем управления доступом и охранной сигнализацией. Энергонезависимая память на 4096 номеров карт, 4096 событий, 64 временные зоны, 64 уровня доступа.

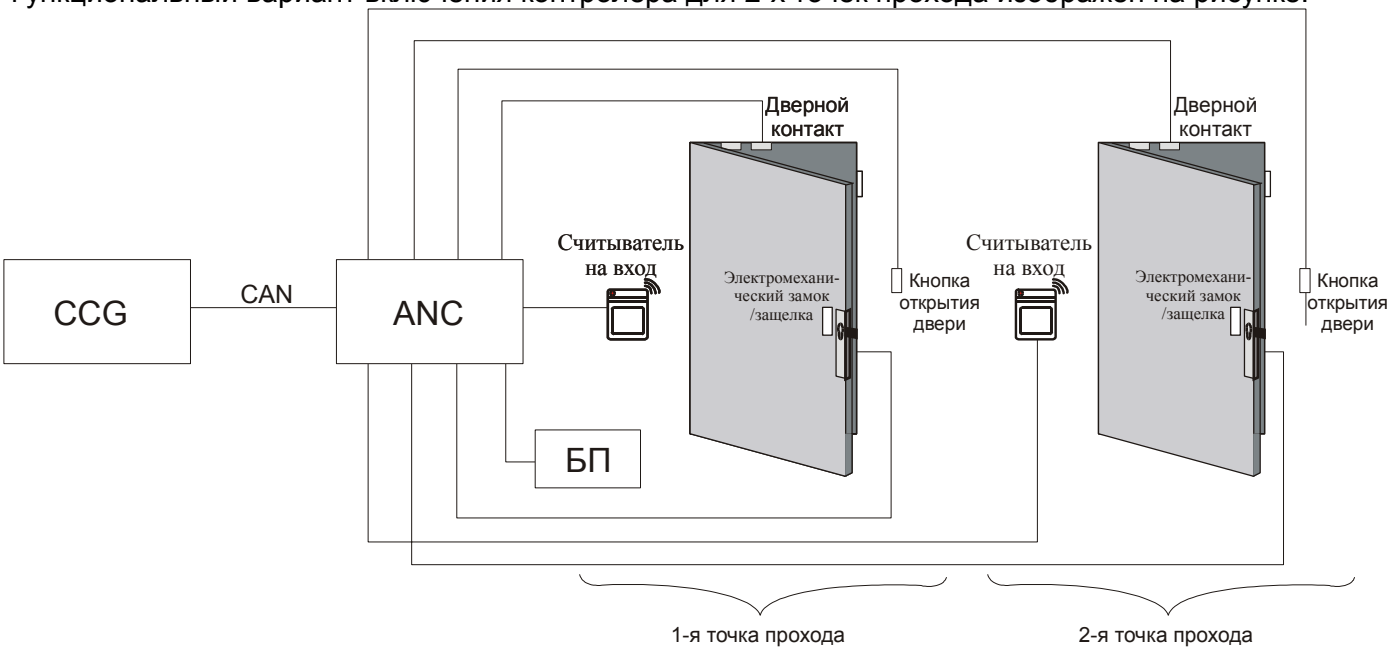
Управляющий контроллер ANC обеспечивает решение следующих основных задач:

- работа в автономном режиме (без участия компьютера);
- организация систем разграничения доступа до 2-х считывателей;
- организация охраны объекта до 6-ти охранных групп;
- управление 4-мя релейными выходами;
- реализация системы реакций;
- накопление базы данных событий в энергонезависимой памяти.

Функциональный вариант включения контролера для двусторонней точки прохода изображен на рисунке.



Функциональный вариант включения контролера для 2-х точек прохода изображен на рисунке.



Управляющий контролер ANC обеспечивает дополнительно контроль параметров питающего напряжения и целостность датчика вскрытия корпуса.

7.3. Функциональное назначение модулей удаленного управления RCP

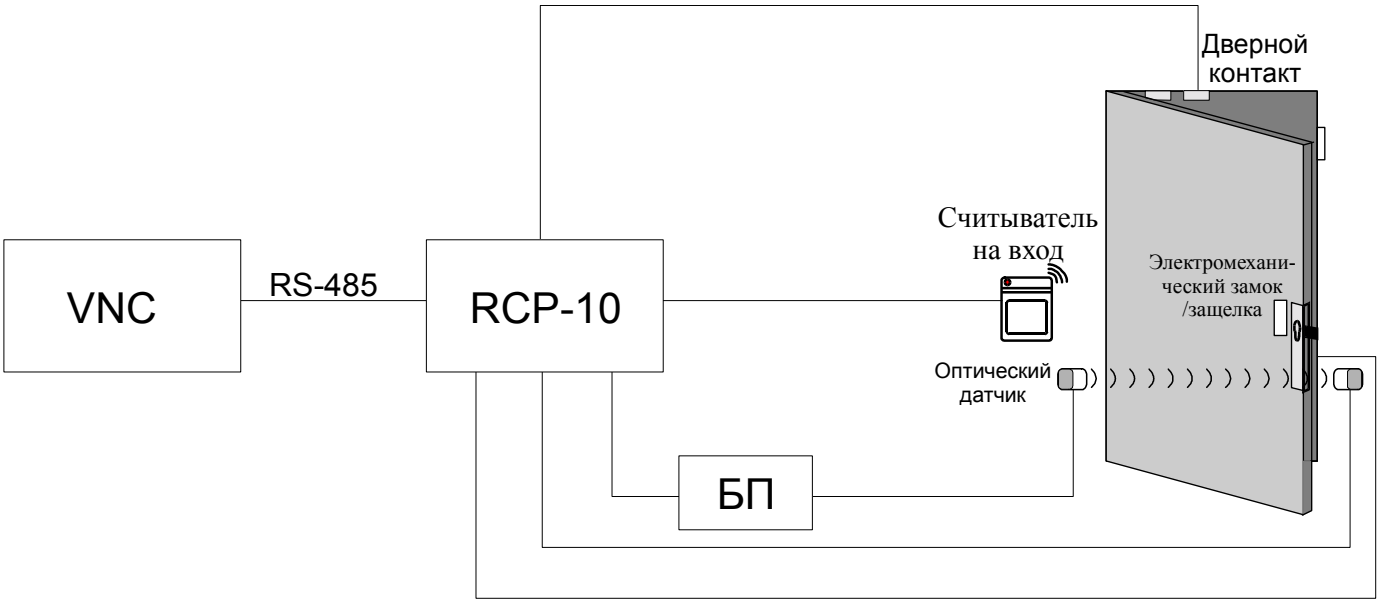
7.3.1. Модуль RCP10

Устройство RCP-10 представляет собой модуль удаленного управления электромагнитным/электромеханическим замком/защелкой и предназначен для организации одной точки прохода. Обеспечивает подключение:

- 1-го считывателя с интерфейсом Виганда;
- 1-го датчика состояния точки прохода;
- 1-го дополнительного (оптического) датчика;
- 1-й кнопки разблокировки точки прохода;
- 1-й дополнительной сирены;
- датчика вскрытия корпуса.

До 32 модулей RCP-10 может быть подключено к одному контроллеру VNC через коммуникационную линию связи стандарта RS - 485. Модуль RCP-10 обеспечивает дополнительно контроль параметров питающего напряжения.

Функциональное назначение контролера изображено на рисунке.



Модуль RCP-10 обеспечивает дополнительно контроль параметров питающего напряжения.

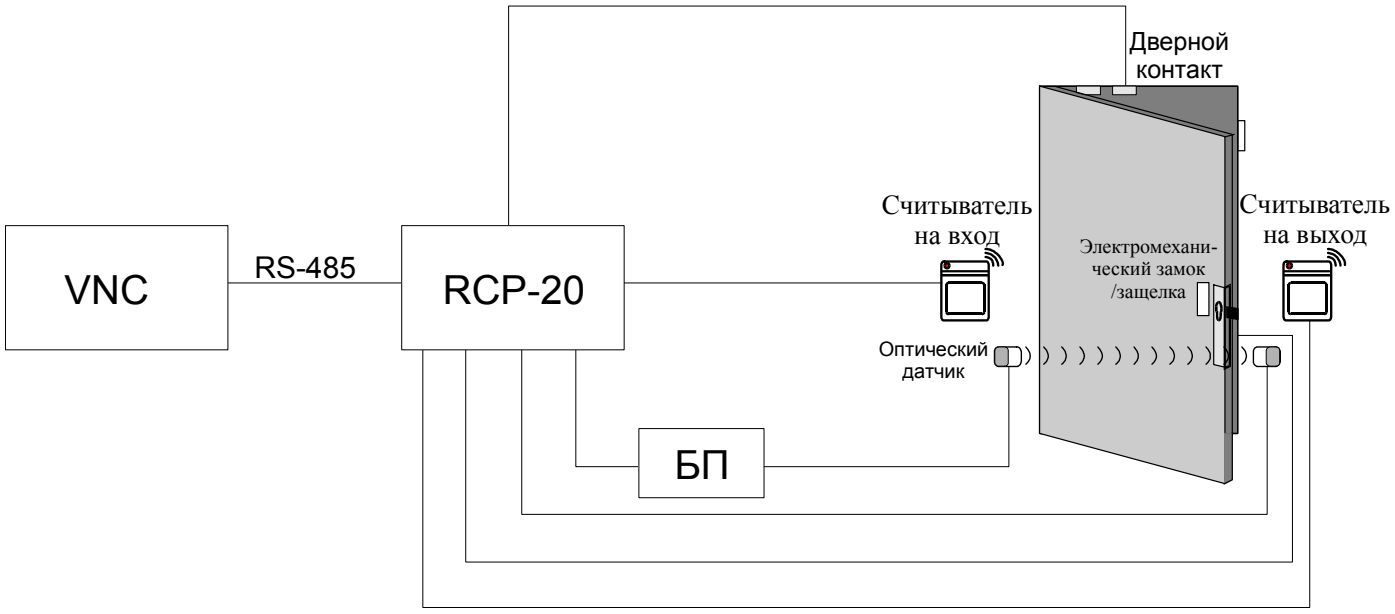
7.3.2. Модуль RCP20

Устройство RCP-20 представляет собой модуль удаленного управления электромагнитным/механическим замком/защелкой и предназначен для организации одной точки прохода. Обеспечивает подключение:

- 2-х считывателей с интерфейсом Виганда;
- 1-го датчика состояния точки прохода;
- 1-го дополнительного (оптического) датчика;
- 1-й кнопки разблокировки точки прохода;
- 1-й дополнительной сирены;
- датчика вскрытия корпуса.

Максимально 16 модулей RCP-20 может быть подключено к одному контроллеру VNC через коммуникационную линию связи стандарта RS - 485. Модуль RCP-20 обеспечивает дополнительно контроль параметров питающего напряжения.

Функциональное назначение контролера изображено на рисунке.



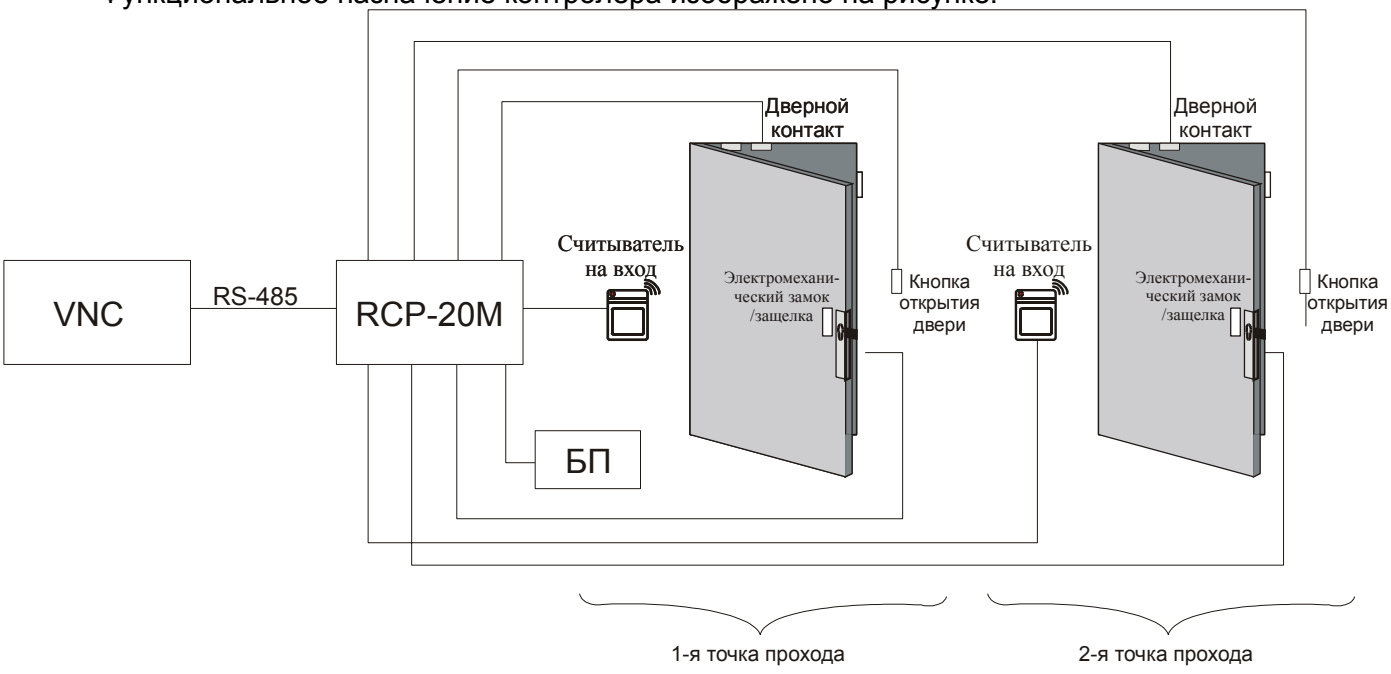
7.3.3. Модуль RCP20м

Устройство RCP-20M представляет собой модуль удаленного управления электромагнитными/механическими замками/защелками и предназначен для организации двух точек прохода с контролем входа по считывателю и кнопкой для выхода. Обеспечивает подключение:

- 2-х считывателей с интерфейсом Виганда;
- 2-х датчиков состояния точки прохода;
- 2-х кнопок разблокировки точки прохода;
- 1-й дополнительной сирены;
- датчика вскрытия корпуса.

Максимально 16 модулей RCP-20M может быть подключено к одному контроллеру VNC через коммуникационную линию связи стандарта RS - 485. Модуль RCP-20M обеспечивает дополнительно контроль параметров питающего напряжения.

Функциональное назначение контролера изображено на рисунке.



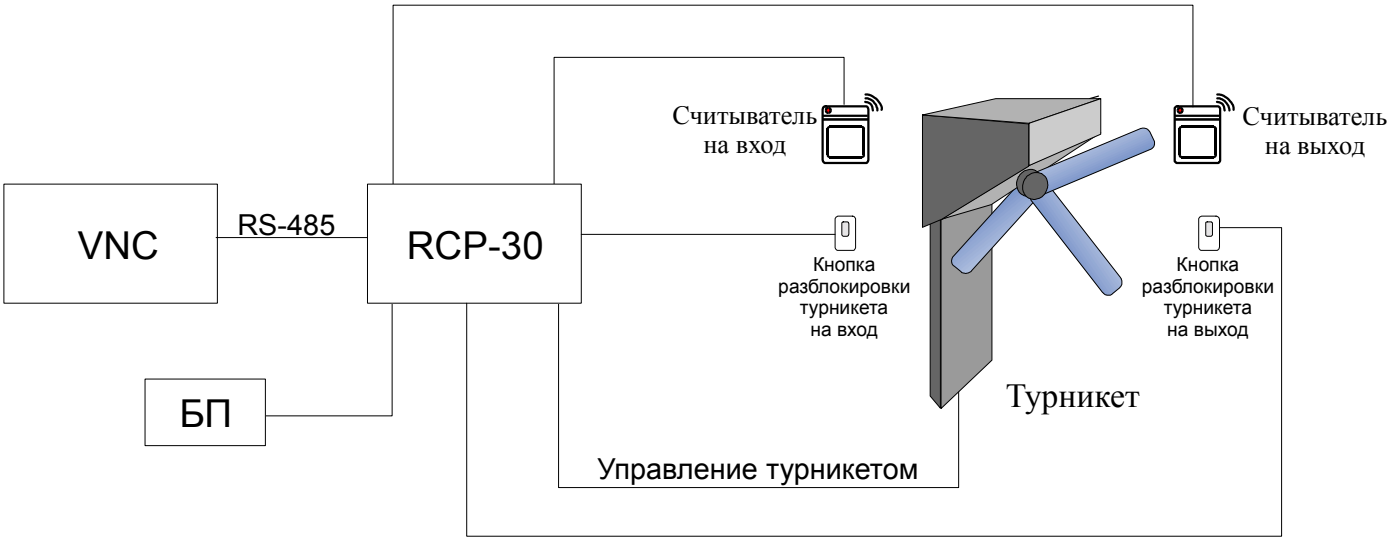
7.3.4. Модуль RCP30

Устройство RCP - 30 представляет собой модуль удаленного управления турникетом и предназначен для организации одной точки прохода. Обеспечивает подключение:

- 2-х считывателей с интерфейсом Виганда;
- 1-го датчика состояния точки прохода;
- 2-х кнопок разблокировки точки прохода;
- датчика вскрытия корпуса.

Максимально 16 модулей RCP - 30 может быть подключено к одному контроллеру VNC-4 через коммуникационную линию связи стандарта RS - 485. Модуль RCP-30 обеспечивает дополнительно контроль параметров питающего напряжения.

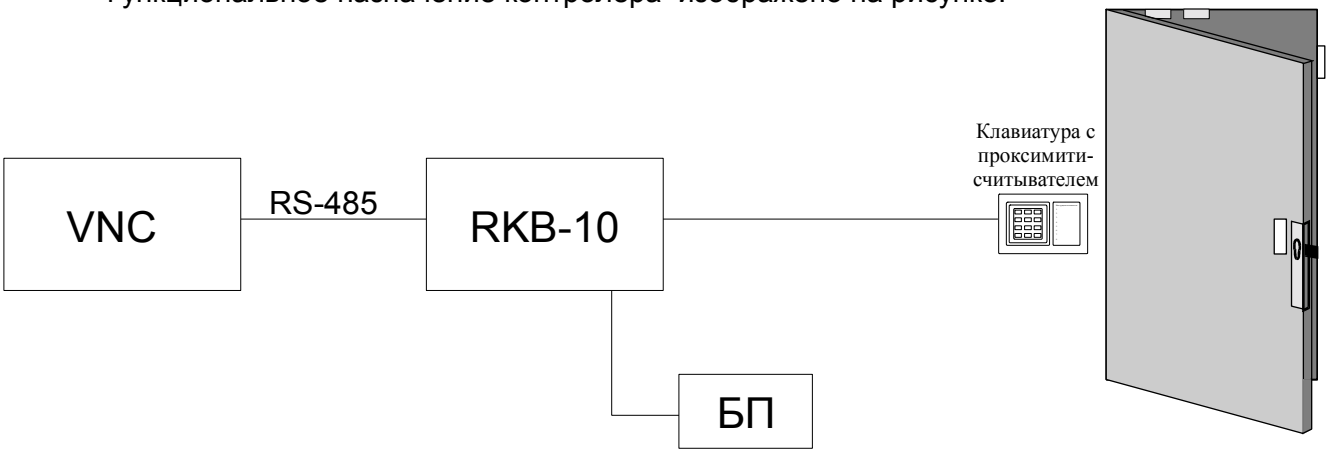
Функциональное назначение контролера изображено на рисунке.



7.4. Функциональное назначение модуля RKB-10

Устройство RKB-10 представляет собой модуль удаленного подключения клавиатуры и предназначен для организации точки управления охранными зонами. Обеспечивает подключение 1-й клавиатуры, совмещенной с проксимити-считывателем по интерфейсу Виганда. До 32 модулей RKB-10 может быть подключено к одному контроллеру VNC-4M через коммуникационную линию связи стандарта RS - 485.

Функциональное назначение контролера изображено на рисунке.

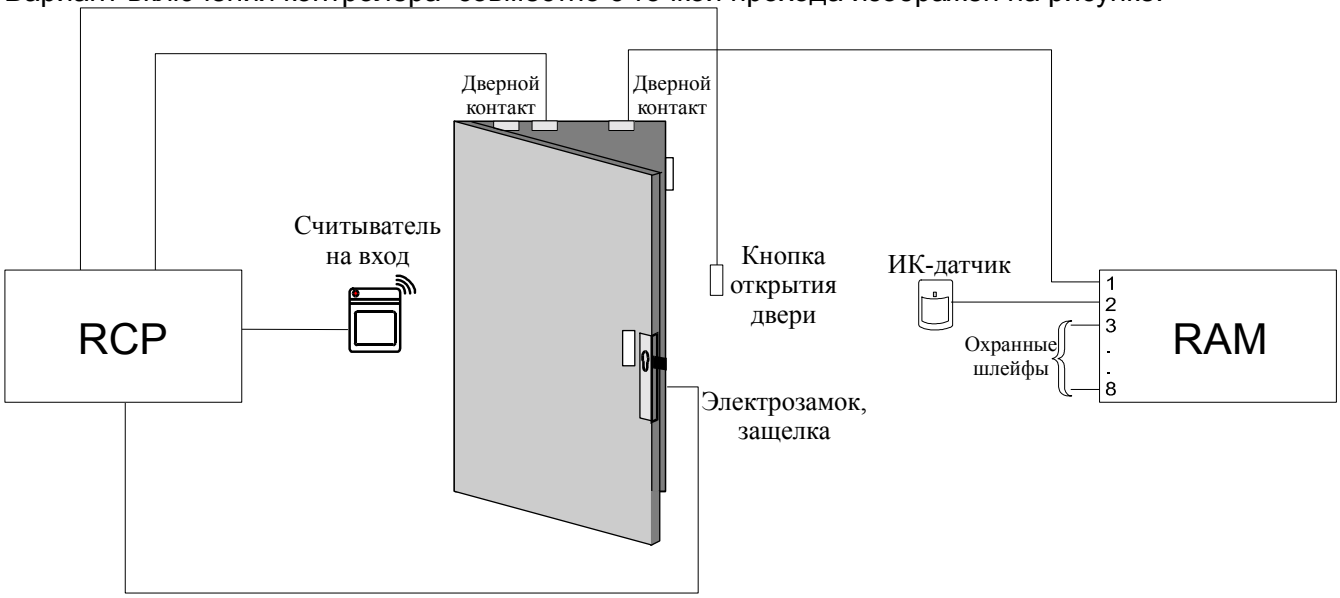


7.5. Функциональное назначение модуля RAM-8

Модуль охранных шлейфов RAM-8 предназначен для расширения количества охранных

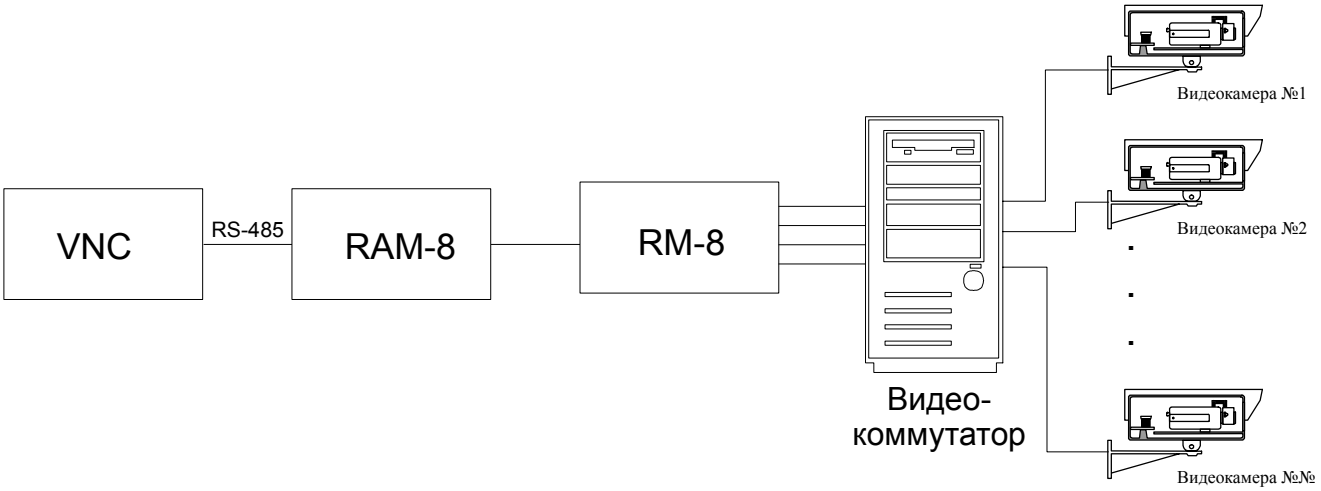
шлейфов и управляемых выходов контролера VNC до 128-ми. Модуль охранных шлейфов RAM-8 контролирует состояние 8-ми охранных шлейфов. Модуль охранных шлейфов RAM-8 подключается к контролеру VNC посредством интерфейса RS-485. Максимально до 16 контроллеров RAM-8 может быть подключено на линию связи RS-485 к одному контролеру VNC .

Вариант включения контролера совместно с точкой прохода изображен на рисунке.



7.6. Функциональное назначение модуля RM-8

Модуль релейных выходов RM-8 предназначен для расширения количества управляемых выходов контролера VNC до 128-ми. Модуль обеспечивает управление 8-ми релейными выходами. Модуль RM-8 подключается к контролеру VNC посредством контроллера RM-8 по интерфейсу RS-485. См. «Руководство пользователя. Модуль RM-8. Модуль RAM-8». Вариант включения изображен на рисунке.



Модуль RAM-8 получает команды от управляющего контроллера VNC на включение соответствующего реле и транслирует эти команды в модуль релейных выходов. К модулю релейных выходов может быть подключен коммутатор видео камер, производящий коммутацию необходимой камеры на экран охранника.

8. Каналы связи

Каналы связи в системе предназначены для организации обмена информацией между различными устройствами в процессе функционирования системы. Физически каналы связи представляют собой кабель, соединяющий модули между собой.

8.1. Протокол связи

В интегрированной системе «Фортеця» применяются два основных типа интерфейса передачи данных:

- RS 485;
- CAN.

Интерфейс RS 485 используется для построения локальной шины управляющего контроллера. Интерфейс CAN используется для объединения управляющих контроллеров в единую сеть.

8.1.1. Интерфейс RS 485

Интерфейс RS 485 представляет собой асинхронную, дифференциальную передачу по витой паре. Логическая обработка интерфейса производится микроконтроллерами устройств.

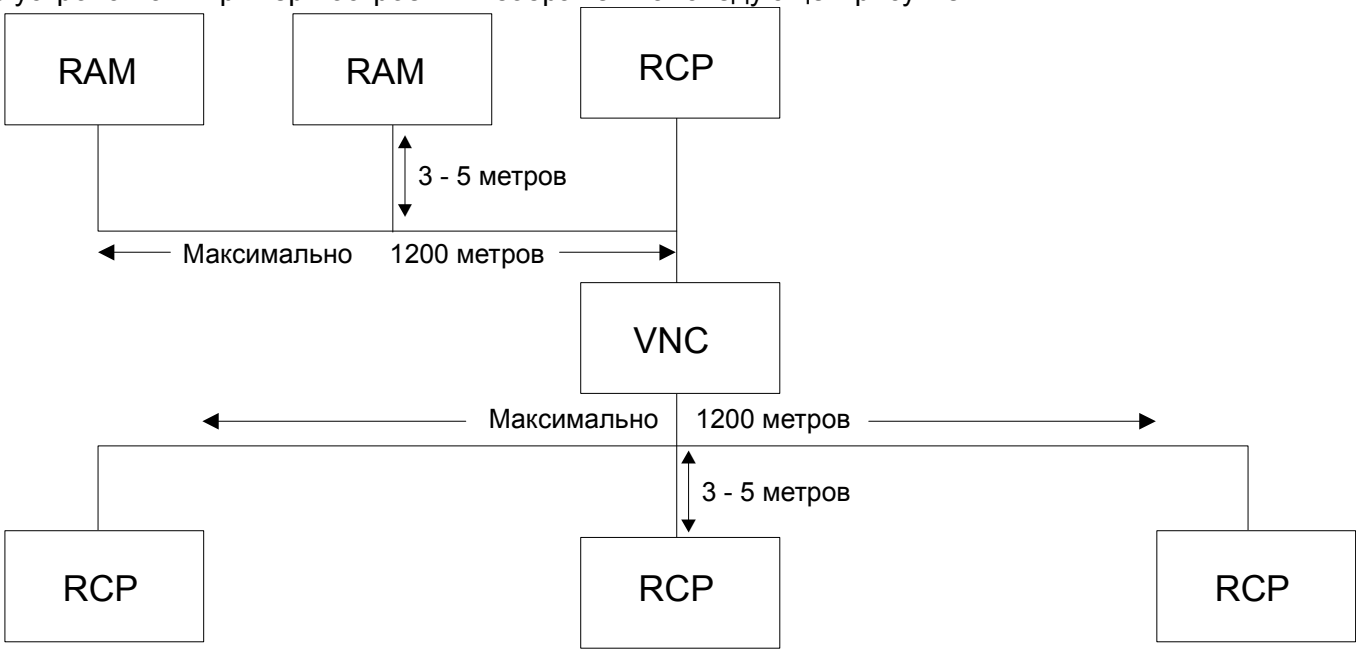
8.1.2. Интерфейс CAN

Интерфейс CAN представляет собой логический протокол, обладающий повышенной устойчивостью и надежностью, практически исключающий ошибки управления. Логическая обработка протокола производится специализированной микросхемой.

Протокол CAN обеспечивает общую вероятность необнаруженной ошибки $4{,}7 \times 10^{-11}$. Это достигается применением специальных методов кодирования информации с применением кодов Хемминга. Физическим уровнем, применяемого протокола CAN, является дифференциальная токовая передача по витой паре.

8.2. Топология сети управляющего контроллера VNC

Структура сети передачи данных управляющего контроллера построена по принципу топологии общей шины (физический уровень сети). Данная топология представляет собой одно или несколько устройств, физически подключенных к одной шине передачи данных. Управляющий контроллер производит отправку сообщений в общую шину. Отправляемое сообщение получают все локальные устройства, подключенные к данному каналу связи. Выбор сообщения конкретным устройством производится на основе информации содержащейся в отправленной передаче – «адрес устройства». Пример построения изображен на следующем рисунке.



По первому каналу связи управляющий контроллер находится в середине общей шины. По второму каналу связи управляющий контроллер находится на конце общей шины.

Ограничение максимальной протяженности общей шины определяется затуханием сигнала в канале связи, и допустим временем получения информации локальным устройством.

Преимущества топологии общей шины:

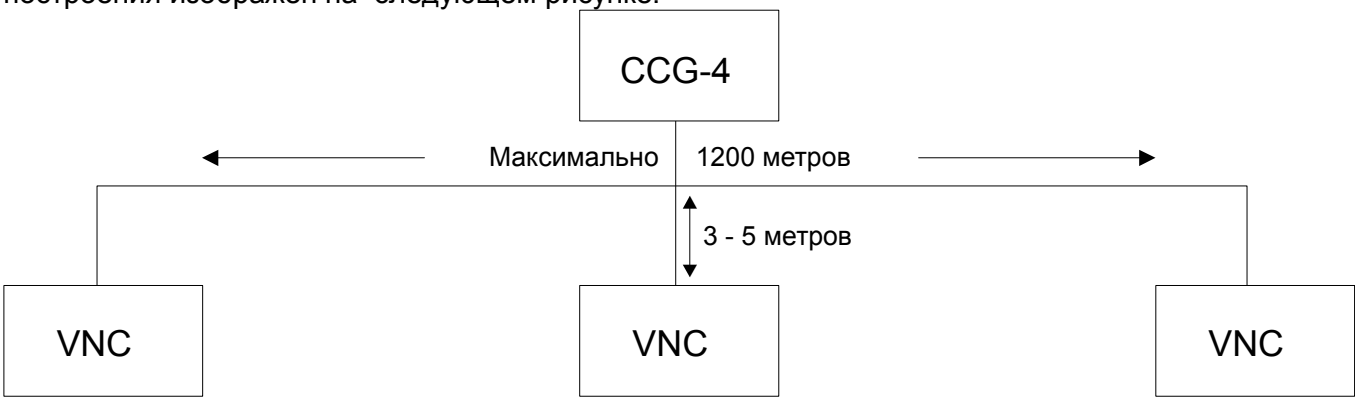
- Наиболее простая схема монтажа;
- Локальные модули подсоединяются только к общей магистрали, поэтому их достаточно просто подключать и удалять из сети.

Недостатки топологии общей шины:

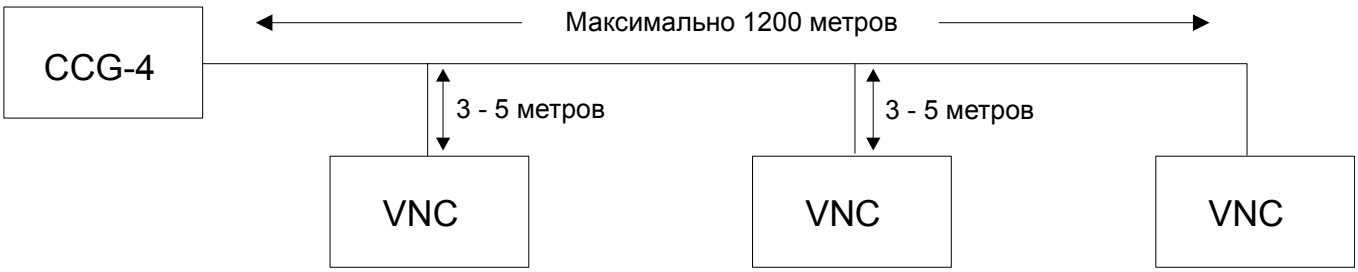
- Возможные затруднения при локализации поврежденного участка сети.

8.3. Топология сети конвертора связи

Структура сети передачи данных конвертора связи построена по принципу топологии общей шины (физический уровень сети). Детальное описание принципа указано в разделе 8.5. Пример построения изображен на следующем рисунке.



Конвертор связи включен в середине общей шины.



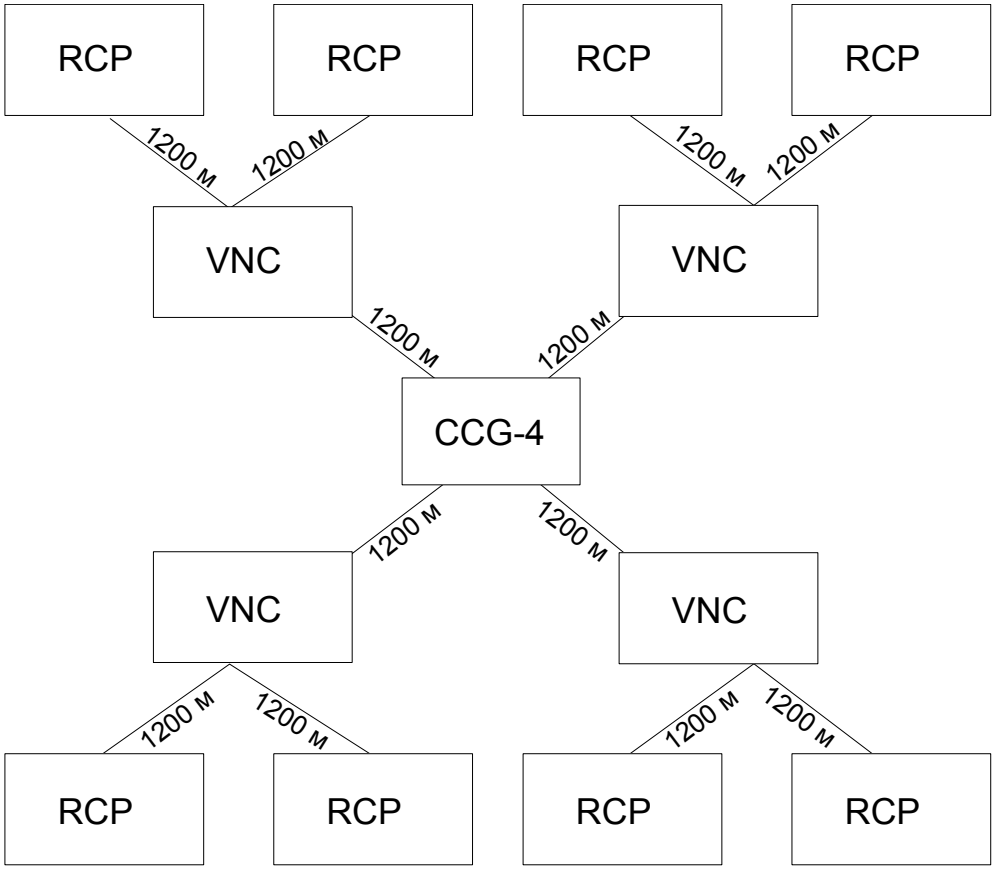
Конвертор связи включен в конце общей шины.

8.4. Топология системы

Общая топология системы имеет смешанный характер, что объясняется использованием лучевой структуры за счет дополнительных каналов CAN конвертора CCG-4 и каналов управляющего контролера VNC. Вариант построения топологии системы изображен на рисунке.

!!! Применение многолучевого принципа позволяет использовать интегрированную систему «Фортеця» на объектах имеющих:

- **большую протяженность;**
- **неравномерный характер размещения структуры;**
- **наличием объектов, имеющих значительное удаление от центра управления.**



8.5. Требования к кабелям связи

Для реализации физического соединения между устройствами в системе «Фортеця» используется кабель с витыми парами.

Кабель с витыми парами состоит из двух перевитых между собой проводников, по которым сигнал распространяется в дифференциальном виде. Передача по проводам двух дифференциальных сигналов позволяет:

- уменьшить влияние внешних электромагнитных помех;
- уменьшить влияние внешних радиочастотных помех;
- скомпенсировать излучение во внешнюю среду от каждого провода.

Два перевитых между собой провода, составляющих одну пару, имеют также пониженный уровень перекрестных наводок, которые могут иметь место между отдельными парами и невысокое ослабление сигнала, вызванное емкостным сопротивлением кабеля.

!!! В системе «Фортеця» допускается применение только кабеля с экранированными витыми парами. Полоса пропускания кабеля должна быть не менее 10 мБит/сек.

!!! КАТЕГОРИЧЕСКИ ЗАПРЕЩАЕТСЯ Использовать неэкранированные кабели с витыми парами.

Рекомендуемая длина для физической линии составляет 4000 футов (1219 метров). Однако допускается увеличивать протяженность физической линии при улучшении параметров кабеля. Перечень параметров кабелей для разных типов скоростей по каналу CAN указан в следующей таблице.

Протяженность линии связи	Рекомендуемое сечение провода для разводки			Рекомендуемая скорость по каналу CAN
0 – 152 м	24AWG	Диаметр 0,51мм	0,22 кв.мм.	125 000 бод

0 – 304 м	24AWG	Диаметр 0,51мм	0,22 кв.мм.	40 000 бод
0 – 800 м	24AWG	Диаметр 0,51мм	0,22 кв.мм.	20 000 бод
0 – 1219 м	24AWG	Диаметр 0,51мм	0,22 кв.мм.	10 000 бод
0 – 608 м	20AWG	Диаметр 0,8мм	0,51 кв.мм.	40 000 бод
0 – 1219 м	20AWG	Диаметр 0,8мм	0,51 кв.мм.	20 000 бод
0 – 1800 м	20AWG	Диаметр 0,8мм	0,51 кв.мм.	10 000 бод

9. Программное обеспечение

9.1. Назначение программного обеспечения

Программное обеспечение (ПО) "Фортеця" предназначено для работы в составе интегрированной системы безопасности «Фортеця». Обеспечивает работу с управляющими контроллерами серий VNC (Versitile Node Controller) и ANC (Access Node Controller).

Задачи ПО "Фортеця":

- обеспечение конфигурирования и управления аппаратуры системы контроля доступа (СКД) при помощи персонального компьютера (ПК);
- ведение базы данных (БД) идентификаторов доступа и их владельцев;
- протоколирование событий системы контроля доступа (СКД);
- обеспечение функций анализа событий системы (выборка из протокола событий по фильтру, учет рабочего времени).

ПО реализовано по архитектуре "Клиент-сервер". В качестве БД используется SQL сервер InterBase. ПО ориентировано на работу в компьютерной сети. Связь между модулями осуществляется через сетевые соединения между компьютерами.

9.2. Требования к аппаратному обеспечению

Для нормального функционирования системы персональный компьютер (ПК) должен удовлетворять следующим требованиям:

- процессор Pentium 200 и выше;
- объем оперативной памяти 64Mb и более;
- операционная система Windows NT 4.0/Windows 2000.

9.3. Состав программного обеспечения

В состав пакета программного обеспечения «Фортеця» входит нескольких рабочих модулей. Каждый модуль сориентирован на выполнение определенных задач. Детальное назначение и описание работы каждого модуля описано в «электронном справочнике», входящем в состав программного обеспечения.

ПО "Фортеця" состоит из следующих модулей:

- Модуль опроса аппаратуры;
- Конфигуратор;
- АРМ "Бюро пропусков";
- АРМ "Охранник";
- Генератор отчетов;
- Учет рабочего времени.

9.3.1. Модуль опроса аппаратуры

Модуль опроса аппаратуры обеспечивает организацию связи сервера системы с управляющими контроллерами, посредством конвертора CCG-4. Модуль обеспечивает постоянный прием данных от системы и накопление их в промежуточном буфере.

9.3.2. Конфигуратор

Конфигуратор позволяет создавать, добавлять и производить изменения в структуре построения системы. Для максимальной наглядности отображаемые данные представлены в виде древовидной графической структуры. Возможность работы с конкретными объектами определяется правами оператора. При вводе данных система автоматически производит контроль правильности и производит «подсказку» оператору.

9.3.3. АРМ «Бюро пропусков»

Модуль «Бюро пропусков» предназначен для организации работы с базой данных пользователей. Модуль позволяет вносить в базу данных сведения о карточках, анкетные данные их владельцев, фотографии пользователя карточки, а также дополнительную информацию о пользователе: сведения о работе (должность, табельный номер, телефон, график работы) и т.д.

Входящий в состав модуля редактор макетов карт, позволяет оператору быстро внести необходимые данные и сформировать готовый макет для печати. Возможность быстрой и оперативной печати позволяет оператору бюро пропусков всего через несколько минут подготовить электронный пропуск с фотографией для нового сотрудника.

Возможность подключения электронного фотоаппарата позволяет быстро получить фотографию нового сотрудника.

9.3.4. Генератор отчетов

Модуль генератора отчетов обеспечивает полную автоматизацию формирования списка сообщений системы для оперативного просмотра, анализа и распечатки данных. Выборку результатов отчета можно организовать по различным критериям, например:

- по дате и времени;
- по фамилии;
- по карточкам – пропускам;
- любой дополнительной информации и т.д.

9.3.5. АРМ «Охранник»

Модуль автоматизированного рабочего места (АРМ) «Охранник» предназначен для организации рабочего места оператора службы безопасности. Все события в системе выводятся на монитор охранника и регистрируются в базе данных. Оператор системы в зависимости от своих полномочий может иметь возможность управления, как отдельными частями системы, так и всей системой в целом.

Вывод событий может осуществляться в графическом виде, например, в виде поэтажных планов с участками охранных зон, на которых произошла «сработка».

Режим фото идентификации позволяет работнику службу безопасности визуально сверить посетителя с его фотографией, хранящейся в базе данных.

9.3.6. Учет рабочего времени

Модуль учета рабочего времени позволяет гибко описывать графики рабочего времени сотрудников предприятия, производить регистрацию времени работы каждого сотрудника (приход\ уход на работу, факты опозданий, переработки, преждевременные уходы и т.д.)

Модуль производит формирование соответствующих отчетов. Наглядное графическое представление отчета по каждому из сотрудников делает восприятие информации максимально простым и оперативным. Для предприятий с круглосуточным режимом работы формирование отчета производится с учетом графика рабочих смен.