ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

С.А. Гречаный
А.В. Сидоров
Д.Ю. Калков

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Практикум

Воронеж
2022

УДК 004.78:681.139.3
ББК 32.965
Г81

Рецензенты:

Р. О. Лисянский – начальник ООВиЭИТСОиБ ФГКУ «УВО ВНГ России по Воронежской области», подполковник полиции;

В. В. Марков – начальник УВО по г. Воронежу – филиала ФГКУ «УВО ВНГ России по Воронежской области», подполковник полиции.

Гречаный С. А.

Г81 Системы контроля и управления доступом : практикум / С. А. Гречаный, А. В. Сидоров, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2022. – 107 с.

ISBN 978-5-88591-927-2

Практикум содержит методические указания по выполнению практических работ по дисциплине «Системы контроля и управления доступом» для курсантов и слушателей радиотехнического факультета.

Издание может быть использовано слушателями факультета профессиональной подготовки и факультета переподготовки и повышения квалификации.

Г35-22(I)-2022 **УДК 004.78:681.139.3**
ББК 32.965

ISBN 978-5-88591-927-2

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные системы контроля и управления доступом (СКУД), как правило, являются неотъемлемыми частями систем безопасности крупных объектов различного функционального назначения.

В общем случае системы контроля и управления доступом являются сложными и многоплановыми электронными системами, которые обеспечивают возможность доступа субъектов в определенные помещения, а также визуальный контроль состояния контролируемого объекта.

Бурное развитие рынка СКУД связано, прежде всего, с повышением качества и надежности систем, снижением их стоимости, расширением круга решаемых задач и функциональных возможностей. На рынке появилось большое количество разнообразных фирм, занимающихся производством и распространением подобных систем.

Будучи электронными информационными системами, СКУД постоянно модернизируются. Растущая вычислительная мощность микропроцессоров, увеличение объема и надежности элементов памяти является основой для обеспечения соответствия возможностей СКУД растущим требованиям заказчиков. Появление мощных микропроцессоров со встроенной программируемой памятью обеспечило возможность дистанционного обновления и развития аппаратной части СКУД без демонтажа ее элементов, что позволяет поддерживать актуальность системы на протяжении всего срока эксплуатации без дополнительных финансовых затрат. С точки зрения производителя, такой подход обеспечивает дополнительные конкурентные преимущества и позволяет развивать систему за счет вывода на рынок нового оборудования и сохранения совместимости со старыми аппаратными версиями.

Среди тенденций развития СКУД следует особо отметить всеобщий интерес к внедрению IP-технологий. Возможность использования локальных вычислительных сетей (ЛВС) для передачи информации в некоторых системах существует уже более 10 лет. Их структура предусматривает использование последовательных интерфейсов RS-485, или аналогичных для объединения линейных контроллеров и специальных шлюзов, или центральных контроллеров для объединения оборудования в единую информационную сеть по каналам Ethernet. Основным отличием оборудования нового поколения является полный отказ от использования последовательных интерфейсов. Практически все ведущие производители вывели на рынок или анонсировали контроллеры доступа с возможностью прямого подключения к сети Ethernet. Новые технологии привносят дополнительные возможности, к которым можно отнести удобство использования оборудования и более низкую стоимость внедрения СКУД на объектах с развитой IT-инфраструктурой. Производители получают возможность организации

прямого обмена информацией между контроллерами и питания устройств от сети Ethernet с применением технологии PoE (Power over Ethernet).

Следует однако отметить, что далеко не везде имеется необходимая оснащенность каналами Ethernet, а приобретение дополнительного оборудования и прокладка соответствующих коммуникаций может оказаться невыгодной, если в местах организации точек доступа не планируется размещение других IP-устройств или компьютеров. Ограниченная нагрузочная способность не позволяет использовать технологию PoE для питания контроллеров и исполнительных устройств суммарной мощностью более 13 Вт, а ее структура усложняет реализацию длительного резервирования электропитания системы и повышает общую стоимость оборудования ЛВС. Вопросы защиты сети от несанкционированного доступа, обеспечения достаточной пропускной способности и правильная организация маршрутизации пакетов данных также требуют внимательного рассмотрения. Учитывая эти моменты, можно предположить, что наиболее востребованными будут универсальные системы, обеспечивающие возможность использования оборудования с классическими и Ethernet интерфейсами как по отдельности, так и в необходимых сочетаниях. Некоторые производители уже имеют в своем арсенале подобные решения, причем в ряде случаев для выбора того или иного типа интерфейса достаточно приобрести соответствующие модули расширения контроллеров СКУД.

Практикум содержит рекомендации по выполнению практических работ по дисциплине «Системы контроля и управления доступом» с использованием оборудования системы безопасности и повышения эффективности PERCo-S-20.

Выполнение практических работ позволит расширить и закрепить полученные теоретические знания, сформировать умения настройки и программирования компонентов системы, а также работы со специализированным программным обеспечением, сформировать компетенции для практической деятельности.

ПРАКТИЧЕСКАЯ РАБОТА № 1

Установка и удаление программного обеспечения системы безопасности и повышения эффективности PERCo-S-20. Настройка базы данных

Цели занятия:

Образовательные: изучение принципов построения многофункциональной системы обеспечения безопасности и повышения эффективности PERCo-S-20; формирование умений установки и удаления программного обеспечения PERCo-S-20, настройки центра управления системы безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекций № 1.1 «Предмет и задачи курса. Основные понятия и определения. Задачи, решаемые с использованием СКУД».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.

Учебные вопросы:

1. Установка и удаление программного обеспечения PERCo-S-20.
2. Настройка серверов и создание базы данных.
3. Управление базой данных.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.

2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Системы контроля и управления доступом: методические рекомендации / С. А. Гречаный, М. С. Романов, М. В. Таравков, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2021. – 78 с. – Текст : непосредственный.

Краткие теоретические сведения

PERCo-S-20 – это многофункциональная система для обеспечения безопасности и повышения эффективности работы промышленных предприятий, банков, бизнес-центров, медицинских, образовательных, государственных учреждений и организаций других сфер деятельности.

Структурный состав системы PERCo-S-20 показан на рис. 1.1. Все технические средства и ПО системы PERCo-S-20 работают в единой информационной среде передачи данных, реализованной на основе сети Ethernet. Структурно систему можно разделить на две составляющие – оперативного управления и наблюдения и управленческой части.

К первой части можно отнести контроллеры, пожарную сигнализацию, системы видеонаблюдения, АРМы службы безопасности и мониторинга. Ко второй – АРМы, не требующие оперативного контроля.

Для управления СКУД PERCo-S-20 используется специализированное программное обеспечения компании Perco. Для подготовки пользователя к работе с данным программным обеспечением, подготовлено мето-

дическое указание, которое представляет собой описание данного программного обеспечения и руководство по управлению функциями данной СКУД.

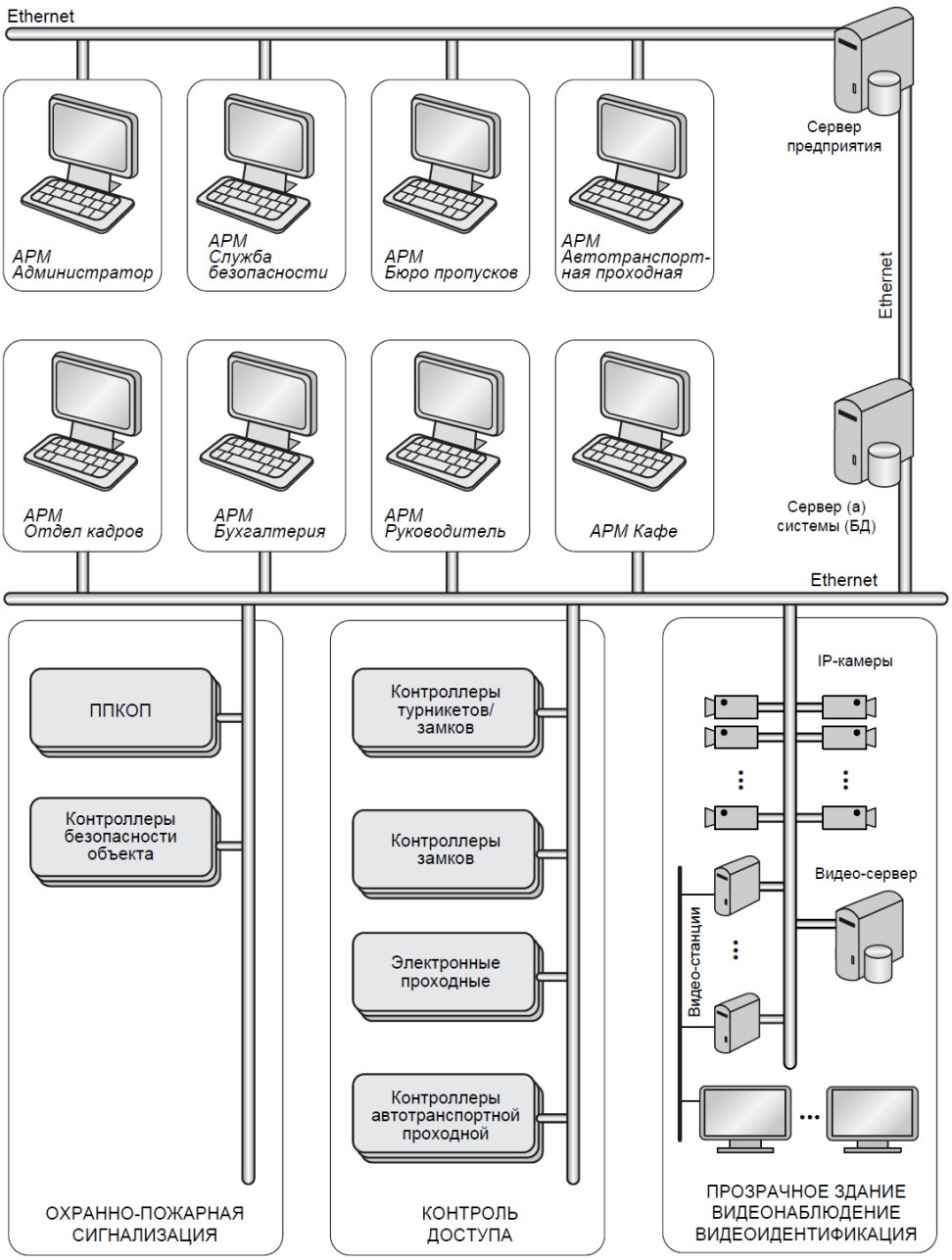


Рис. 1.1. Структурный состав системы PERCo-S-20

Для работы с системой PERCo-S-20 существуют две программы – «Центр управления PERCo-S-20» и «Консоль управления PERCo-S-20».

Данное ПО позволяет выполнять следующие задачи:

– программировать расписания и временные параметры контроллера;
– вести список идентификаторов с именами пользователей;
– программировать права доступа пользователей;

– производить мониторинг в реальном времени текущих событий контроллера;

– сохранять все события на контроллере на жестком диске с возможностью последующих действий с ними;

– создавать графики работы;

– формировать отчеты.

Подсистема *СКУД PERCo-S-20* с элементами охранной сигнализации предназначена для организации контроля и управления доступом сотрудников, посетителей и ТС на территорию и в помещения предприятия.

Доступ может осуществляться по пропускам на основе бесконтактных карт через специально оборудованные точки прохода. Каждая карта обладает уникальной информацией – *идентификатором.* В БД системы идентификатор связан с данными сотрудника, посетителя или ТС, которому она выдана. В качестве идентификатора в системе также могут выступать и биометрические признаки человека, в частности, в системе *PERCo-S-20* предусмотрена интеграция с биометрическими контроллерами *Suprema,* которые осуществляют биоидентификацию по отпечаткам пальцев.

Контроллеры всех точек прохода связаны по сети Ethernet между собой и с единой БД системы. Каждое событие предъявления идентификатора фиксируется в БД с указанием места и времени предъявления. Это позволяет отслеживать время пребывания и перемещения пользователей по территории и в помещениях предприятия.

Для каждого контролируемого направления через исполнительные устройства точек прохода может быть установлен один из режимов контроля доступа (РКД): *«Открыто», «Закрыто», «Контроль».* Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. РКД *«Контроль»* используется для прохода по идентификаторам.

Для точек прохода типа «дверь» доступна возможность конфигурирования ОЗ. В зависимости от модели контроллера в ОЗ может входить ИУ и ШС. Эту ОЗ можно перевести в режим *«ОХРАНА»* и снять с охраны при помощи идентификатора – бесконтактной карты доступа, которой выдан соответствующий тип прав, или оператором через ПО. При постановке на охрану для считывателей точки прохода устанавливается РКД *«Охрана».* Поддержка ШС позволяет контролировать не только вход в помещение, но также и весь его объем.

В состав каждого рабочего места входит следующее оборудование системы PERCo-S-20:

1. Прибор приемно-контрольный охранно-пожарный PU01.
2. Блок управления и индикацией AU02.
3. Контроллер замка CL05.
4. Контроллер замка CL201.

5. Контроллер турникета / замка CT/L04.
6. Считыватель IR03.
7. Считыватель IR04.
8. Пожарный извещатель.

Базу данных (БД) можно определить как унифицированную совокупность данных, совместно используемую различными задачами в рамках некоторой единой автоматизированной информационной системы.

Процедуры хранения данных в базе должны подчиняться некоторым общим принципам, среди которых в первую очередь следует выделить:

1) целостность и непротиворечивость данных, под которыми понимается как физическая сохранность данных, так и предотвращение неверного использования данных, поддержка допустимых сочетаний их значений, защита от структурных искажений и несанкционированного доступа;

2) минимальную избыточность данных, которая обозначает, что любой элемент данных должен храниться в базе в единственном виде, что позволяет избежать необходимости дублирования операций, производимых с ним.

Программное обеспечение, осуществляющее операции над базами данных, получило название СУБД – система управления базами данных.

Набор принципов, определяющих организацию логической структуры хранения данных в базе, получил название модели данных. Модели баз данных определяются тремя компонентами: допустимой организацией данных; ограничениями целостности; множеством допустимых операций.

В теории систем управления базами данных выделяют модели четырех основных типов: иерархическую, сетевую, реляционную и объектно-реляционную.

Терминологической основой для иерархической и сетевой моделей являются понятия: атрибут, агрегат и запись. Под атрибутом понимается наименьшая поименованная структурная единица данных. Поименованное множество атрибутов может образовывать агрегат данных. В некоторых случаях отдельно взятый агрегат может состоять из множества экземпляров однотипных данных, или являться множественным элементом. Записью называют составной агрегат, который не входит в состав других агрегатов.

Методические указания по отработке учебных вопросов

1. Установка и удаление программного обеспечения PERCo-S-20

Перед началом инсталляции программного обеспечения ознакомьтесь с разработанной структурной схемой системы безопасности.

1.1. Запустите системный блок персонального компьютера.

1.2. Для корректной установки ПО запустите программу «RegCleaner» и процедуру очистки: Tools/Registry Cleanup/Do them All.

1.3. Установите Базовое ПО. Для этого запустите инсталляционный модуль SetupBase.exe, расположение которого укажет преподаватель. Следуйте указаниям мастера установки.

Внимательно ознакомьтесь с прилагаемой информацией и лицензионным соглашением. После принятия лицензионного соглашения будет предложено выбрать устанавливаемые компоненты программного обеспечения, окно выбора которых показано на рис. 1.2.

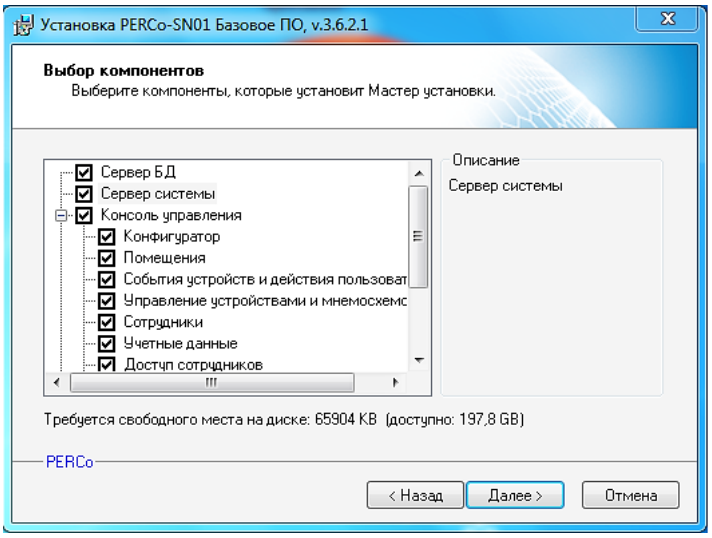


Рис. 1.2. Окно выбора устанавливаемых компонентов для Базового ПО

В составе системы безопасности сервер системы может быть установлен только в единственном экземпляре. Однако, в данном случае, каждое рабочее место представляет отдельную систему. Установка сервера системы автоматически приводит к установке сервера управления базой данных Firebird 2.0. Следуйте указаниям мастера установки. После завершения установки программное обеспечение готово к работе.

1.4. Установите расширенное ПО. Для этого запустите инсталляционный модуль SetupExtend.exe, расположение которого укажет преподаватель. Следуйте указаниям мастера установки.

Внимательно ознакомьтесь с прилагаемой информацией и лицензионным соглашением. После принятия лицензионного соглашения будет предложено выбрать устанавливаемые компоненты программного обеспечения, окно выбора которых показано на рис. 1.3.

Выбрать все компоненты программного обеспечения, за исключением модуля интеграции с 1С.

После завершения установки программное обеспечение готово к работе. Изменяя или обновляя состав задействованных системных модулей, установить сначала базовое программное обеспечение, если его компоненты используются, а затем расширенное. После удаления расширенной версии следует переустановить базовую.

1.5. Для удаления компонентов программного обеспечения необходимо запустить инсталляционный модуль «SetupExtend.exe» (рис. 1.4) и следовать указаниям мастера установки.

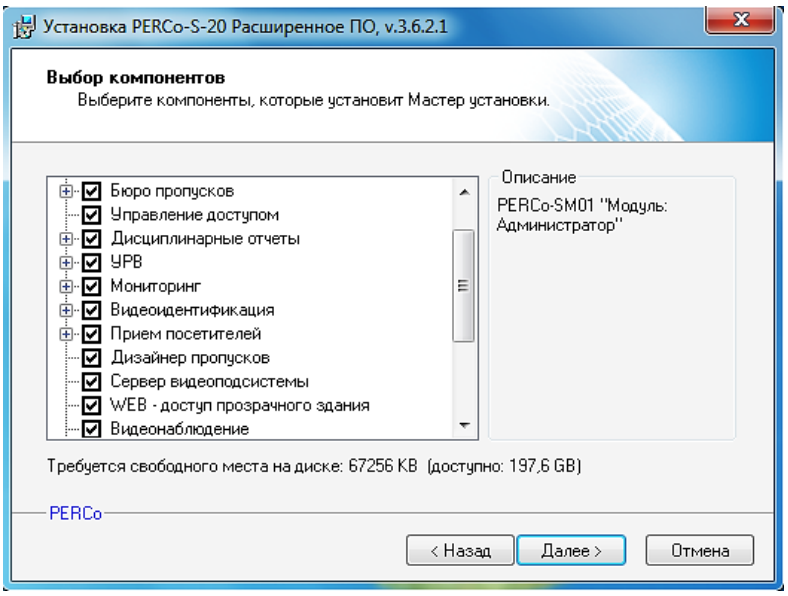


Рис. 1.3. Окно выбора устанавливаемых компонентов для Расширенного ПО

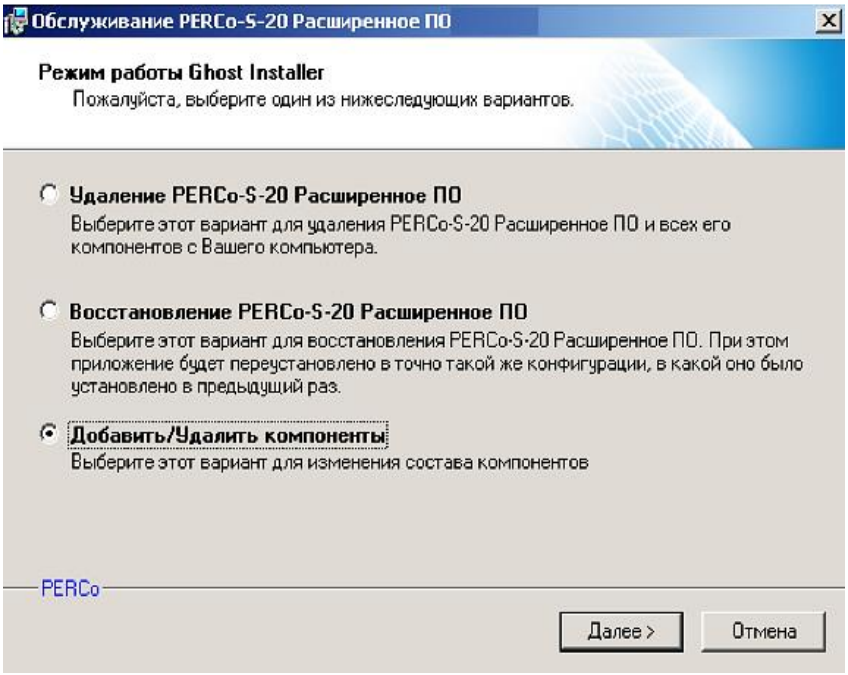


Рис. 1.4. Окно удаления компонентов ПО

2. Настройка серверов и создание базы данных

2.1. Запустите центр управления системы безопасности PERCo-S-20, кликнув по соответствующей иконке на рабочем столе.

В разделе «Настройка серверов» можно остановить или запустить

Firebird SQL сервер управления данных и сервер системы PERCo-S-20 (рис.1.5). Оба сервера должны быть запущены.

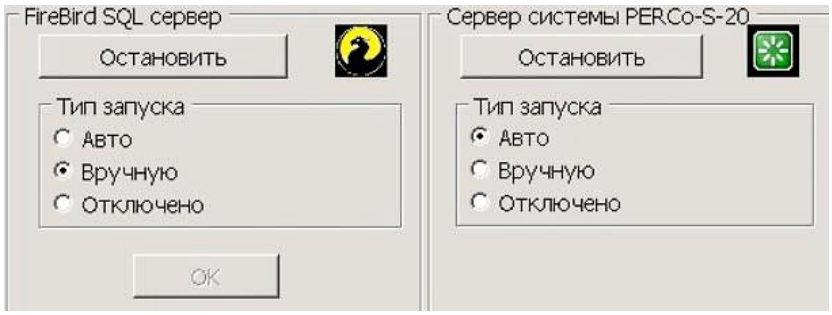


Рис. 1.5. Окно раздела настроек сервера

2.2. Перейдите в раздел «Создание и управление БД». При возникновении уведомления, представленного на рис. 1.6, система информирует, что БД отсутствует, или нужно указать к ней путь.

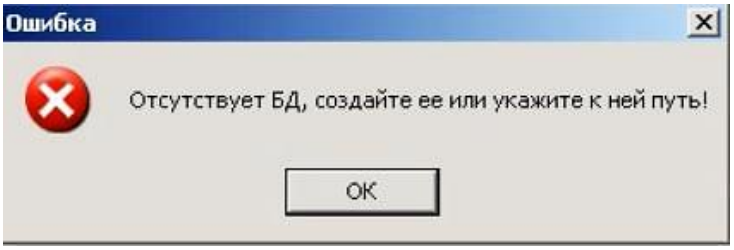


Рис. 1.6. Уведомление об ошибке

Для того чтобы создать БД, в нижнем правом углу выбрать режим «Создание базы данных». На рис. 1.7 представлено окно данного раздела.

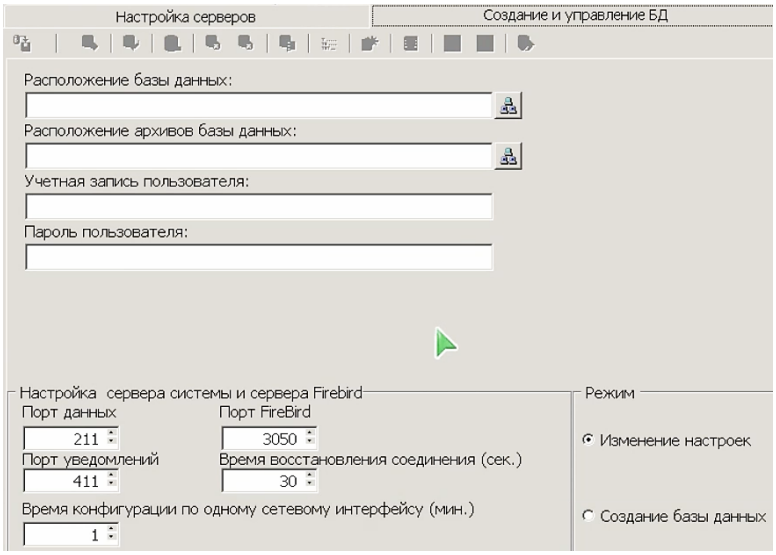


Рис. 1.7. Окно раздела создания и управления БД

После этого автоматически заполняются поля «Расположение базы данных», «Расположение архивов базы данных», «Учетная запись пользователя», «Пароль пользователя» и «Пароль администратора БД».

Перед созданием базы данных имеется возможность выбрать место ее расположения и расположения архивов. Создание базы данных осуществляется нажатием соответствующей иконки панели инструментов (рис. 1.8).

2.3. Законспектируйте в рабочих тетрадях назначение иконок панели инструментов.

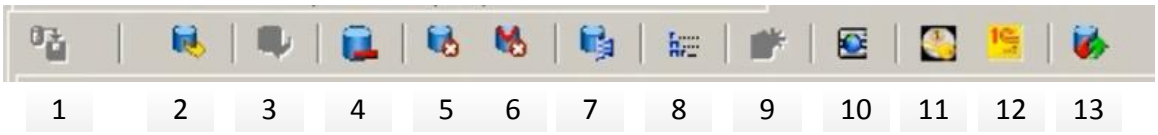


Рис. 1.8. Иконки панели инструментов

Назначение пиктограмм панели инструментов

1. «Сохранение настроек базы данных». Данная иконка нажимается при изменении расположения базы данных, расположения архивов базы данных, учетной записи пользователя или пароля.

2. «Сохранение базы данных, оптимизация и проверка целостности». Предназначена для создания архива БД в ту папку, которая была указана при создании базы.

3. «Восстановление БД». Для восстановления БД из созданного архива.

4. «Удаление данных мониторинга».

5. «Удаление данных по событиям».

6. «Удаление данных по видеоидентификации». Эти иконки (4-6) отвечают за очистку БД от устаревших событий. По нажатию на иконку система спрашивает, за какой период предполагается удаление данных. Необходимо выбрать период, за который удалить события, и нажать «Ок».

7. «Настройки сервера БД». Для входа в раздел «Настройки БД» необходимо ввести пароль администратора БД-«masterkey», и нажать «Ок». После этого отображаются окно настройки сервера БД и окно пользователей, которые созданы в БД. По умолчанию в программе две учетные записи: SYSDBA- встроенная административная учетная запись FireBird и SCD17_USER – запись пользователя PERCo-S-20.

8. «Оптимизация индексов». В случае существенного увеличения данных в БД можно перенумеровать все строки для более быстрого формирования отчетов.

9. «Создание базы данных». Необходима для создания БД на первоначальном этапе работы.

10. «Обновление версии базы данных». Необходима для обновления

версии БД при обновлении версии ПО. В случае необходимости обновления подключить БД, выбрать файл UpdatestructureDB.dll, который находится в каталоге «program files/PERCo/PERCo-S-20» и нажать «Открыть». После этого приступить к обновлению. Версия БД и текущая версия программы должны быть одинаковы. Файл UpdatestructureDB.dll входит в дистрибутив Базового ПО и обновляется каждый раз при переустановке программы.

11. «Восстановление предыдущего пароля устройств». В случае если на контроллеры установлен пароль доступа, а в БД он отсутствует, то существует возможность добавить данный пароль в БД.

12. «Настройка работы с 1С». В соответствующей вкладке имеется две функции: «Провести подготовку БД к совместной работе с 1С (удаление всех данных о сотрудниках)» – проведение синхронизации БД 1С и БД PERCo-S-20; «Провести подготовку к обрыву связей с 1С» – восстановление заблокированной функции ввода сотрудников, графиков работ, подразделений в PERCo-S-20.

13. «Проверка целостности БД». С определенной периодичностью один, два раза в месяц необходимо проверять БД на ошибки и целостность. В случае наличия небольших ошибок система автоматически их исправит, в случае существенных нарушений программа сообщит телефон и электронную почту службы технической поддержки компании PERCo.

3. Управление базой данных

3.1. Перейдите в раздел «Резервное копирование БД».

В данном разделе можно запланировать автоматическое резервное копирование БД на любой из дней недели. Изображение окна данного раздела представлено на рис. 1.9.

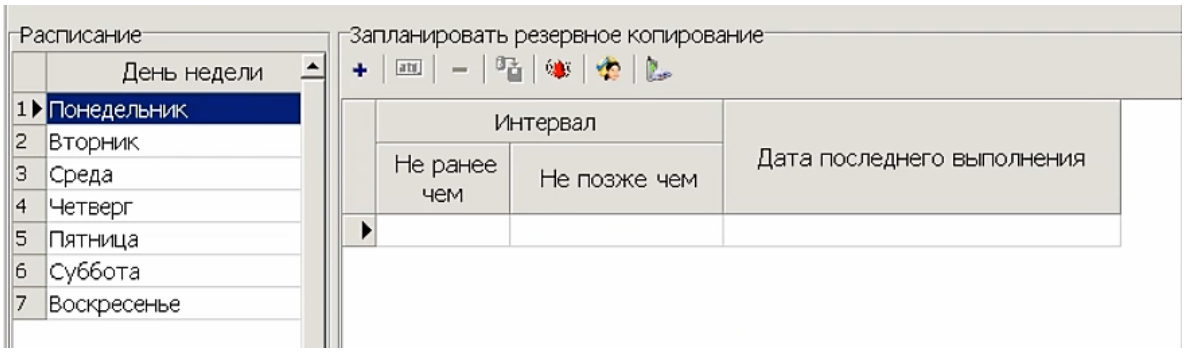


Рис. 1.9. Окно раздела резервного копирования БД

3.2. На все дни недели запланируйте резервное копирование БД. Для этого выбрать день недели, нажать иконку «Добавление», ввести интервал времени, когда будет происходить сохранение БД, нажать «Ок», и иконку «Сохранить расписание».

Система позволяет настроить сетевую, почтовую или СМС рассылки сообщений об успешно или не успешно выполненном сохранении БД.

3.3. Перейдите в раздел «Управление лицензиями». В данном разделе активируются те модули ПО, которые были приобретены согласно лицензионному соглашению. Изображение окна данного раздела представлено на рис. 1.10.

Для активации модулей ПО необходимо выбрать контроллер, к которому привязана лицензия. Привязка лицензии осуществляется по MAC адресу контроллера.

3.4. Для активации модулей ПО необходимо подключиться к существующей БД, в которой уже сконфигурировано требуемое устройство. Для этого следует перейти в раздел «Создание и управление БД». Далее необходимо выбрать путь к нужной БД и нажать иконку «Сохранение настроек базы данных». После этого перейти в раздел «Управление лицензиями» и произвести следующие действия:

– выбрать иконку «Выбор контроллера, содержащего лицензию»;

– выбрать тот контроллер, который прописан в лицензионном соглашении, и нажать «ОК»;

– выбрать модуль ПО, который предполагается активировать, и нажать иконку «Изменить лицензию»;

– в поле «Лицензия» ввести значение, которое получено в лицензионном соглашении, и нажать «ОК».

Также раздел дает возможность посмотреть, какие разделы содержатся в каждом модуле ПО.

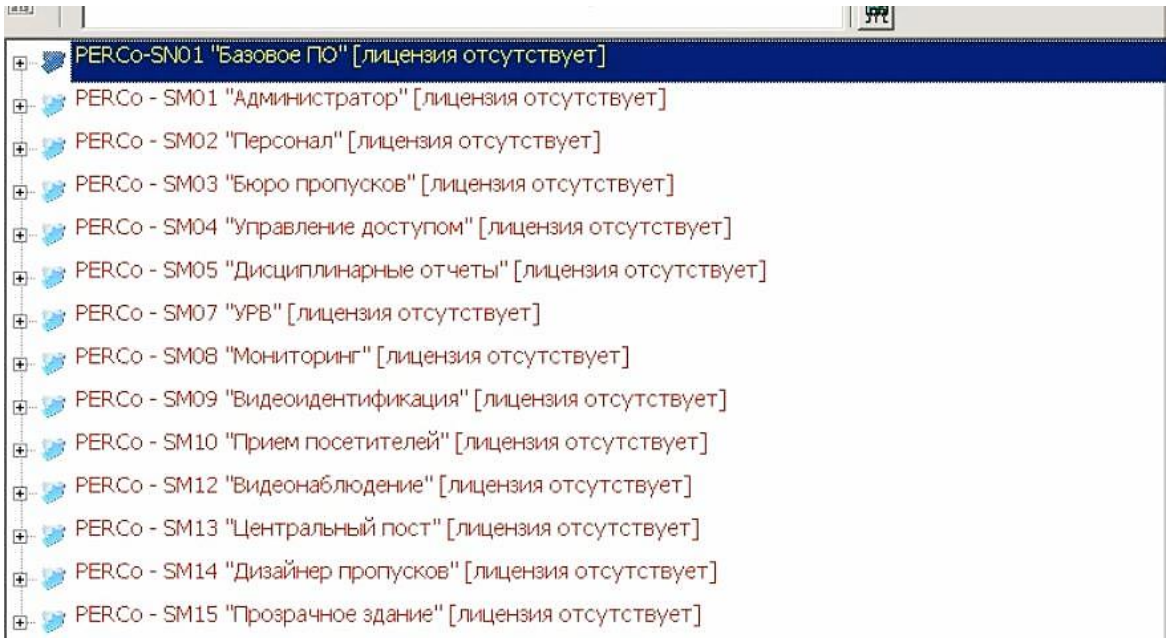


Рис. 1.10. Окно раздела управления лицензиями

3.5. Перейдите в раздел «Настройка USB-модема». При необходимости использования функционала SMS-информирования необходимо подключить USB 3G-модем. Список рекомендуемых модемов находится на сайте perco.ru в разделе «Программное обеспечение».

Для подключения модема необходимо выбрать тот модем, который будет использоваться из списка модемов. Далее вводится телефонный номер, и соответствующий PIN-код. В получателе SMS необходимо ввести телефонный номер администратора системы, который будет получать SMS об успешно или неуспешно выполненном сохранении БД.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Центр управления системы безопасности PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Поясните назначение центра управления системы безопасности PERCo-S-20.
2. Какие разделы включает центр управления системы безопасности PERCo-S-20?
3. Какие задачи решаются с использованием раздела «Создание и управление БД»?
4. Что необходимо для активации модулей ПО?
5. На какие составляющие можно структурно разделить систему?
6. Поясните состав АРМ системы.
7. Какие программы используются для работы с системой?
8. Какие задачи позволяет выполнять ПО?
9. Раскройте состав и виды топологий баз данных.
10. Что представляет собой аппаратный ключ в СКУД PERCo?

Задания для самостоятельной работы

1. Посетите официальный сайт компании PERCo и ознакомьтесь с разделами «Решения», «Новости» и «Каталог».
2. Изучите и законспектируйте в рабочей тетради теоретические сведения о ERP-системах.

ПРАКТИЧЕСКАЯ РАБОТА № 2

Конфигурирование контроллеров и видеокамер
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений конфигурирования контроллеров и видеокамер в системе безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации слушателям по проведению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекции по теме 1.2 «Классификация и тактика применения систем контроля и управления доступом».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Получить у преподавателя адреса контроллеров и коды активации модулей ПО.

Учебные вопросы:

1. Осуществление предварительной настройки оборудования.
2. Конфигурирование контроллеров и видеокамер.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.
2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

В составе любой системы контроля и управления доступом присутствует обязательное техническое устройство, называемое контроллером. Контроллеры – технические приборы, которые осуществляют прием сигналов от считывателей идентификаторов, обработку полученной информации, принятие решение о разрешении/отказе в доступе в контролируемую зону носителя идентификатора и управление исполнительными элементами преграждающих устройств. Именно контроллеры разрешают или запрещают проход через точки доступа. Контроллеры различаются емкостью базы данных, буфера событий, обслуживаемых устройств идентификации.

Любой контроллер СКУД состоит из четырех основных частей:блок обработки сигналов, буфер событий, база данных, блок принятия решения (рис. 2.1).

Считыватель карт (устройство идентификации) передает полученную информацию в блок обработки сигналов. Далее эта информация в цифровом виде передается в блок принятия решения, который в свою очередь заносит факт попытки прохода в схему буфера событий и одновременно формирует запрос в базу данных на предмет правомочности прохода в зону контроля владельца идентификатора и в случае положительного

ответа приводит в действие исполнительное устройство. В этот момент ограничение на доступ в зону контроля уже снято, но система ещё не завершила обработку информации: сам факт прохода именно этого предъявителя идентификатора заносится в буфер событий.

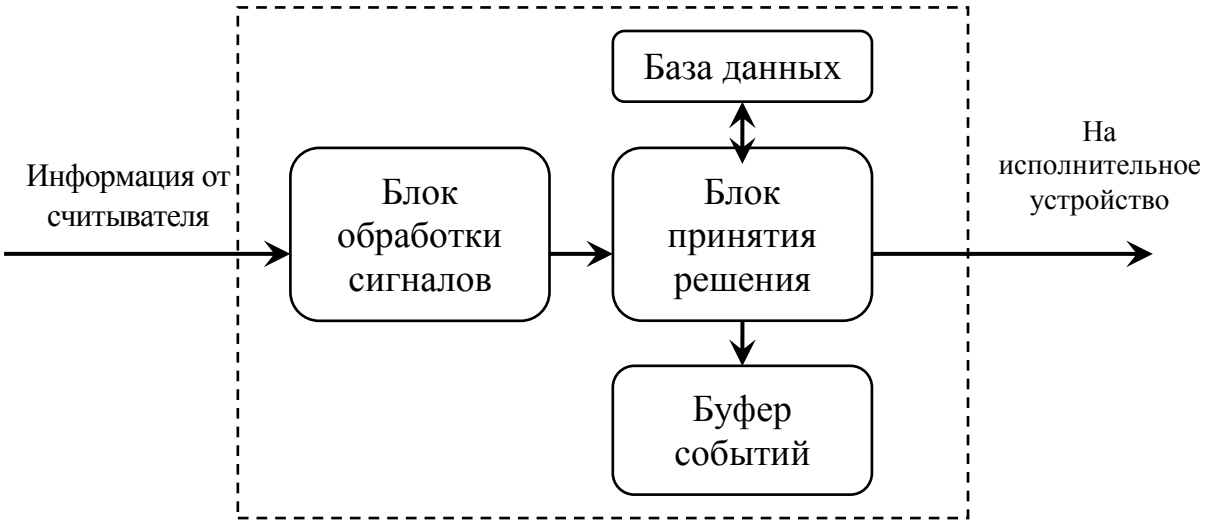


Рис. 2.1. Структурная схема контроллера СКУД

По способу управления (возможности объединения) контроллеры СКУД делятся на три класса: автономные (локальные), сетевые (централизованные) и универсальные (комбинированные).

Независимо от типа применяемых считывателей контроллеры должны поддерживать следующие режимы доступа:

- по одной карте и/или PIN-коду;
- доступ с подтверждением оператором;
- контроль количества людей в помещении (минимум и максимум).

Последнее важно в ситуациях, когда, например, по условиям службы в заданном помещении не должно оставаться менее или более определенного количества человек.

Автономные СКУД.

Автономными СКУД, обычно оборудуются квартиры, коттеджи, небольшие офисы, магазины, аптеки, гостиницы и т. п. и мало значимые зоны на важных объектах.

Данные СКУД это небольшие и недорогие системы, обслуживающие, как правило, до 8 устройств заграждения (дверей, ворот, турникетов и т. п.).

На рис. 2.2 приведена структурная схема варианта автономной СКУД в помещении с одной дверью.

В системе можно устанавливать так называемый офисный режим. Его смысл состоит в том, что пользователь открывает закрытый замок с

помощью идентификатора и проходит в помещение. Далее снаружи открывать замок можно свободно, простым нажатием ручки. Этот режим устанавливается по желанию пользователя, например, для того чтобы каждый раз не подходить к двери (не нажимать кнопку автоматического открывания двери) и открывать ее изнутри, когда стучатся посетители.

Программирование системы осуществляется с помощью мастер-карточки и клавиатуры. Данный состав СКУД может варьироваться в широких пределах и в минимуме состоять из одного конструктивно законченного блока (в виде замка), в котором размещены считыватель, контроллер, исполнительное устройство (запор, ригель, задвижка и т. п.), индикаторы режимов работы. При этом СКУД работает в режиме обычного замка, т. е. при совпадении кодов идентификатора и считывателя запорный механизм срабатывает и разблокирует дверь, разрешая через нее проход.

Рис. 2.2. Структурная схема варианта автономной СКУД в помещении с одной дверью

В процессе расширения системы дополнительно может устанавливаться еще один считыватель для контроля прохода в обратную сторону (или организации многоуровневого контроля доступа), выносные световые/звуковые оповещатели, устройства автоматического открывания/закрывания двери и т. д.

На рис. 2.3 приведен вариант оборудования СКУД, работающей в автономном режиме объекта с несколькими дверями.

Данный вариант построения системы отличается от предыдущего только лишь расширением функций и объемом памяти управляющего контроллера, а также его конструкцией. Считыватели и исполнительные устройства размещены в разных конструктивных блоках и управление ими осуществляется через общий контроллер.

В систему могут быть введены дополнительные функции: контроль прохода в двух направлениях; автоматическое открытие и закрытие дверей

при аварийных и тревожных ситуациях; передача тревожных сообщений на пост охраны; регистрация происходящих событий с помощью принтера, подключаемого к контроллеру.

Программирование системы осуществляется как с помощью мастер-карточки и клавиатуры, так и с помощью переносного компьютера. В своем законченном виде данную систему можно легко включить в СКУД, работающую в сетевом режиме. Для этого необходимо использовать контроллер, позволяющий работать в сетевом режиме с другими контроллерами или использовать дополнительный модуль связи, обеспечивающий объединение контроллеров посредством интерфейса.

Рис. 2.3. Структурная схема варианта автономной СКУД с несколькими дверями

Сетевые СКУД.

Сетевые СКУД предназначены для оборудования крупных объектов таких как банки, крупные учреждения и офисные здания. Несомненным достоинством этих систем является возможность практически не ограниченного расширения.

Такие системы позволяют обслуживать десятки тысяч пользователей. Эффективность работы сетевых СКУД обусловлена возможностью создавать разветвленные, достаточно многочисленные соединения контроллеров и управляющих компьютеров в единую систему.

Модульность построения данных систем обеспечивает: гибкость конфигурации; простоту монтажа, технического обслуживания и ремонта; возможность расширения системы; ценовую эффективность; легкость со-

пряжения с устройствами сервисной автоматики (управление лифтом, освещением, системами кондиционирования и т. д.).

Соединение контроллеров между собой и подключение контроллера к различным периферийным устройствам, входящим в состав системы обеспечивается при помощи различных модулей. К одному контроллеру может быть подключено до 8 считывателей различного типа, например, считыватель магнитных карточек, считыватель бесконтактных карточек, клавиатура (кодонаборное устройство) и др. Подключение считывателей осуществляется через соответствующий считывающий модуль, работающий с двумя считывающими устройствами. Помимо считывателей он также контролирует датчики состояния дверей и кнопки их открывания, другие вспомогательные устройства.

Информация о состоянии иных внешних устройств поступает в контроллер через модуль входа/выхода. Посредством этого же модуля контроллер управляет работой исполнительных устройств, устройством выдачи тревожных извещений. Модуль связи обеспечивает объединение контроллеров в единую систему, протяженностью до 1 км с помощью интерфейса RS-485, а также при необходимости объединение контроллеров и управляющего компьютера в компьютеризированную систему с помощью интерфейса RS-232. Модуль приемо-передачи управляет работой считывателей бесконтактных карточек (Proximity). Один контроллер может обслуживать до 10 000 пользователей. Для увеличения числа пользователей может применяться модуль расширения памяти. При создании компьютерной сети контроллеры в количестве до 32 единиц могут быть объединены в одну ветвь. В этом случае модуль связи включается в первый по порядку контроллер ветви. Через него осуществляется связь этого контроллера с компьютером по интерфейсу RS-232. Обмен информацией между контроллерами производит по интерфейсу RS-485. Кроме того, модуль связи осуществляет преобразование формата и скорости передачи данных RS-232/RS-485. Каждый контроллер в ветви имеет свой адрес. Дальнейшее наращивание системы возможно путем организации нескольких (до 10) ветвей контроллеров. Модуль связи первого контроллера преобразовывает с одной стороны поток данных, посылаемых с управляющего компьютера на контроллер, а с другой поток выходных данных, параллельно подаваемых на адресные модули связи в ветвях. Каждый адресный модуль связи обменивается данными с контроллерами в ветвях и модулями связи.

Такая расширенная сеть позволяет обслуживать до 320 контроллеров и 2 048 контролируемых точек. При необходимости ветвь контроллеров может быть увеличена еще на 1 км. Для этого удлиняемая ветвь подключается к первому контроллеру новой ветви через модуль связи. Для связи между контроллерами по-прежнему используется интерфейс RS-485.

Наличие описанных модулей многофункционального контроллера создает большие возможности по управлению разнообразной периферией

системы. В качестве контролируемых точек могут выступать замкнутые/разомкнутые контакты кнопок, реле, выходные контакты различных объемных или поверхностных извещателей. В качестве исполнительных устройств могут использоваться электрозамки дверей, исполнительные устройства шлагбаумов, турникетов, устройства тревожного оповещения и освещения, телевизионные камеры и т. д. Логическое устройство (процессор) контроллера позволяет производить необходимую установку параметров доступа в каждой контрольной точке при помощи программного обеспечения, то есть конфигурировать систему. Системный оператор может задавать параметры (замкнутое/разомкнутое состояние контактов реле или кнопок, состояние и режим работы счетчиков, состояние флатовых регистров, временные интервалы регистраторов событий и т. д.) прямо с клавиатуры компьютера. Это дает возможность реализовывать различные варианты организации контроля и управления доступом, гибко меняя их в соответствии с текущими требованиями. Программа предоставляет большие сервисные возможности оператору, выводя разнообразную информацию на экран. Например, на дисплее компьютера можно иметь план одного или нескольких помещений с обозначенными на нем контролируемыми точками, индикацию несанкционированных проникновении.

Подсистема видеонаблюдения построена на основе использования IP видеокамер и IP видеосерверов с подключенными к ним аналоговыми видеокамерами. Подсистема видеонаблюдения разработана для использования в составе системы безопасности и повышения эффективности PERCo-S-20 и предназначена для регистрации видеоинформации в тревожных ситуациях и организации рабочих мест сотрудников безопасности по контролю за состоянием охраняемого объекта.

Подсистема видеонаблюдения дает возможность контроля зон детекции движения по каждой камере, позволяет управлять системой по событиям системы безопасности, управлять и конфигурировать до 1000 IP видеокамер и IP видеосерверов.

Методические указания по отработке учебных вопросов

1. Осуществление предварительной настройки оборудования

1.1. Проверьте сетевые настройки компьютера.

Войдите во вкладку «Подключение по локальной сети – свойства» и нажмите «Свойства». Необходимо выбрать протокол интернета версии 4 (TCP/IPv4) и нажать «Свойства».

Для работы с системой PERCo-S-20 компьютер и контроллеры должны находиться в одной подсети 10.0.0.0 с маской подсети 255.0.0.0. Контроллеры серии S-20 по умолчанию имеют IP-адреса, которые начинаются с цифры 10. Таким образом, необходимо ввести вручную IP- адрес из подсети 10.0.10.X, где X – номер рабочего стенда.

1.2. Изучите и законспектируйте теоретические сведения.

Существует три способа задания IP-адреса контроллера CT/L04, которые определяются положением перемычки на разъеме XP1 на плате контроллера, изображение фрагмента которой представлено на рис. 2.4.

Выбор способа задания IP-адреса контроллера осуществляется установкой или снятием перемычки на разъем XP1 на плате контроллера. Возможны следующие способы задания IP-адреса:

– перемычка снята. Если IP-адрес (шлюз, маска подсети) не был изменен пользователем, контроллер работает с заводскими установками. При изменении IP-адреса (шлюза, маски подсети) в «ручном» режиме (UDP1), контроллер сразу начинает работать с параметрами, заданными пользователем (без переключения питания);

– перемычка в положение 1–2. Вариант предназначен для работы в сетях с динамическим распределением IP-адресов и контроллер получает IP-адрес (шлюз, маску подсети) от DHCP-сервера;

– перемычка в положение 2–3. Контроллер работает с заводскими установками IP-адреса (шлюза, маски подсети). Пароль для доступа к контроллеру сбрасывается.

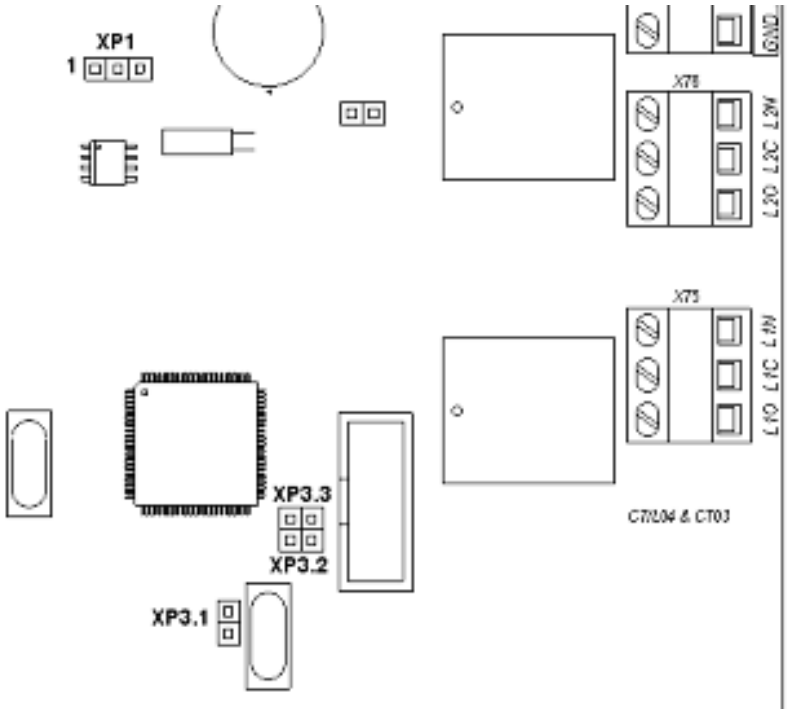


Рис. 2.4. Внешний вид фрагмента печатной платы контроллера

Выбор конфигурации контроллера производится с помощью перемычек XP3.1-XP3.3. Варианты конфигурации контроллера представлены в таблице 2.1.

Таблица 2.1

Варианты конфигурации контроллера CT/L04

№ п/п	Выбор конфигурации	Установлена перемычка		
		XP3.1	XP3.2	XP3.3
1	Контроллер для управления одной двухсторонней дверью	Нет	Нет	Нет
2	Контроллер для управления одной двухсторонней дверью с подключением к интерфейсу RS-485 до 8 контроллеров замка PERCo-CL201.	Да	Нет	Нет
3	Контроллер для управления двумя односторонними дверьми с подключением к интерфейсу RS-485 до 8 контроллеров замка PERCo-CL201.	Да	Да	Нет
4	Контроллер для управления турникетом.	Нет	Нет	Да
5	Контроллер для управления турникетом с подключением к интерфейсу RS-485 до 8 контроллеров замка PERCo-CL201.	Да	Нет	Да
6	Контроллер автотранспортной проходной.	Нет	Да	Да
7	Контроллер автотранспортной проходной с подключением к интерфейсу RS-485 до 8 контроллеров замка PERCo-CL201	Да	Да	Да

1.4. Перед началом работы в системе проверьте сетевые настройки тех контроллеров, которые будут конфигурироваться.

Адреса контроллеров для программирования получите у преподавателя.

Для проверки сетевых настроек контроллера необходимо перейти в меню Windows «Пуск» – «Выполнить». В окне «Запуск программы» ввести команду «CMD» и нажать «Ок». В командной строке ввести команду «ping» и IP-адрес контролера. Система должна отправить и получить пакеты на контроллер и с контроллера. После этого необходимо закрыть командную строку.

2. Конфигурирование контроллеров и видеокамер

2.1. Для начала работы с системой PERCo-S-20 запустите «Консоль управления PERCo-S-20» на рабочем столе. Пользователь – «ADMIN», пароль – без пароля.

2.2. Осуществите поиск контроллеров, установленных на рабочем месте. В системе PERCo-S-20 существует два варианта нахождения контроллеров в системе: автоматический поиск всех контроллеров в сети и адресный поиск. Для автоматического поиска всех контроллеров в сети, необходимо нажать на иконку 1 (рис. 2.5) «Провести конфигурацию», выбрать подсеть, тип оборудования и нажать «Ок». Для адресного поиска, используя IP-адрес контроллера необходимо нажать на иконку 2 «Доба-

вить новое устройство». Выбрать категорию, ввести IP-адрес контроллера и выбрать «Найти». Для скрытия панели поиска нового устройства, требуется повторное нажатие на «Добавить новое устройство».

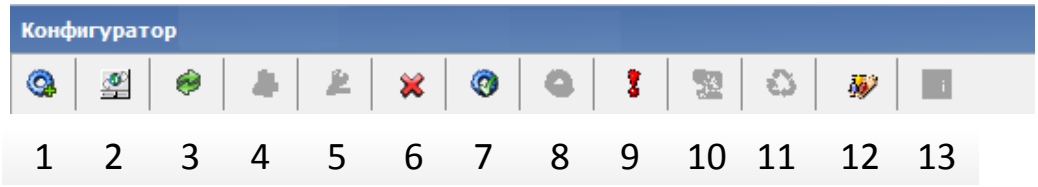


Рис. 2.5. Иконки панели инструментов

2.3. Настройте сервер видеоподсистемы.

Запустите с рабочего стола ярлык «Видеоподсистема PERCo-S-20». Откроется окно сервера видеоподсистемы. Для указания места, где будет создан файл архива видеоданных, надо выбрать «Добавить файл (Ins)», выбрать диск и задать размер файла. Нажать «Ок».

Для возможности задать IP-фильтрацию, т. е. разрешение или запрет на доступ к видеосерверу с определенных ПК, необходимо нажать на «Добавить правило» в разделе «Настройки». Настройка видеоподсистемы закончена.

Для поиска видеоподсистемы выбрать в строке конфигуратора иконку 2 «Добавить новое устройство», выбрать категорию «Видеоподсистемы», ввести IP-адрес ПК с установленным сервером видеоподсистемы, и нажать «Найти». Для скрытия панели поиска нового устройства необходимо «отжать» кнопку «Добавить новое устройство».

2.4. Передача параметров в контроллеры.

Для того чтобы передать параметры в контроллеры, необходимо установить курсор на верхнюю строчку «Система безопасности», и выбрать иконку 7 «Передать параметры всей системы». Базовые параметры переданы в контроллеры, теперь можно приступить к настройке системы.

2.5. Активируйте модули ПО (см. практическую работу № 1).

2.6. Ознакомьтесь с некоторыми возможностями, предоставляемыми конфигуратором.

При установке курсора на объект «Система безопасности», становятся активными иконки 12 «Получить информацию о версиях прошивок контроллеров» и 10 «Изменение пароля».

Кнопка «Получить информацию о версиях прошивок контроллеров» служит для просмотра версий прошивок на каждом контроллере, и в случае если она отлична от текущей, ее обновить.

Кнопка «Изменения пароля системы» предназначена для создания пароля на контроллер. При введении пустого пароля система запросит необходимость отменить защиту устройства паролем. При установке курсора на

контроллер становится активной иконка 6 «Исключить из конфигурации». Если контроллер исключен из конфигурации, появляется возможность его удалить и появляется возможность изменения 11 сетевых настроек.

В рамках контроллера можно изменить следующие параметры: IP-адрес, маску подсети, адрес основного шлюза и MAC-адрес контроллера. Изменение MAC-адреса происходит только в рамках базы данных. В случае изменения нужно снять галочку с параметра «Передать в аппаратуру». Если необходимо изменить IP-адрес, маску подсети и адрес основного шлюза, то галочка должна быть установлена. В случае изменения IP-адреса на адрес из другой подсети, на компьютеры должны быть установлены два IP-адреса: из подсети, в которой сейчас находится контроллер, и из подсети, куда он перемещается.

Для включения контроллера в конфигурацию необходимо отжать иконку 6 «Включить в конфигурацию». После включения контроллера в конфигурацию система информирует о том, что конфигурация не изменилась (перемычки настроек контроллера не изменены), или изменилась. После этого необходимо передать параметры в контроллер.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Консоль управления PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Поясните общие принципы сетевой адресации протокола TCP/IP?
2. Каким образом конфигурируются контроллеры и видеокамеры в системе безопасности и повышения эффективности PERCo-S-20?
3. Как изменить сетевые настройки контроллера, используя консоль управления?
4. Варианты конфигурации контроллера CT/L04?
5. Сколько байт информации содержится в IP-адресе?
6. Каким образом сконфигурировать контроллер CT/L04 на управление автотранспортной проходной?

Задания для самостоятельной работы

1. Изучите и законспектируйте в рабочей тетради принцип работы микроконтроллеров.
2. Проведите сравнительный анализ контроллеров CT/L04.2 и CT/L14.

ПРАКТИЧЕСКАЯ РАБОТА № 3

Создание помещений и управление мнемосхемой
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений моделирования помещений, управления мнемосхемой, размещения и настройки оборудования в системе безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекции по теме № 1.3 «Технологии идентификации».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Подготовить экспликацию объекта в формате *.jpeg.

Учебные вопросы:

1. Построение иерархии помещений. Закрепление оборудования.
2. Создание и настройка мнемосхемы.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.
2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

6. Р 071-2017. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 20 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

Для удобства наглядного восприятия функциональных схем объектов, контролируемых либо управляемых, применяют мнемосхемы – графические изображения схем этих объектов. Мнемосхема может отображать какой-либо технологический процесс или систему. Другими словами, мнемосхема являет собой информационную условную модель системы или процесса в виде символов, обозначающих части системы, а также их связи.

Мнемосхема отражает графически структуру всей системы, облегчая тем самым работу оператора, который, благодаря такой схеме, легче запоминает структуру системы, взаимосвязи параметров, назначение тех или иных органов управления, приборов, станков и т. д.

Для оператора, управляющего процессами, мнемосхема служит одним из важнейших источников информации о процессах, происходящих в данный момент в системе, о структуре и характере этих процессов, о те-

кущем статусе системы, в частности, об авариях и нарушениях нормальных режимов работы.

Рекомендации «Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения», разработанные научно-исследовательским центром «Охрана» Росгвардии в 2017 году, устанавливают основные условные графические обозначения элементов технических средств охраны (систем охранно-тревожной сигнализации, контроля и управления доступом, охранного телевидения и других), а также буквенно-цифровые обозначения этих систем на чертежах и схемах при разработке проектной документации систем обеспечения антитеррористической и противокриминальной безопасности.

При разработке чертежей схем СКУД необходимо руководствоваться следующими основными принципами:

– в случаях применения неизвестных условных обозначений и знаков их значение должно быть расшифровано в таблице «Условные знаки и обозначения», прилагаемой к чертежу (схеме);

– размеры условных графических обозначений элементов систем в чертежах и схемах принимают без соблюдения масштаба;

– условные графические обозначения не показывают фактическую конструкцию элементов;

– в схемах, выполняемых в аксонометрической проекции, элементы систем допускается изображать упрощенно, в виде контурных очертаний;

– условные обозначения приборов и систем безопасности, применяемые в схемах, включают в себя графические, буквенные и цифровые обозначения.

Условные графические обозначения элементов, наиболее чаще применяемые в схемах систем контроля и управления доступом, приведены в таблицах 3.1 – 3.11.

Таблица 3.1

Приборы приемно-контрольные охранные и пульты

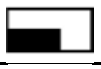
№ п/п	Наименование	Обозначение
1.	Прибор приемно-контрольный охранный	
2.	Расширитель на N зон	
3.	Пульт управления непрограммируемый	
4.	Пульт управления программируемый	
5.	Релейный модуль управления	

Таблица 3.2

Оповещатели и системы оповещения

№ п/п	Наименование	Обозначение
1.	Речевой, звуковой	
2.	Речевой, звуковой (потолочный)	
3.	Световой	
4.	Комбинированный (световой + звуковой)	

Таблица 3.3

Шифроустройства

№ п/п	Наименование	Обозначение
1.	Шифроустройство	
2.	Считыватель без клавиатуры	
3.	Считыватель с клавиатурой	

Таблица 3.4

Видеодомофоны

№ п/п	Наименование	Обозначение
1.	Панель вызова видеодомофона	
2.	Панель приема видеодомофона	

Таблица 3.5

Источники электропитания для технических средств охраны

№ п/п	Наименование	Обозначение
1.	Источник бесперебойного электропитания	
2.	Источник электропитания постоянного тока	

Таблица 3.6

Устройства преграждающие

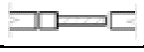
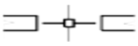
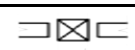
№ п/п	Наименование	Обозначение
1.	Шлагбаум	
2.	Турникет	
3.	Шлюз, тамбур-шлюз, проходная кабина	
4.	Устройство досмотра (обнаружители металла, взрывчатых, наркотических веществ и другие)	
5.	Система паркинговая	
6.	Секция дорожная подъемная	

Таблица 3.7

Устройства исполнительные

№ п/п	Наименование	Обозначение
1.	Замок электромеханический	
2.	Замок электромагнитный	
3.	Защелка электромеханическая	
4.	Доводчик двери механический	
5.	Доводчик двери электромеханический	
6.	Кнопка выхода	

Таблица 3.8

Устройства управления

№ п/п	Наименование	Обозначение
1.	Контроллер	
2.	Модуль интерфейсный	
3.	Сервер	

Таблица 3.9

Домофоны

№ п/п	Наименование	Обозначение
1.	Микрофон домофона	
2.	Панель вызова домофона	
3.	Панель приема домофона	

Таблица 3.10

Устройства коммутации и проводок

№ п/п	Наименование	Обозначение
1.	Линия проводки (общее изображение)	
2.	Линия электропитания	
3.	Коробка соединительная	
4.	Бокс телефонный	
5.	Устройство коммутационное	

Таблица 3.11

Условные графические обозначения унифицированного и иного специального оборудования

№ п/п	Наименование	Обозначение
1.	Персональный компьютер	
2.	Дополнительное оборудование	
3.	Оборудование освещения	

Методические указания по отработке учебных вопросов

1. Построение иерархии помещений. Закрепление оборудования

Подраздел «Помещения и мнемосхема» раздела «Администрирование» предназначен для создания структурной схемы помещений объекта и создания мнемосхемы – графической схемы территории объекта с расположенными на ней устройствами системы безопасности. Изображение окна раздела представлено на рис. 3.1.

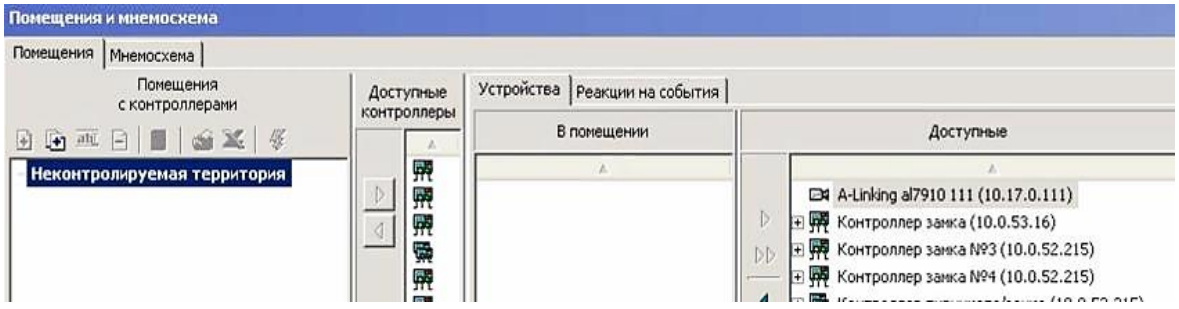


Рис. 3.1. Окно раздела помещений и мнемосхем

Создание помещений и мнемосхем дает возможность управления не только индивидуально каждыми устройством, но и всеми устройствами в помещении. Структурная схема помещений также используется для контроля перемещений сотрудников по территории предприятия в случае активной системы контроля зональности. В случае реализации автоматического учета рабочего времени схема помещений используется для указания помещений, время пребывания сотрудников в которых будет учитываться как рабочее.

По умолчанию в схеме имеется только одно помещение – «Неконтролируемая территория», являющееся нулевым уровнем иерархии помещений. Относительно этого уровня начинается построение мнемосхемы. Помещения, связанные с неконтролируемой территорией, являются первым уровнем.

Для добавления нового помещения необходимо нажать активную иконку «Добавить внутреннее помещение в выделенное помещение» и ввести название. Установив курсор на созданное помещение, можно добавить помещение на этот же уровень – иконка «Добавить помещение», или добавить внутреннее (вложенное) помещение. После этого необходимо «Сохранить».

Помещения второго уровня – помещения, для доступа в которые нужно пройти первый уровень помещений (рис. 3.2).

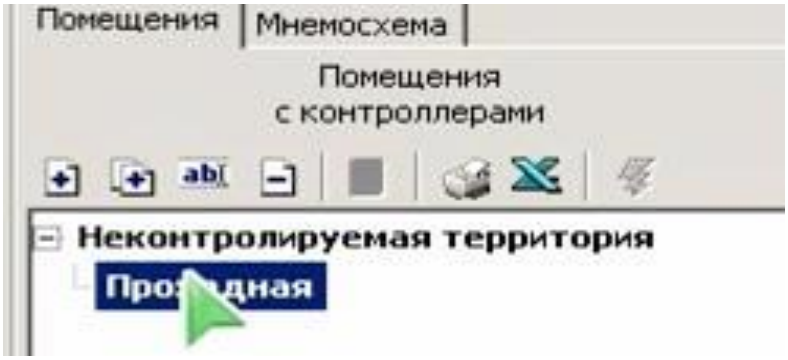


Рис. 3.2. Помещение второго уровня

Для добавления контроллера в помещение необходимо установить курсор на помещение и из списка доступных контроллеров выбрать необходимый, и нажать иконку «Добавить контроллер в помещение».

Далее проверяем параметры, что связывает данный контроллер. Если все верно, нажать «Ок». Для просмотра расположения считывателей необходимо нажать иконку «Показать считыватели».

Для добавления в помещение других устройств необходимо выбрать устройство, выбрать помещение, в котором необходимо установить и нажать на иконку «Закрепить устройство за помещением» (рис. 3.3).

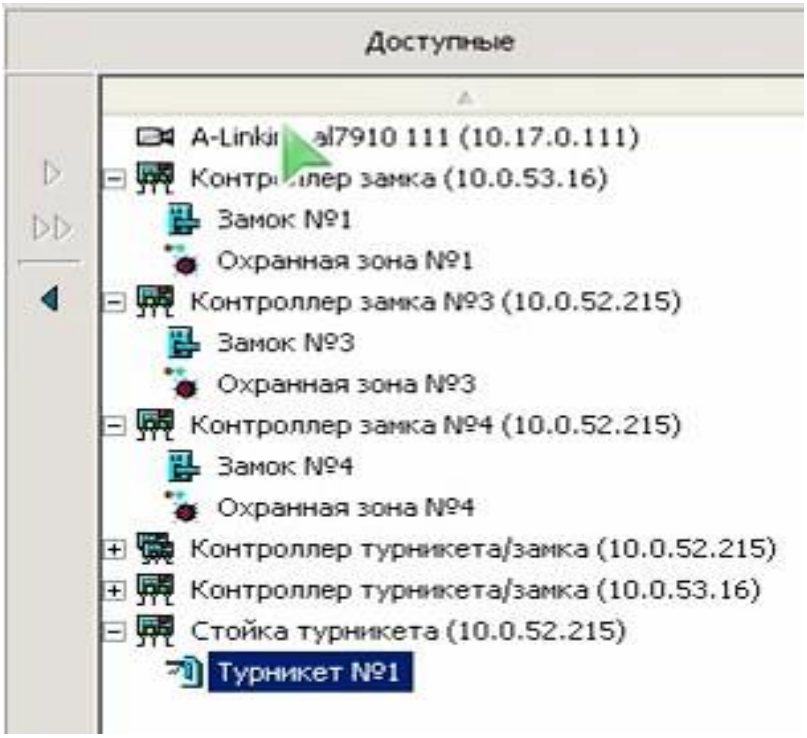


Рис. 3.3. Окно выбора доступных устройств для размещения

После всех действий сохранить конфигурацию, для чего нажать на иконку «Сохранить».

Общие для контроллера турникета и замка устройства (дополнительные входы и выходы) отображаются как компоненты контроллера турникета/замка (рис. 3.4).

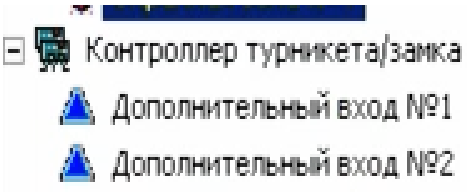


Рис. 3.4. Компоненты контроллера турникета/замка

Если контроллер сконфигурирован для управления турникетом, его устройства отображаются иконкой «Стойка турникета». Если контроллер сконфигурирован для управления замком, его устройства отображаются как контроллер замка.

2. Создание и настройка мнемосхемы

2.1. Получите у преподавателя задание.

Для создания мнемосхемы (графического отображения структуры помещений) необходимо перейти во вкладку «Мнемосхема» и нажать

иконку «Создать схему», ввести название и нажать «Ок» (рис. 3.5).

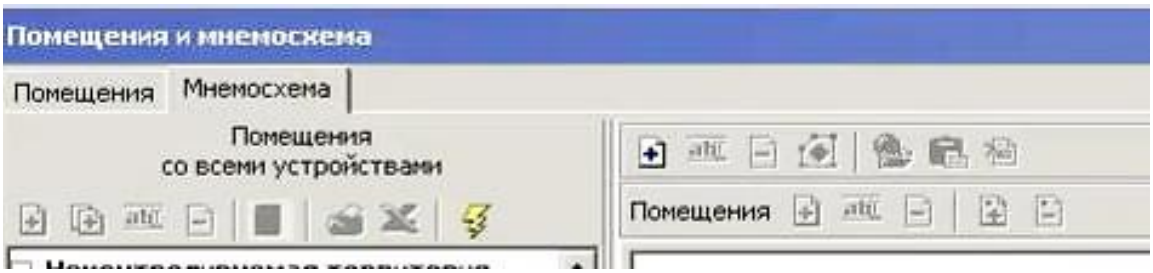


Рис. 3.5. Окно вкладки мнемосхемы

После этого становятся активными иконки «Изменить название схемы», «Удалить мнемосхему» и «Редактирование схемы». После нажатия на «Начать редактирование», становится активной иконка «Загрузить рисунок из файла», и необходимо выбрать ее. Далее выбрать графический файл одного из трех форматов: JPG, JPEG и BMP, и нажать «Открыть». Загрузив графический файл, он будет использоваться как подложка мнемосхемы. Для расположения помещений на мнемосхеме необходимо установить курсор на помещении, которое требуется разместить на схеме. После этого становится активной иконка «Расположить на схеме», и выбрать ее.

Для схематического отображения помещения нужно в любом месте схемы кликнуть один раз левой кнопкой мыши (рис. 3.6).

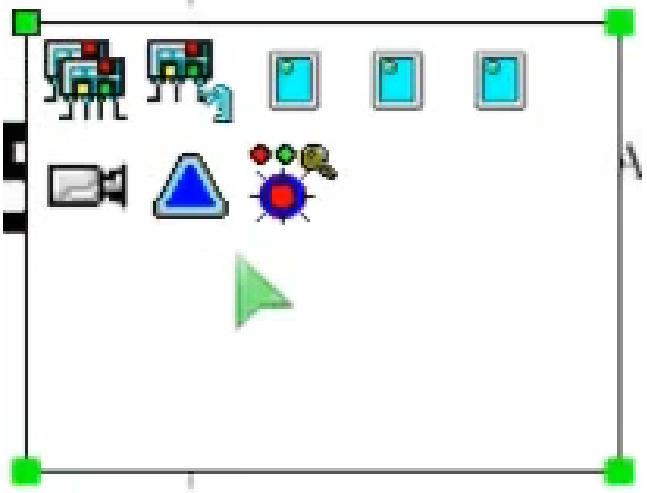


Рис. 3.6. Окно схематического отображения помещения

Для перемещения помещения зажать его левой кнопкой мыши. В добавляемом схематичемском отображении видны устройства, которые можно добавить в помещение.

Для задания полупрозрачности помещения (чтобы была видна подложка) требуется нажать иконку «Изменить визуальные параметры» и

выбрать заполнение, цвет заполнения и нажать «Ок». Для того чтобы растянуть схематичный прямоугольник на помещение, нужно зажать левой кнопкой мыши угловые точки, и растянуть до необходимого положения. Для добавления угловых точек требуется нажать иконку «Добавить точку в контур объекта». Теперь можно располагать устройства на схеме. Для этого выбрать устройство, которое находится с схематическом отображении, и расположить его в нужном месте на схеме. Для выхода из режима редактирования требуется отжать кнопку «Завершить редактирование» и нажать иконку «Сохранить все изменения». С данного момента появляется возможность управлять всеми устройствами в помещении. Перейти в раздел «Управление устройствами и мнемосхемой» (рис. 3.7).

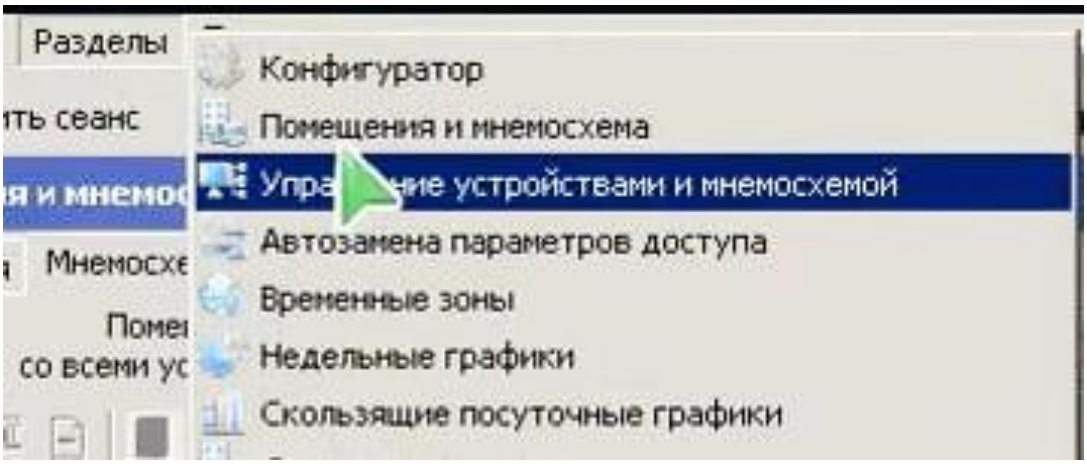


Рис. 3.7. Окно раздела управления устройствами и мнемосхемой

В данном разделе три вкладки: «Устройства», «Помещения» и «Мнемосхема» (рис. 3.8).

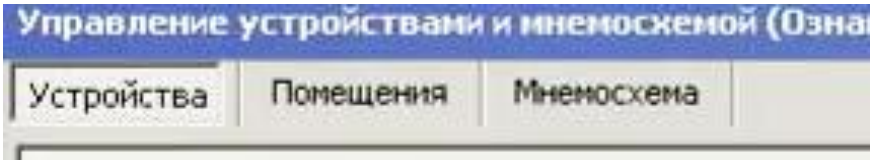


Рис. 3.8. Окно вкладок раздела

Вкладка «Устройства» дает возможность управлять каждым устройством по отдельности (рис. 3.9). В данной вкладке можно задать определенные команды каждому устройству и задавать оповещения о событиях. Для этого необходимо выбрать устройств, и назначить ему соответствующие команды. Также во вкладке есть возможность настраивать оповещения о событиях, для этого нужно выбрать курсором нужное событие. В поле «Текстовое» можно ввести текстовое оповещение. В поле «Звуковое» можно присвоить звуковой файл определенным событиям.

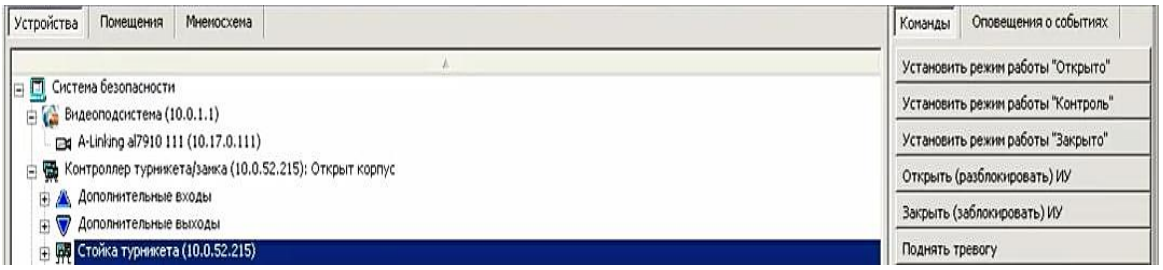


Рис. 3.9. Окно вкладки устройства

Вкладка «Помещения» дает возможность подавать команды всем устройствам в рамках одного помещения (рис. 3.10).

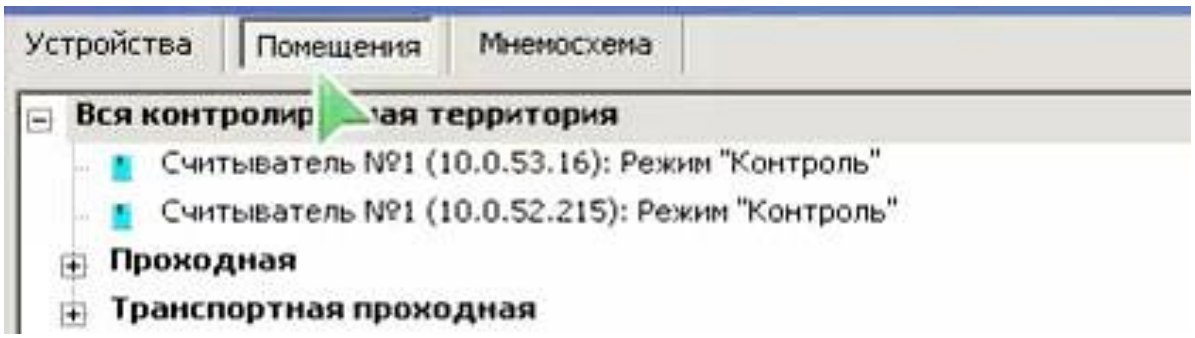


Рис. 3.10. Окно вкладки помещения

Например, установить режимы «Открыто», «Закрыто», «Контроль» или разблокировать все устройства в выбранном помещении или на всей территории объекта. Для этого нужно выбрать часть помещения и установить команды.

Вкладка «Мнемосхема» отображает созданную графическую структуру (рис. 3.11). Также в рамках каждого из устройств или помещений существует возможность управления.

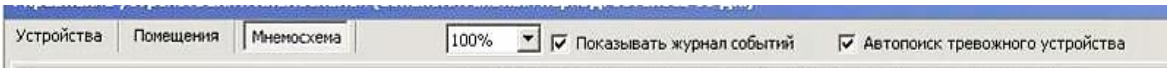


Рис. 3.11. Окно вкладки мнемосхема

Клик правой кнопкой мыши по устройству или помещению вызывает список команд устройства. В выпадающем меню присутствуют все возможные команды, которые можно задавать на устройстве или в помещении. Внизу раздела отображается «Журнал событий» – отображение всей системной информации от устройств системы безопасности в режиме реального времени. Функционал раздела позволяет скрывать и отображать журнал событий, за это отвечает флажок «Показать журнал событий». Флажок «Автопоиск тревожного события» включает функционал автома-

тического переключения на мнемосхему с тревожным событием. Также есть возможность выбрать масштаб отображаемой мнемосхемы от 40% до 100%.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Консоль управления PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Поясните принципы построения иерархии помещений в системе.
2. Что означает термин «Неконтролируемая территория»?
3. Поясните назначение дополнительных входов и выходов контроллера CT/L04.
4. Опишите последовательность создания мнемосхемы.
5. Каким документом регламентируются рекомендуемые условно-графические обозначения средств контроля и управления доступом?
6. Раскройте определение термина «мнемосхема».
7. В чем заключается назначение мнемосхем?

Задания для самостоятельной работы

1. Отразите в тетради мнемосхему объекта (отделения банка), состоящего из 5 помещений, с расположенными элементами системы контроля и управления доступом.
2. Разработайте структурную схему системы контроля и управления доступом на базе мнемосхемы, выполненной в первом задании.

ПРАКТИЧЕСКАЯ РАБОТА № 4

Создание графиков работы
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений программирования и создания графиков работы в системе безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекций по теме № 2.1 «Особенности организации и настройки сетевых систем контроля и управления доступом».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Подготовить экспликацию объекта в формате *.jpeg.

Учебные вопросы:

1. Создание именованных интервалов и схемы работы.
2. Создание графиков работы.
3. Создание временных зон.
4. Создание графиков доступа.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.

2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

В системе PERCo поддерживаются следующие режимы работы:

– «Открыто» (аварийный режим);

– «Контроль»;

– «Совещание» (только для контроллера замка PERCo-CL05 и контроллера PERCo-CT/L04 в варианте конфигурации «управление двумя односторонними дверьми» и для подключенных контроллеров замка PERCo-CL201);

– «Охрана» (только для контроллера замка PERCo-CL05 и контроллера PERCo-CT/L04 в вариантах конфигурации «управление дверьми» и для подключенных контроллеров замка PERCo-CL201). Режим работы *«Охрана»* устанавливается контроллером автоматически при успешной постановке на охрану зоны, в которую входит УПУ. Постановка под охрану (по карте доступа) и снятие с охраны возможны только при нахождении контроллера в режимах работы «Контроль», «Совещание», «Открыто» и «Охрана»;

– «Закрыто» (аварийный режим).

Переходы между режимами работы.

1. Режим работы «Охрана» (только для контроллера замка PERCo-CL05 и контроллера PERCo-CT/L04 для вариантов конфигураций «управление дверьми» и для подключенных контроллеров замка PERCo-CL201).

Переход в режим работы «Охрана» по карте возможен из режимов работы «Контроль», «Совещание» и «Открыто» (картой, имеющей право постановки).

Выход из режима работы «Охрана» по карте производится в предыдущий режим работы, если это были режимы работы «Контроль», «Совещание» или «Открыто» либо в режим работы «Контроль», если предыдущий режим работы был «Закрыто» (т. е. режим работы «Охрана» был установлен от ПО).

Переход в режим работы «Охрана» от ПО возможен из любого режима работы. Выход из режима работы «Охрана» от ПО возможен в любой режим работы.

Выход из режима работы «Охрана» по ИК–пульту невозможен.

2. Режим работы «Закрыто».

Переход в режим «Закрыто» и от ПО возможен из любого режима работы. Выход из режима работы «Закрыто» от ПО возможен в любой режим работы.

Переход в режим «Закрыто» по ИК–пульту возможен из любого режима работы, кроме режима работы «Охрана». Выход из режима «Закрыто» по ИК–пульту возможен в любой режим работы (кроме режима работы «Охрана»).

Если режим работы «Закрыто» был установлен от ИК–пульта, то при открывании ИУ производится возврат в предыдущий режим.

3. Режим работы «Открыто».

Переход в режим «Открыто» от ПО возможен из любого режима работы. Выход из режима работы «Открыто» от ПО возможен в любой режим работы.

Переход в режим «Открыто» по ИК–пульту возможен из любого режима работы, (кроме режима работы «Охрана»). Выход из режима работы «Открыто» по ИК–пульту возможен в любой режим (кроме режима работы «Охрана»).

Возврат в режим работы «Открыто» по карте возможен из режима работы «Охрана» (картой, имеющей право снятия).

Выход из режима работы «Открыто» по карте возможен в режим работы «Охрана» (картой, имеющей право постановки).

4. Режим работы «Контроль».

Переход в режим работы «Контроль» от ПО возможен из любого режима работы.

Переход в режим работы «Контроль» по ИК–пульту возможен из любого режима работы (кроме режима работы «Охрана»).

Переход в режим работы «Контроль» по карте возможен из режима работы «Охрана».

Выход из режима работы «Контроль» от ПО возможен в любой режим работы.

Выход из режима работы «Контроль» по ИК–пульту возможен в любой режим работы (кроме режима работы «Охрана»).

Выход из режима работы «Контроль» по карте возможен в режим работы «Охрана».

5. Режим работы «Совещание» – аналогичен режиму работы «Контроль» (только для контроллера замка PERCo-CL05 и контроллера PERCo-CT/L04 для варианта конфигурации «управление двумя односторонними дверьми» и для подключенных контроллеров замка PERCo-CL201).

Временные критерии доступа.

К временным критериям доступа относятся: временные зоны; недельные графики; скользящий посуточный график; скользящий понедельный график; календарь праздничных дней.

Временная зона состоит из четырех интервалов времени суток. В случае если групповые права доступа содержат временную зону, то доступ идентификаторов этой группы возможен только в разрешенные временной зоной интервалы, независимо от дня недели и календаря праздничных дней. На базе временных зон строятся все остальные временные критерии доступа.

Присвоение карте временной зоны позволяет автоматически изменять временные ограничения для этой карты в зависимости от текущего времени суток.

Недельный график состоит из списка номеров временных зон для каждого дня недели, причем для каждого конкретного дня недели временная зона выбирается либо установленная для этого дня недели, либо установленная для 1-го, 2-го, …., 8-го типа дня из календаря праздничных дней. В случае если групповые права доступа содержат недельный график, то доступ идентификаторов этой группы зависит от дня недели и данных, запрограммированных в календаре праздничных дней, и возможен только в разрешенные интервалы временной зоны, связанной с текущим днем недели или типом дня из календаря праздничных дней.

Присвоение карте недельного графика позволяет автоматически изменять временные ограничения для этой карты в зависимости от дней недели, праздничных и предпраздничных дней.

Скользящий посуточный график состоит из списка номеров временных зон для каждого дня графика и имеет циклический характер построения: за последним днем графика следует его первый день, и график начинается заново. Максимальная длина графика равна 30 дням. В случае если групповые права доступа содержат скользящий посуточный график,

то доступ идентификаторов этой группы не зависит от дня недели и данных, запрограммированных в календаре праздничных дней, и возможен в разрешенные интервалы временной зоны, связанной с текущим порядковым номером дня в этом графике.

Присвоение карте скользящего посуточного графика позволяет автоматически изменять временные ограничения для этой карты в зависимости от текущего дня смены.

Скользящий понедельный график состоит из списка номеров недельных графиков для каждой недели графика и имеет циклический характер построения: за последним днем последней недели графика следует его первый день первой недели, и график начинается заново. Максимальная длина графика равна 54 неделям, т. е. строится глубиной до 1 года. В случае если групповые права доступа содержат скользящий понедельный график, то доступ идентификаторов этой группы зависит от дня недели и данных, запрограммированных в календаре праздничных дней, и возможен в разрешенные интервалы временной зоны, входящей в текущий недельный график данного скользящего графика.

Присвоение карте скользящего понедельного графика позволяет автоматически изменять временные ограничения для этой карты в зависимости от дней недели, номеров недели, праздничных и предпраздничных дней, т. е. позволяет составлять графики работы с учетом отпусков.

Календарь праздничных дней состоит из списка номеров типов дней для каждого дня года и предназначен как для придания дням года свойств, отличающих их от обычных дней недели, так и для возможности переноса дней недели при необходимости. Каждому дню года в календаре присваивается признак типа дня. Всего может быть признаков 16: день соответствует текущему календарному дню недели; 1 – понедельник; 2 – вторник; …, 7 – воскресенье; 8 – день соответствует 1 типу; 9 – день соответствует 2 типу; 10 – день соответствует 3 типу; 11 – день соответствует 4 типу; 12 – день соответствует 5 типу; 13 – день соответствует 6 типу; 14 – день соответствует 7 типу; 15 – день соответствует 8 типу.

Доступ карт, связанных с недельным и скользящим недельным графиками, в праздничные дни ограничивается по времени временной зоной, присвоенной празднику соответствующего типа, и не зависит от текущего дня недели.

Методические указания по отработке учебных вопросов

1. Создание именованных интервалов и схемы работы

Формирование графиков работы для каждого сотрудника в системе PERCo-S-20 осуществляется в разделе программного обеспечения «Графики работы», подраздел «Сотрудники» (рис. 4.1).

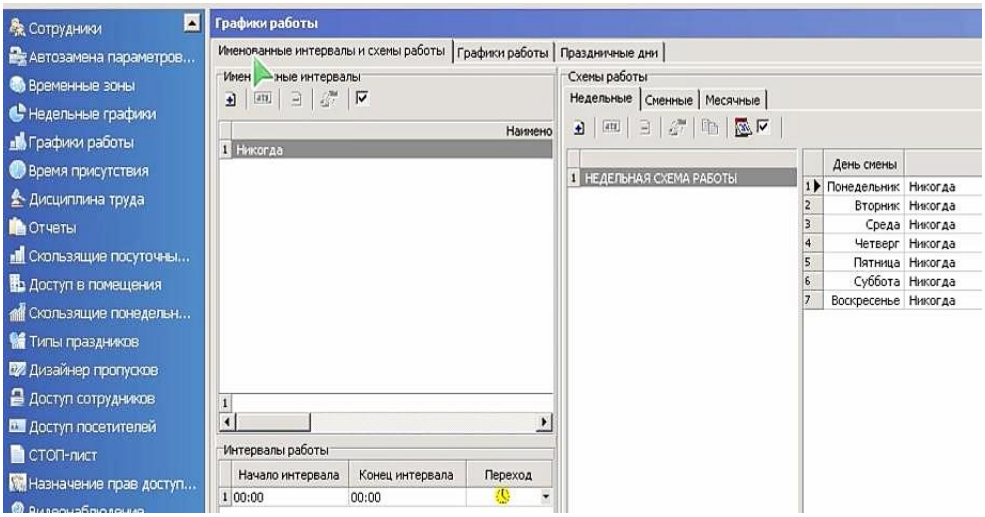


Рис. 4.1. Окно раздела графиков работы

График работы необходим для формирования дисциплинарных отчетов и отчетов по учету рабочего времени. Функционал создания графиков работы доступен в базовом ПО. Функционал учета рабочего времени доступен и дисциплинарных отчетах в одноименных модулях расширенного ПО.

Перейдите в раздел «Графики работы». Здесь имеются три вкладки:

– именованные интервалы схемы работы;
– графики работы;
– праздничные дни.

Первоначально создаются именованные интервалы – это интервалы в течение рабочего дня, на основании которых создаются схемы работы и графики работы.

1.1. Создание именованного интервала

Для создания именованного интервала необходимо нажать иконку «Добавить именнованный интервал» и ввести его название, например, «Стандарт». После этого нажмите иконку «Добавить интервал» – вводится предустановленный интервал с 9.00 – 13.00. Повторное нажатие иконки «Добавить интервал» приводит к появлению интервала с 13.45 – 17.45. Таким образом, время с 13.00 и до 13.45 не будет учитываться.

Количество интервалов в рамках одного именованного интервала не ограничено. Графа переход – «без перехода» означает, что начало и конец интервала находятся в рамках одного дня. Полностью черные часы означают, что значения времени определяют завтрашний день. После нажатия «Ок» будет создан именованный интервал «Стандарт».

Самостоятельно создайте три именованных суточных интервала с различным временем отдыха. Создайте суточный интервал работы «Смена». Создайте скользящий интервал.

1.2. Создание схем работы

Для создания недельной схемы работы нажмите иконку «Добавить схему» и введите ее название, например, «Стандарт» (рис. 4.2). После этого необходимо выбрать уже созданные интервалы на каждый из дней недели.

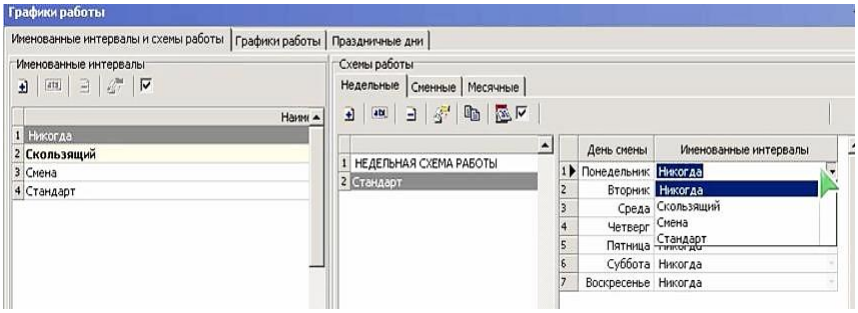


Рис. 4.2. Окно создания графиков работы

Для создания сменной схемы работы необходимо перейти во вкладку «Сменные схемы». Нажав иконку «Добавить схему», ввести ее название, например, «Смена». Далее необходимо выбрать даты начало смен, количество дней в смене и нажать «Ок». После этого для всех дней смены необходимо определить именованные интервалы.

Для создания месячной схемы работы нажмите иконку «Добавить схему» и введите ее название, например, «Скользящая» (рис. 4.3). Теперь на все дни месяца необходимо установить именованные интервалы. Для этого, после выбора именованного интервала, можно использовать операцию «Копирование». В окончании нажмите иконку «Сохранить».

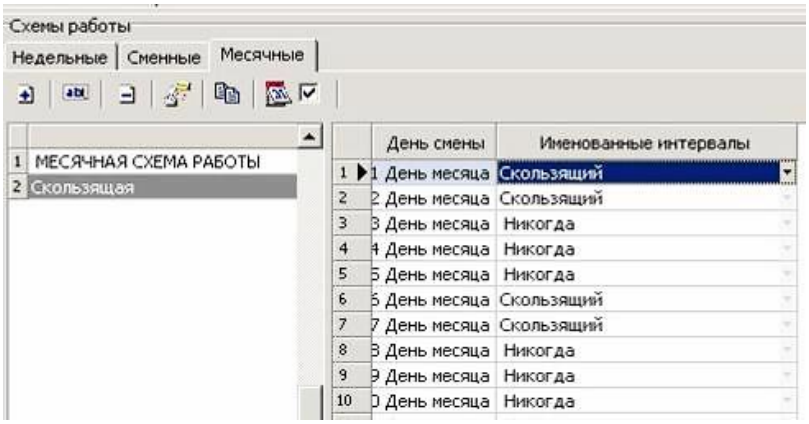


Рис. 4.3. Окно месячных схем работы

2. Создание графиков работы

2.1. Для создания графика работы перейдите в раздел «Графики работы», нажмите иконку «Добавить график работы» и введите его название, например, «Стандарт» (рис. 4.4).

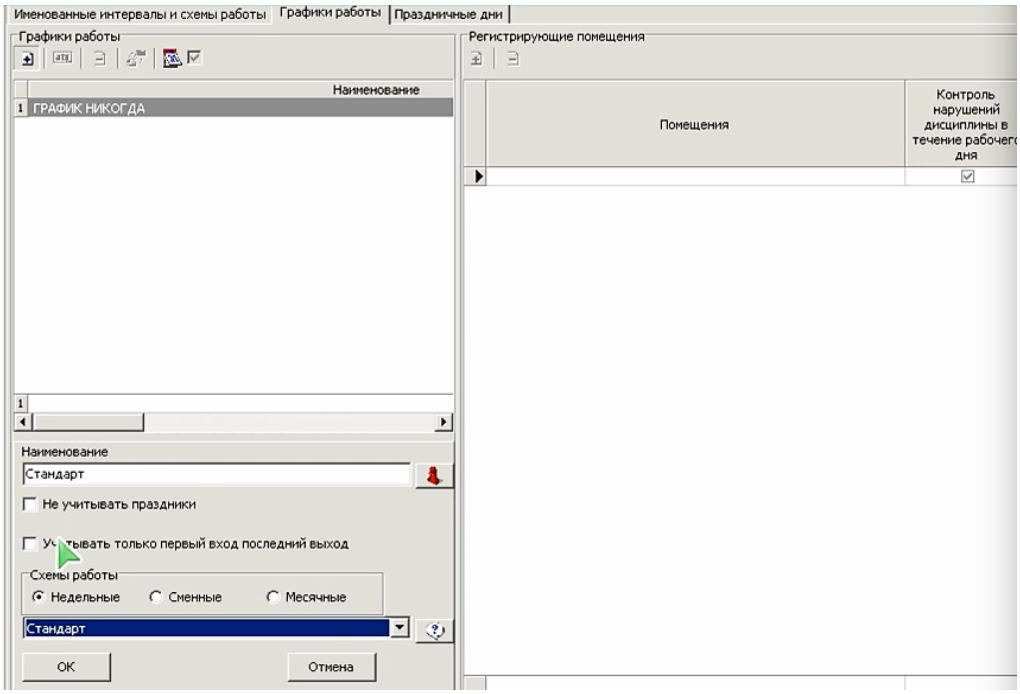


Рис. 4.4. Окно создания графиков работы

В выпадающем меню «Схемы работы» выбираем раздел «Недельные» и в нем уже выбираем созданную схему «Стандарт». Для проверки откройте дополнительную информацию о схемах.

При создании графика работы есть возможность выбрать следующие параметры: «Не учитывать праздники», «Учитывать только первый вход, последний выход». При установке параметра «Не учитывать праздники», при выпадении рабочего дня на праздник сотрудник должен выйти на работу. Параметр «Учитывать только первый вход, последний выход» позволяет при расчете рабочего времени не учитывать промежуточные входы и выходы.

2.2. Ознакомьтесь и законспектируйте информацию из раздела «Дополнительная информация к отчетам по дисциплине труда». Здесь имеется возможность устанавливать смягчения контроля дисциплинарных нарушений. Данные установки влияют только на отчеты по дисциплине труда. На учет рабочего времени данные установки не влияют. После создания графика работы нажать «Ок».

2.3. Каждому графику работы необходимо присвоить регистрирующее помещение, где будет учитываться начало и окончание рабочего времени. Для этого необходимо перейти в раздел «Регистрирующие помещения» и нажать иконку «Добавить помещение». Появляется список доступных помещений из раздела «Помещения и мнемосхема». Можно выбрать головные помещения, то есть те, которые связаны с неконтролируемой территорией. В этом случае будет засчитано все время, проведенное на территории предприятия.

Если необходимо учитывать рабочее время, проведенное в конкретном помещении, то следует его выбрать и нажать «Ок».

Параметр «Контроль нарушений дисциплины в течении рабочего дня» отвечает за попадание сотрудников в отчеты по дисциплине труда в случае ухода на обед ранее положенного срока и возвращении позднее положенного срока.

2.4. Создайте график работы «Сменный». Выберите «Схемы работы» – сменные и в выпадающем меню выберите «Смена». Установите параметры: «Не учитывать праздники»; в «Дополнительной информации …» – все нулевые значения. В регистрирующие помещения добавьте, например, проходные.

2.5. Создайте график работы «Скользящий». Выберите «Схемы работы» – месячные и в выпадающем меню выберите «Скользящая». Параметр «Не учитывать праздники» – уберите. В регистрирующие помещения добавьте внутренние помещения. Нажмите иконку «Сохранить».

2.6. Перейдите на вкладку «Праздничные дни». Данный раздел используются при формировании отчетов по дисциплине труда и учета рабочего времени (рис. 4.5).

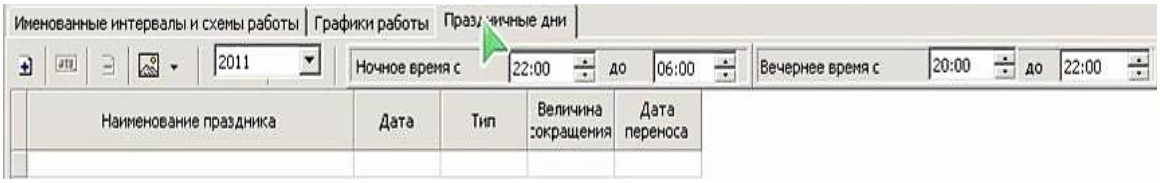


Рис. 4.5. Окно вкладки праздничных дней

Первоначально необходимо заполнить поля предопределенными значениями (рис. 4.6).

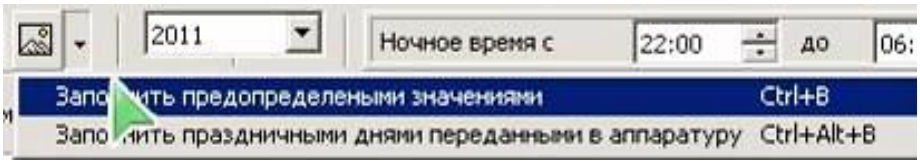


Рис. 4.6. Окно заполнения предопределенными значениями

Возможны три типа записи: праздник, предпраздничный день и рабочий выходной. Для добавления праздника необходимо нажать иконку «Добавить», выбрать тип праздника, ввести наименование, выбрать дату и нажать «Ок». Для добавления предпраздничного дня нажать на иконку «Добавить», выбрать тип предпраздничный день, ввести наименование, выбрать дату, величину сокращения и нажать «Ок». И необходимо сохранить конфигурацию. Также во вкладке «Праздничные дни» устанавливает-

ся то время, которое будет считаться вечерним и ночным в отчетах по учетам рабочего времени.

Перейдите в раздел «Сотрудники» и определите для всех графики работы.

3. Создание временных зон

Графики доступа – это определенным образом структурированные временные интервалы, согласно которым сотрудник получает доступ в охраняемое помещение или происходит запрет доступа в охраняемое помещение.

Графики доступа подразделяются на следующие типы:

– недельные графики доступа;
– скользящие посуточные графики доступа;
– скользящие понедельные графики доступа;
– временные зоны.

Количество графиков каждого типа ограниченно 256 графиками. Это связано с ограничением памяти контроллеров. Графики доступа после создания передаются в аппаратуру и хранятся в энергонезависимой памяти каждого контроллера.

Для создания графиков доступа в системе PERCo-S-20 необходимо создать временные зоны.

1.1. Перейдите на вкладку «Параметры доступа\Временные зоны». Графики доступа могут базироваться на созданных графиках работы. Для создания графика доступа используйте:

– недельный график, с 9:00 утра до 17:45, суббота и воскресенье – выходные (рис. 4.7);

– сменный график, 2 дня через 2, с 20:00 до 8:00 следующего дня (рис. 4.8).

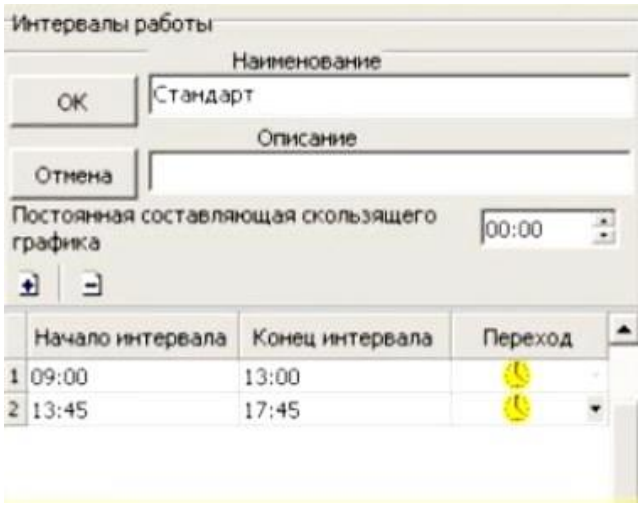


Рис. 4.7. Окно задания недельного графика работы

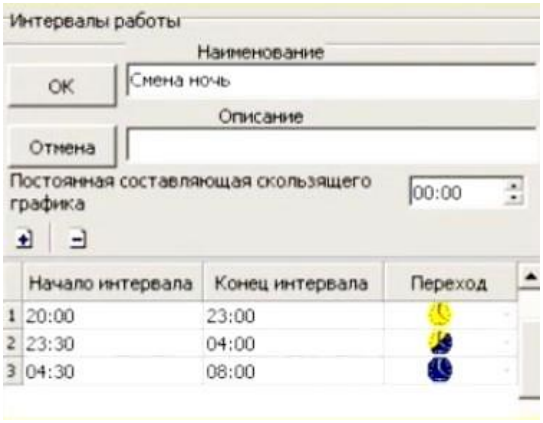


Рис. 4.8. Окно задания сменного графика работы

По умолчанию существует 2 неизменяемых временных зоны: зона «Всегда» с 00:00 до 23:59 (рис. 4.9); «Никогда» с 00:00 по 00:00 (рис. 4.10).

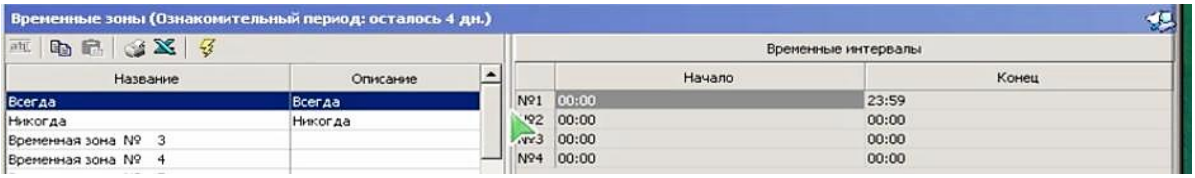


Рис. 4.9. Окно зоны всегда

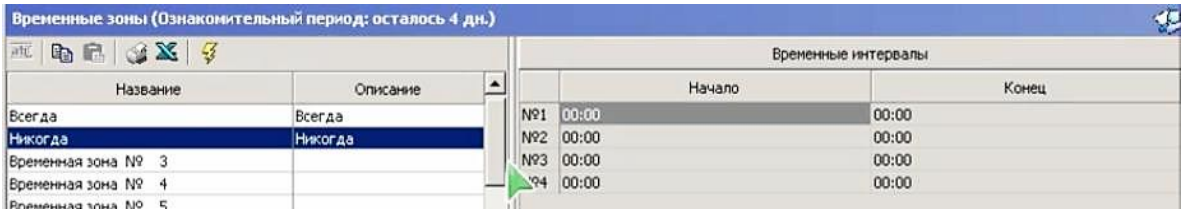


Рис. 4.10. Окно зоны никогда

1.2. Создайте временные зоны. Для этого выберите любую зону (рис. 4.11) и нажмите иконку «Изменить название\описание». Введите название «Стандарт», и нажмите «Ок».

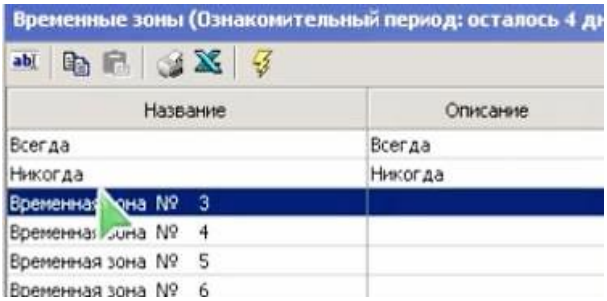


Рис. 4.11. Окно выбора временной зоны

Во вкладке «Временные интервалы» выберите интервал № 1 и нажмите иконку «Изменить».

Так как график работы с 9:00 до 17:45, поэтому доступ необходимо предоставить, например, с 08:30 по 18:15. На основании этой временной зоны в дальнейшем создается недельный график доступа.

Выберите другую временную зону и аналогичным образом создайте зону «Смена 1». На основании этой временной зоны в дальнейшем создается сменный график доступа с 20:00 до 08:00.

Основное отличие графиков доступа от графиков работ состоит в том, что графики работы хранятся только в БД и используются для формирования отчетов УРВ, а графики доступа передаются в аппаратуру.

В контроллерах отсутствуют понятия «вчера», «сегодня», «завтра», только «сегодня». Поэтому интервал с 20:00 до 08:00 контроллер интерпретирует, как интервал с 08:00 до 20:00. В связи с этим, временные интервалы необходимо разбивать в рамках одного дня.

Так как смена начинается в 20:00, доступ необходимо предоставить, например, с 19:30 до 23:59.

Выберите другую временную зону и аналогичным образом создайте зону «Смена 2».

Во второй день смены сотрудник работает с 00:00 до 08:00 и с 20:00 до 00:00. Следовательно, необходимо предоставить временные интервалы доступа с 00:00 до 08:30 (№ 1) и с 19:30 до 23:59 (№ 2).

Создайте зону «Смена 3».

В третий день смены необходимо дать доступ только с 00:00 до 08:30. После установки времени нажмите иконку «Передать временные критерии» в аппаратуру.

4. Создание графиков доступа

2.1. Создайте недельный график доступа. Для этого необходимо перейти в раздел «Недельные графики».

По умолчанию существует два встроенных недельных графика:

– «Доступ запрещен»;

– «Доступ разрешен».

Для создания недельного графика – выберите любой график, иконку «Изменить название\описание», введите название «Стандарт неделя» и нажмите «Ок».

С понедельника по пятницу в выпадающем меню необходимо заменить зону «Никогда» на ту зону, которая была создана (Стандарт). Суббота, воскресенье и все праздники – интервал «Никогда» (доступа нет). Нажмите иконку «Передать временные критерии».

2.2. Создайте скользящий посуточный график. Для этого необходимо перейти в раздел «Скользящие посуточные графики».

По умолчанию существует один встроенный график: Доступ запрещен.

Для создания скользящего посуточного графика – выберите любой график, иконку «Изменить название\описание», введите название «Смена ночь», укажите первый день графика и нажмите «Ок».

Нажмите иконку «Добавить день» столько раз, сколько дней необходимо. В данном случае имеем 4 дня (Смена 1 – 3, день отдыха). На каждый день выберите необходимую временную зону (Смена 1 – 3, Никогда). Нажмите иконку «Передать временные критерии».

Созданные графики доступа можно присваивать сотрудникам и посетителям в разделах «Доступ сотрудников» и «Доступ посетителей».

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Консоль управления PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Перечислите способы добавления сотрудников в систему контроля и управления доступом.
2. Поясните назначение графика работы в системе контроля и управления доступом.
3. Поясните алгоритм создания графика работы.
4. Что такое именованные интервалы?
5. Перечислите типы схем организации работы сотрудников.
6. Поясните принципы создания графиков доступа.
7. Каковы отличия между графиками доступа и графиками работы?
8. Опишите процедуру регистрации персонала в Графике доступа.

Задания для самостоятельной работы

1. Добавьте в систему контроля и управления доступом PERCo-S-20 всех обучающихся вашей учебной группы.
2. Опираясь на трудовое и ведомственное законодательство, составьте в системе контроля и управления доступом PERCo-S-20 график работы дежурной смены пункта централизованной охраны, состоящей из трех человек, несущих службу круглосуточно.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Предоставление доступа
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений разграничения доступа для каждого отдела и сотрудников в системе безопасности и повышения эффективности PERCo-S-20;

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекций по теме № 2.2 «Сетевые возможности системы безопасности PERCo-S-20».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.

Учебные вопросы:

1. Программирование и настройка параметров доступа сотрудников.
2. Программирование и настройка параметров доступа посетителей.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.
2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).
3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

Каждый защищаемый объект имеет свои характерные особенности, что в свою очередь требует индивидуального подхода при проектировании на нем систем безопасности, в частности системы контроля и управления доступом. При проектировании системы контроля и управления доступом необходимо обращать внимание на категорию объекта, количество помещений, наличие или отсутствие физической охраны, постов, режим работы объекта, категории сотрудников и т. д.

Важным аспектом также является выбор и способы прокладки кабельной продукции, соединяющей элементы системы контроля и управления доступом. После проведенного анализа защищаемого объекта, проектировщик определяет задачи, которые необходимо решить для обеспечения безопасности и пропускного режима на объекте, и осуществляет обоснованный выбор всех необходимых технических средств безопасности.

Выбор варианта оборудования объекта средствами СКУД следует начинать с его обследования. При обследовании определяются характеристики значимости помещений объекта, его строительные и архитектурно-планировочные решения, условия эксплуатации, режимы работы, ограничения или, наоборот, расширения права доступа отдельных сотрудников,

параметры установленных (или предполагаемых к установке на данном объекте) средств, входящих в СКУД.

По результатам обследования определяются тактические характеристики и структура СКУД, а также составляется техническое задание на оборудование объекта СКУД.

В техническом задании указывается:

– назначение СКУД, техническое обоснование и описание системы;

– размещение составных частей системы;

– условия эксплуатации средств КУД;

– основные технические характеристики:

К ним относятся:

– пропускная способность в охраняемые зоны особенно в час-пик;

– максимально возможное число пользователей на один считыватель;

– максимальное число и виды идентификаторов;

– требования к маскировке и защите средств КУД от вандализма;

– оповещение о тревожных и аварийных ситуациях и принятие соответствующих мер по их пресечению или предупреждению;

– возможность работы и сохранения данных без компьютера или при его отказе; алгоритм работы системы КУД в аварийных и чрезвычайных ситуациях;

– программное обеспечение системы;

– требования к безопасности;

– требования к электропитанию;

– обслуживание и ремонт системы;

– требования к возможности включения системы КУД в интегрированную систему безопасности.

При этом определяются:

– количество входов/выходов и их геометрические размеры (площадь, линейные размеры, пропускная способность и т. п.);

– материал строительных конструкций; количество отдельно стоящих зданий, их этажность; количество открытых площадок;

– количество отапливаемых и неотапливаемых помещений и их расположение.

Вредное воздействие окружающей среды учитывается лишь для исполнительных устройств, считывателей и контроллеров, предназначенных для работы вне отапливаемых закрытых помещений либо в особых условиях (запыленность, повышенная влажность, отрицательная температура, агрессивная среда и т. п.).

Для надежной работы СКУД на объекте необходимо учитывать влияние электромагнитных помех, перепады напряжения питания, удаленность считывателей и контроллеров от управляющего центра, заземление составных частей системы и т. п.

В настоящее время любой крупный и особенно важный объект имеет весь набор технических средств безопасности, включающий в себя системы ОПС, ТСВ, СКУД и др.

Многообразие и разрозненность этих систем на одном объекте приводит к неэффективности их работы, трудностям в управлении и обслуживании. Объединение всех систем в единый программно-аппаратный комплекс (или другими словами создание ИСБ с общей информационной средой и единой базой данных) позволяет минимизировать капитальные затраты на оснащение объекта.

Преимущества ИБС:

– значительно сокращается аппаратная часть как за счет исключения дублирующей аппаратуры в разных системах, так и из-за увеличения эффективности работы каждой системы;

– на основе полной и объективной информации, поступающей оператору, значительно сокращается время, необходимое на принятие соответствующих решений по пресечению несанкционированного проникновения, проходу и других чрезвычайных ситуаций на объекте;

– оптимизируется необходимое число постов охраны и существенно снижаются расходы на их содержание, а также уменьшается влияние субъективного человеческого фактора;

– четко разграничиваются права доступа как своих сотрудников, так и посторонних в охраняемые помещения и к получению информации;

– автоматизируются процессы взятия, снятия охраняемых помещений, включения телевизионных камер, контроля шлейфов охранно-пожарной сигнализации и т. п.

При создании ИСБ следует учитывать:

– возможность совместной синхронизации всех составляющих ИСБ устройств;

– возможность интеграции на программном, аппаратном и релейных уровнях;

– возможность организации линий связи стандартных интерфейсов (при значительной удаленности панелей систем сигнализации и управления доступом);

– состояние выходов тревоги средств сигнализации и управления доступом в различных режимах, так как отечественные и большинство зарубежных средств охранной сигнализации имеют в дежурном режиме на выходе замкнутые контакты, которые размыкаются при тревоге.

Устройства центрального управления (персональные компьютеры), являющиеся «мозгом» СКУД, рекомендуется устанавливать в отдельных служебных помещениях, защищенных от доступа посторонних лиц, например, в помещении службы безопасности или помещении поста охраны объекта.

Основные положения, в соответствии с которыми разрабатываются режимы работы всей системы безопасности, определяются руководящим составом службы безопасности, исходя из общей концепции обеспечения безопасности объекта.

Управляющие программы загружаются в центральный управляющий и вспомогательные компьютеры или контроллеры и запираются секретными кодами.

Персонал охраны, а также других служб, которые подключены к общей компьютерной сети, не должен иметь доступа к программным средствам и возможности влиять на установленные режимы работы, за исключением лиц ответственных за данные работы.

При объединении компьютеров в сеть целесообразно разделять функциональные возможности среди пользователей сети и в соответствии с этим размещать компьютеры в помещениях объекта.

Методические указания по отработке учебных вопросов

1. Программирование и настройка параметров доступа сотрудников

Функционал предоставления доступа – это функционал разделов «Доступ сотрудников» и «Доступ посетителей» модуля ПО «Бюро пропусков» (рис. 5.1).

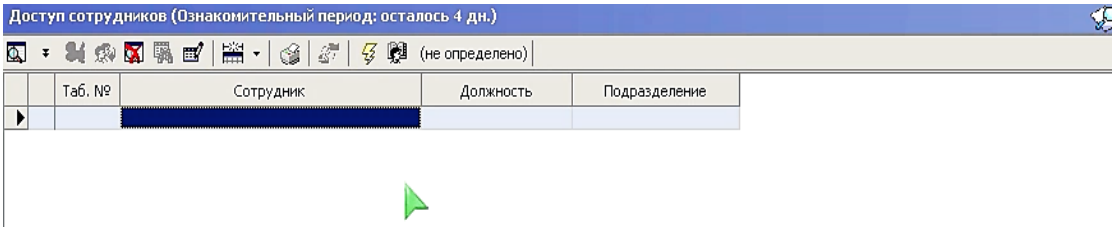


Рис. 5.1. Окно раздела доступ сотрудников

1.1. Осуществите выбор подразделения, сотрудникам которого будут выданы карты и предоставлен доступ (для этого надо выбрать подразделение, и нажать «Ок»). Если подразделения отсутствуют, то необходимо осуществить их создание в разделе Персонал/Учетные данные. В созданном подразделении определите не менее трех сотрудников.

В разделе будут видны сотрудники без карты и прав доступа и сотрудники с предоставленной картой, например, импортированной из файла Excel, но без прав доступа. В дальнейшем, в разделе доступ сотрудников и доступ посетителей значок в первом столбце будет означать сотрудника с картой доступа, но без прав, переданных в контроллеры.

1.2. Для выдачи карты доступа выберите сотрудника и нажмите иконку «Выдать карту». Панель предоставления карты доступа показана на рис. 5.2.

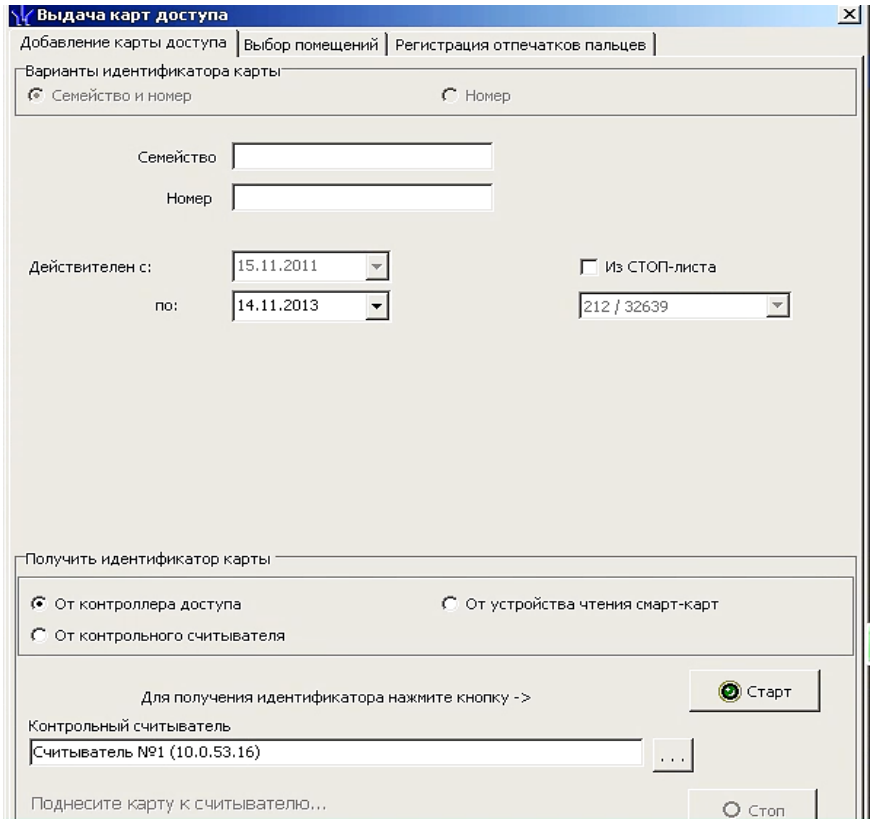


Рис. 5.2. Окно выдачи карт доступа

В подразделе «Добавление карт доступа» существует 4 варианта, как выдать карту:

– ввести вручную семейство и номер карты. Также вводится срок, когда карта будет действительна;

– получить идентификатор карты от контроллера доступа. Для этого выбрать соответствующую функцию и нажать иконку «Выбрать считыватель контроллера». После этого необходимо выбрать считыватель (с использованием которого будет добавлена карта), нажать «Ок» и «Старт». Далее поднести карточку к выбранному считывателю;

– получить идентификатор карты от контрольного USB считывателя;

– получить идентификатор карты от устройства чтения смарт-карт, в случае использования карт Mifire.

1.3. Осуществите выдачу карт с использованием имеющихся считывателей.

В разделе «Выбор помещения» следует выбрать те помещения, куда сотрудник будет иметь доступ.

В разделе «Помещения и устройства» находятся все помещения в которые разрешен доступ сотруднику. Здесь можно настроить права доступа к каждому из устройств помещений. Для этого следует установить курсор на обозначение контроллера, который требуется настроить. Справа появляется окно настройки параметров доступа (рис. 5.3).

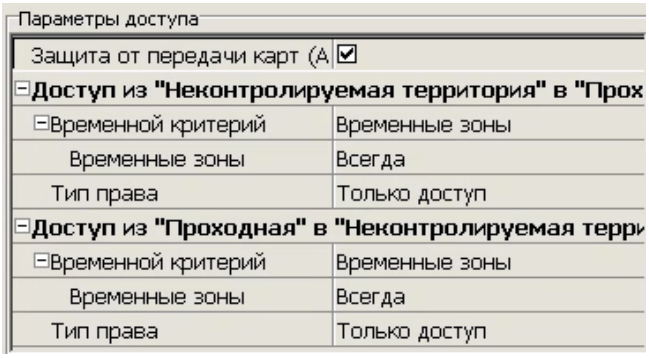


Рис. 5.3. Окно настройки параметров доступа

Ознакомьтесь с имеющимися параметрами доступа.

В разделе имеется возможность включения или выключения параметра «Защита от передачи карт».

В любом направлении (из неконтролируемой территории и в неконтролируемую территорию) существует возможность выбрать различные критерии доступа. Существует 4 критерия доступа в помещения:

– временные зоны;
– недельные графики;
– скользящие посуточные графики;
– скользящие понедельные графики доступа.

1.4. Осуществите установку одного из критериев, например, «Недельные графики». Для этого типа временного критерия определите график «Стандарт». Аналогичную операцию проделайте для доступа в обратном направлении.

1.5. Проделайте эти операции для всех устройств.

1.6. Установите для контроллеров тип права («Только доступ», «Доступ с постановкой на охрану» и т. п.).

После предоставления прав на помещения необходимо передать эти права в контроллеры. Для этого необходимо нажать иконку «Передача карт в аппаратуру». Здесь необходимо выбрать один из 4 вариантов:

– «Всей системы» – передача всех параметров доступа и карт доступа в контроллеры;
– «Все измененные» – передача изменений с момента последней передачи;
– «Всех сотрудников»;
– «Текущего сотрудника».

Осуществите передачу для «Текущего сотрудника» в аппаратуру.

1.7. Установите в разделе «Конфигуратор», в параметрах каждого считывателя критерий «Контроль времени» в положение «Жесткий» для того, чтобы аппаратура контролировала графики доступа.

Если все сотрудники подразделения имеют аналогичные права,

необходимо осуществить копирование прав доступа.

1.8. Осуществите копирование прав доступа.

Для этого в разделе «Доступ сотрудников» надо выбрать сотрудника с картой и правами доступа, нажать иконку «Копирование прав доступа». Выбрать сотрудников, которым будут скопированы права, выбрать тип копирования («Полная замена прав доступа») и нажать иконку «Копировать». Права первой карты копируются на остальные.

1.9. Осуществите групповое предоставление прав доступа.

Для этого выберите любого сотрудника. Присвойте сотруднику идентификатор и право на помещение. Нажмите иконку «Групповое предоставление прав доступа» (рис. 5.4). В данной вкладке возможно сгруппировать все контроллеры по типу.

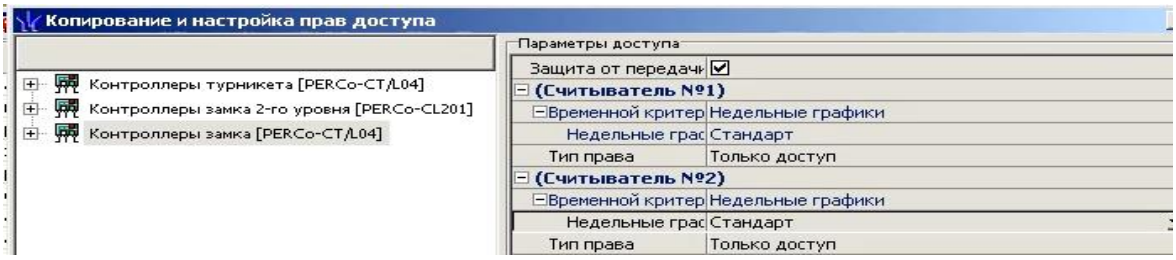


Рис. 5.4. Окно копирования и настройки прав доступа

На каждую группу контроллеров (3 группы) можно настроить параметры доступа («Временной критерий», «Тип права»). Групповое предоставление права доступа работает на любом количестве контроллеров в группе. Нажмите «Ок».

Для загрузки карт в контроллеры нажмите иконку «Передача прав доступа», и с данного момента по этим картам можно получать доступ к контролируемым помещениям. Аналогично происходит предоставление доступа посетителям.

2. Программирование и настройка параметра доступа посетителей

2.1. Перейдите в раздел «Доступ посетителей».

2.2. Нажмите иконку «Выдать идентификатор». Введите ФИО посетителя и нажмите иконку «Задать» для предоставления карты. Введите семейство и номер карты, измените срок действия карты.

2.3. Перейдите во вкладку «Выбор помещений» и задайте те помещения, куда посетитель будет иметь доступ. Нажмите «ОК». После введения всех данных необходимо нажать «Сохранить».

2.4. Задайте параметры доступа для контроллеров (рис.5.5). После настройки параметров доступа нажмите иконку «Сохранить».

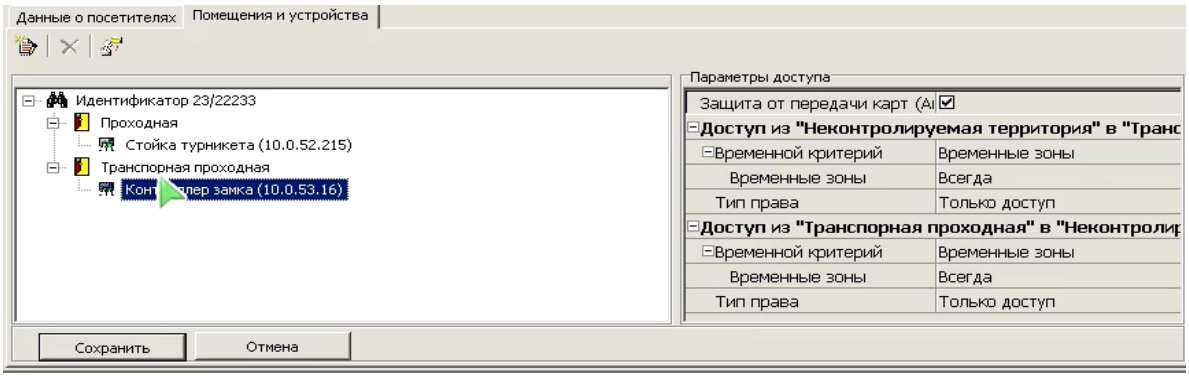


Рис. 5.5. Окно настройки помещений и устройств

Для передачи прав доступа в контроллеры необходимо нажать иконку «Передать права доступа гостей», выбрать соответствующий параметр, и нажать «Ок».

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Консоль управления PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Поясните технологию программирования и настройки параметров доступа сотрудников и посетителей.
2. Какие идентификаторы могут быть внесены в систему контроля и управления доступом PERCo?
3. Как осуществляется групповое предоставление прав доступа в системе PERCo-S-20?
4. Как осуществляется копирование прав доступа в системе PERCo-S-20?
5. Что программируется во вкладке «Параметры доступа»?
6. Перечислите критерии доступа в помещение.

Задания для самостоятельной работы

1. Отразите в рабочих тетрадях план режимного объекта с разбиением на зоны доступа (зон доступа должно быть не менее 5). Поясните принцип разграничения зон доступа.
2. Составьте график с временными интервалами доступа в определенные охраняемые зоны из задания № 1.

ПРАКТИЧЕСКАЯ РАБОТА № 6

Формирование отчетов
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений формирования отчетов для каждого отдела и сотрудника в системе безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекций по теме № 2.3 «Особенности построения, состав и структурные схемы автономной, централизованной и универсальной СКУД».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Подготовить экспликацию объекта в формате *.jpeg.

Учебные вопросы:

1. Изучение функций модуля «Дисциплинарные отчеты» программного обеспечения системы PERCo-S-20 для формирования отчетов.
2. Изучение функций модуля «Учет рабочего времени» программного обеспечения системы PERCo-S-20 для формирования отчетов.
3. Формирование оправдательного документа.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.

2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

В деятельности каждого предприятия неизбежны процессы формирования разнообразной отчетности для внутренних и внешних пользователей. Для крупных предприятий, как правило, характерны высокая трудоемкость, низкая формализация, недостаточная оперативность и недостоверность предоставляемой отчетной информации.

Каждое структурное подразделение крупных предприятий зачастую формирует собственный пакет отчетности, при этом состав показателей в отчетах разных подразделений может пересекаться, но это никем не контролируется. При смене руководителей состав отчетности подразделений обычно пересматривается, что приводит к появлению новых форм, но не отменяет уже существующих. В итоге отчетность предприятия неуклонно разрастается и становится избыточной, повышается трудоемкость процессов ее формирования, однако информативность отчета при этом не возрастает.

Низкая формализация, безусловно, способствует хаотичности процессов формирования отчетности и умышленному искажению соответ-

ствующей информации. Повышение трудоемкости при ограниченном штате сотрудников и сохранении старых методов формирования отчетности неизбежно приводит к снижению оперативности. Сам процесс доставки информации лицу, принимающему решения (конечному пользователю отчета), может состоять из множества звеньев, каждое из которых чревато задержками и искажением информации.

Разумеется, предприятие может успешно работать и даже развиваться, несмотря на перечисленные проблемы. Однако их воздействие на эффективность и конкурентоспособность предприятия, по мере его укрупнения, становится все более негативным. Именно поэтому руководство осознает необходимость реорганизации процессов формирования отчетности предприятия, возлагая большие (часто завышенные) надежды на автоматизацию. Кроме того, одной из причин модернизации формирования отчетности часто является внедрение на предприятии информационной системы управления. Инициаторы данных проектов не всегда осознают, что реформирование и автоматизация отчетности тянут за собой шлейф новых взаимосвязанных задач.

Инициаторами проектов реформирования и автоматизации отчетности предприятия чаще всего выступают руководители подразделений, использующих отчетность в своей деятельности, либо топ-менеджеры компании. Руководителем проекта обычно назначается один из его инициаторов или глава информационной службы.

Приступая к реформированию, прежде всего следует пересмотреть состав формируемой отчетности, так как автоматизации процесса должны предшествовать его анализ и оптимизация. Изменить состав государственной отчетности предприятие не может. Поэтому оптимизация возможна за счет пересмотра состава управленческой отчетности. Необходим выбор таких отчетов, которые наиболее соответствуют потребностям менеджеров предприятия в принятии управленческих решений. Критерием адекватности является экономическая эффективность формирования данного отчета, определяемая соотношением затрат на создание отчета и эффектов, получаемых от его использования в принятии управленческих решений. Разумеется, такая точная оценка возможна лишь гипотетически. Если затраты на формирование отчета приблизительно определить можно, то сопоставить его с конкретным управленческим решением, а тем более оценить эффект от использования отчета на практике достаточно трудно. Подобный анализ помогает выявить бесполезность многих отчетов на первой же итерации, при этом выясняется, что пользователи даже не могут сопоставить их с принимаемыми управленческими решениями. Как правило, данная работа способствует сокращению числа отчетов, однако иной раз провоцирует и появление некоторых новых форм. В целом же этот этап – один из самых сложных в проекте, так как предполагает знания в разных предметных областях, связанных с деятельностью предприятия, требует учета

его специфики и согласования интересов всех задействованных сторон. Неоценима роль инициаторов, которые могут поддержать членов проектной группы в спорных ситуациях, неизбежно возникающих при взаимодействии с руководителями различных структурных подразделений. Для успешного разрешения производственных конфликтов целесообразно привлекать внешних экспертов и консультантов, которые в наименьшей степени подвержены влиянию заинтересованных лиц и могут высказать объективное мнение. Основными участниками работ, проводимых на этом этапе, являются сотрудники функциональных подразделений, которым отчетная информация требуется в повседневной деятельности.

Согласовав целевой пакет формируемой отчетности, нужно определить разумные границы его автоматизации. Необходимо учитывать два основных фактора. Во-первых, соотношение затрат на автоматизацию и на формирование отчетности «вручную». Если автоматизация может окупиться в приемлемый период, то она целесообразна, иначе требуется более глубокий анализ с учетом других факторов. Во-вторых, принимаются во внимание требования к достоверности информации. Вследствие автоматизации повышается формализация процессов, что содействует прозрачности функционирования организации и улучшению качества отчетной информации. При этом целевой пакет формируемой отчетности разделяется на автоматизируемую и неавтоматизируемую части. Работы на данном этапе выполняются совместно сотрудниками организаций и ИТ-специалистами, а сам процесс может носить итеративный характер. Согласование состава автоматизируемой отчетности может привести к пересмотру формируемой отчетности.

На следующем этапе целевой пакет автоматизируемой отчетности структурируется на основе ряда интересуемых показателей и признаков. Такое упорядочивание позволяет выявить повторное использование показателей и признаков в различных отчетах. Кроме того, выделенная структура облегчает поиск и определение источников данных (информационных систем предприятия, в том числе системы контроля и управления доступом), на основе которых будут рассчитываться значения показателей отчетности. При этом по каждому из них нужно выделить один источник, иначе какой-либо показатель в различных отчетах будет иметь разные значения, что недопустимо для качественной отчетной информации.

Нередко источник данных по показателю для автоматизации отчета определить не удается. Тогда необходимо выбрать один из двух вариантов дальнейших действий. Первый позволяет получить нужный источник данных, изменив (расширив) функциональность информационных систем предприятия. Второй вариант заставляет отказаться от автоматизации или формирования отчета в прежнем виде. Проработка источников данных показателей отчетности выявит необходимые источники и определит требо-

вания по изменению функциональности информационных систем предприятия.

К сожалению, работы по автоматизации отчетности часто относят на последние этапы внедрения проекта, когда основные настройки информационной системы уже выполнены, и многие требования отчетности к ней оказываются неучтенными. В такой ситуации можно предложить только два непопулярных решения проблемы.

В одном случае нужно перенастраивать информационную систему, что влечет срыв сроков и перерасход бюджета проекта. Либо придется разрабатывать отчетность на информационной системе, не настроенной для этих целей, следовательно, получить низкое качество отчетов и трудоемкое сопровождение. Поэтому требования отчетности необходимо формулировать еще до начала настройки информационной системы, а на последние этапы проекта относить только разработку и тестирование отчетов.

Если источники данных согласованы, то остаются еще два этапа: изменение функциональности информационных систем, а затем разработка и тестирование отчетов. Естественно, что первый из них требует не только выполнения технических настроек программного обеспечения, но и изменения определенных бизнес-процессов предприятия.

Для крупных предприятий, применяющих в своей деятельности различные информационные системы, в целях автоматизации отчетности эффективно использование технологии хранилища данных, специализированных средств генерации отчетов и аналитики. В настоящее время большинство производителей ERP-систем мирового уровня в линейке своих программных продуктов предлагают все необходимые для этого компоненты.

Методические указания по отработке учебных вопросов

Формирование отчетов в программном обеспечении (консоли управления) системы PERCo-S-20 осуществляется в модулях «Дисциплинарные отчеты» и «Учет рабочего времени».

1. Изучение функций модуля «Дисциплинарные отчеты» программного обеспечения системы PERCo-S-20 по формированию отчетов

Модуль «Дисциплинарные отчеты» позволяет автоматизировать формирование отчетов о времени присутствия сотрудников на рабочем месте и контролировать нарушение трудовой дисциплины. В состав данного модуля входят два раздела: «Время присутствия»; «Дисциплина труда».

1.1. Изучите функции раздела «Время присутствия».

Для этого необходимо запустить консоль управления PERCo-S-20, открыть модуль «Дисциплинарные отчеты», раздел «Время присутствия».

Изучите и зафиксируйте в рабочих тетрадях назначение иконок панели инструментов (рис. 6.1).

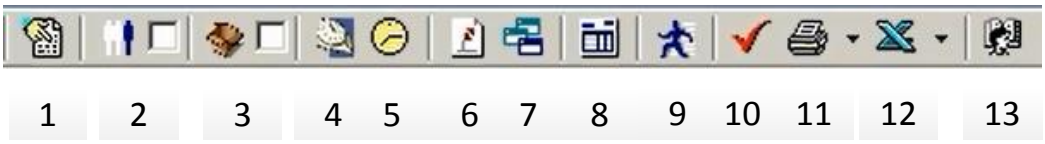


Рис. 6.1. Пиктограммы панели инструментов

Назначение пиктограмм панели инструментов:
1. «Период отчета».
2. «Выборка по персоналу».
3. «Выборка по помещениям».
4. «Точность до секунд».
5. «График работы».
6. «Сокращенный показ ФИО».
7. «Вид отчета».
8. «Настройка столбцов таблицы».
9. «Показать время входов и выходов».
10. «Применить».
11. «Вывод на печать».
12. «Экспорт данных».
13. «Выбор подразделения».

Данный раздел позволяет формировать отчеты следующих видов: «Время присутствия» и отчет «Время прихода – время ухода» (рис. 6.2).

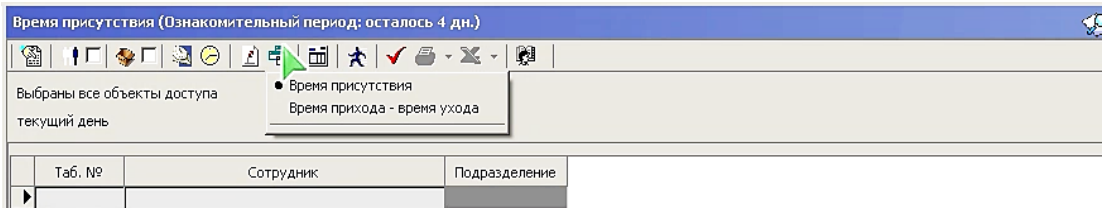


Рис. 6.2. Окно раздела времени присутствия

Рассмотрим формирование отчета «Время присутствия».

Для формирования отчета необходимо выбрать подразделение (иконка 13) и нажать «Ок». Далее необходимо выбрать периода отчета (иконка 1). Это может быть один из заранее установленных периодов, либо период, указываемый пользователем. Выберите из списка «указанный период». Задайте период времени и нажмите иконку «Применить». Изучите сформированный отчет.

Существует возможность по каждому сотруднику посмотреть время входов/выходов. Для этого нажмите иконку «Показать время входов и выходов». Отображаются все входы и выходы по каждому сотруднику. Также есть возможность показать график работы сотрудника, для этого надо нажать иконку «График работы».

Изучите оставшиеся функциональные элементы раздела «Время присутствия».

Выборка по персоналу. Нажмите иконку «Выборка по персоналу». Здесь можно осуществить выбор нужного сотрудника, либо выбрать группу сотрудников с зажатой клавишей Ctrl. В результате сформируется отчет по конкретным сотрудникам.

Выборка по помещениям. Нажмите иконку «Выборка по помещениям». В данном разделе существует возможность сделать выборку по помещениям, например, посмотреть время, проведенное в конкретном помещении сотрудником.

Просмотр времени с точностью до секунды (иконка «Точность до секунд»).

Просмотр сокращенного ФИО (иконка «Сокращенный показ ФИО»).

Отображение определенных дней в отчете (иконка «Настройка столбцов таблицы»).

Вывода на печать и экспорт в форматы MS Excel и OpenOffice (иконки «Вывод на печать» и «Экспорт данных»).

1.2. Раздел «Дисциплина труда».

Войдите в раздел «Дисциплина труда». Отчеты в данном разделе формируются аналогично разделу «Время присутствия». Имеются следующие виды отчетов (иконка «Вид отчета»):

- «Опоздания»;
- «Уходы раньше»;
- «Отсутствующие»;
- «Все нарушители»;
- «Отсутствующие на текущий момент»;
- «Время отсутствия»;
- «Присутствующие на текущий момент»;
- «Время после работы»;
- «Время до начала работы»;
- «Нарушение дисциплины в течение рабочего дня».

Выберите подразделение, период отчета, вид отчета и сформируйте таблицу, нажав иконку «Применить». Возможность просмотра времени входов/выходов и графика работы. Функциональные элементы раздела «Дисциплина труда» аналогичные разделу «Время присутствия».

2. Изучение функций модуля «Учет рабочего времени» программного обеспечения системы PERCo-S-20 по формированию отчетов

Модуль «Учет рабочего времени» обеспечивает автоматизацию учета рабочего времени на предприятии с возможностью сформировать табель учета рабочего времени по стандартным формам Т12 и Т13.

В состав данного модуля входят следующие разделы: «Отчеты»; «Журнал отработанного времени»; «Оправдательные документы»; «Временная замена учетных данных».

2.1. Изучите функции раздела «Отчеты».

Раздел «Отчеты» позволяет сформировать отчет помесячно за определенное подразделение (рис. 6.3). Для этого выберите подразделение и период отчета. Период устанавливается только помесячно. После нажмите иконку «Обновить данные». Сформированный отчет отображает рабочее время присутствия сотрудника в рамках графика работы по дням месяца.

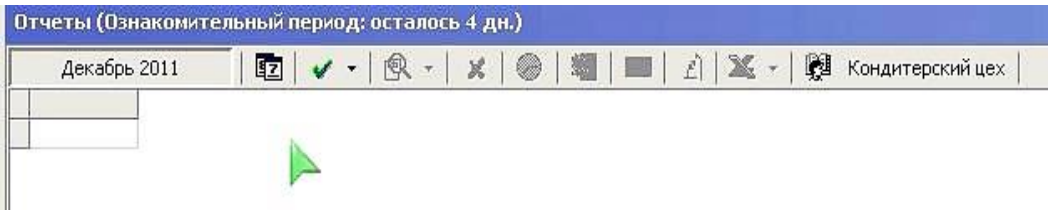


Рис. 6.3. Окно раздела отчеты

Существует возможность просмотра графика работы сотрудника на каждый день. Также есть возможность просмотра времени с точностью до секунды и отображение времени в часах и долях часа. Также имеется возможность просмотра сокращенного ФИО, отчетовТ-12 и Т-13 и простого и экспорта данных отчетов в формат MS Excel.

Осуществите двойной клик на отработанное время – появится таблица просмотра времени входов/выходов.

2.2. Изучите функции раздела «Журнал отработанного времени».

Журнал рабочего времени формируется по выбранному подразделению и определенному временному периоду (рис. 6.4).

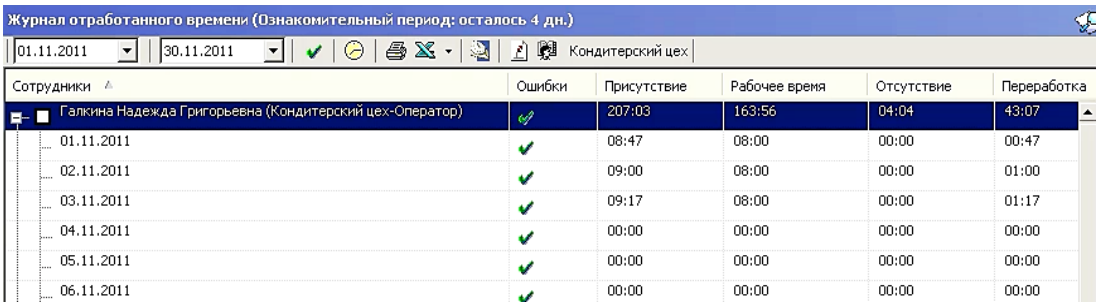


Рис. 6.4. Окно журнала отработанного времени

По каждому сотруднику есть возможность просмотра данных по времени присутствия, рабочему времени, отсутствии, переработке и работы ночью за конкретный день или период. Графа «Ошибки» показывает наличие некорректных событий, например, двойных входов или выходов. Двойным кликом по строке вызывается дополнительное окно вхо-

дов/выходов. Двойной вход или выход из одного и того же помещения подряд является некорректным событием для программы. Двойной клик по значку в столбце «Участвует в расчетах» удаляет событие из расчета или возвращает. Существуют возможности просмотра: графика работы сотрудника на каждый день; времени с точностью до секунды; сокращенного ФИО, а также есть иконки вывода на печать и экспорта в форматы MS Excel и OpenOffice.

3. Формирование оправдательного документа

Оправдательный документ позволяет засчитывать как рабочее время, проведенное не на территории предприятия, т. е. то рабочее время, которое автоматически не учитывается в отчетах. Например, в определенные дни у сотрудника могут отсутствовать входы и выходы. В этом случае необходимо учесть данное время в отчете как рабочее.

В разделе «Оправдательные документы» необходимо выбрать подразделение, в котором числится сотрудник, и период, который захватывает время служебной командировки (рис. 6.5).

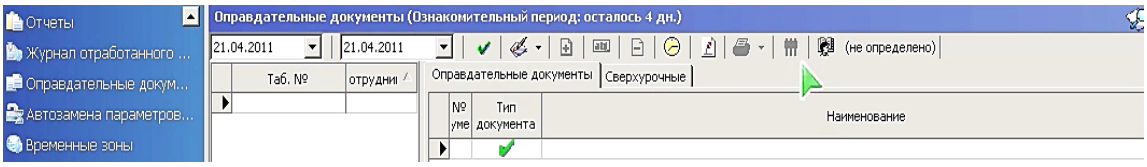


Рис. 6.5. Окно раздела «Оправдательные документы»

Далее – выбрать сотрудника и нажать иконку «Добавить документ». Ввести номер документа, дату создания документа, из выпадающего списка типов оправдательных документов выбрать необходимый, определить период документа, и нажать иконку «Сохранить».

Добавив оправдательный документ, нажать иконку «Сохранить» (с логотипом дискеты). Далее необходимо перейти в раздел «Отчеты», и обновить данные отчета. В отчете зеленым цветом отображается предоставленный оправдательный документ.

Расшифровка индексов: фактически отработанное время по графику, индекс оправдательного документы, время, которое будет учтено как рабочее. Аналогичным образом учитываются все остальные оправдательные документы.

В справочнике оправдательных документов отображаются все встроенные в программу оправдательные документы. Код документа, Цифровой код документа, добавляется к рабочему времени и учитывается по календарным дням. Если параметр «Добавляется к рабочему времени» не установлен, то время документа отображается, но не учитывается при

расчетах рабочего времени. Установленный параметр «Учитывается по календарным дням» не дает возможности предоставить документ на период менее полного дня. Также существует возможность добавления, изменения и удаления оправдательных документов. Аналогичным функционалом обладает справочник документов на сверхурочные. Существуют встроенные документы.

Дополнительный функционал: «Сверхурочные в праздничные и выходные дни» – если параметр установлен, то оправдательный документ охватывающий праздничный день или выходной будет засчитан. Также существует возможность массового добавления оправдательных документов.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты ПО «Консоль управления PERCo-S-20» по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. С какой целью в системе создаются отчеты?
2. Поясните назначение модулей «Дисциплинарные отчеты» и «Учет рабочего времени».
3. Поясните разницу между отчетами, формируемыми в разделах «Отчеты» и «Время присутствия».
4. Опишите этапы создания отчета.
5. Поясните необходимость создания оправдательных документов.

Задания для самостоятельной работы

1. Изучить и законспектировать в рабочей тетради порядок оформлении табеля учёта рабочего времени по формам Т-12 и Т-13.
2. Законспектировать в рабочей тетради состав отчетной информации, формирующийся системой контроля и управления доступом.

ПРАКТИЧЕСКАЯ РАБОТА № 7

Видеоидентификация
в системе безопасности и повышения эффективности PERCo-S-20

Цели занятия:

Образовательные: формирование умений конфигурирования модуля «Видеоидентификация» в системе безопасности и повышения эффективности PERCo-S-20.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формированию у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекций по теме № 2.4 «Конфигурирование оборудования, настройка параметров и реакций в системе».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Подготовить экспликацию объекта в формате *.jpeg.

Учебные вопросы:

1. Создание конфигурации видеоверификации.
2. Настройка параметров видеоточки.
3. Настройка отображаемых данных сотрудников.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.

2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

Системы видеонаблюдения (англ. CCTV – Closed Circuit TeleVision – Системы замкнутого телевидения) или *системы охранного телевидения* (СОТ) предназначены для организации видеонаблюдения на объектах.

Системы CCTV строятся в соответствии с требованиями безопасности, физическими характеристиками объекта и финансовыми возможностями Заказчика.

Стандартными ***задачами***, стоящими перед видеонаблюдением на любом объекте, являются:

– текущее наблюдение;

– работа с архивом видеозаписей;

– дистанционный просмотр текущего изображения и архива;

– запись видеоизображения по детектору движения, а также при срабатывании охранных датчиков.

На крупном объекте к стандартным задачам добавляются следующие:

– интеграция с системой охранной и пожарной сигнализации;

– интеграция с аппаратно-программным комплексом системы контроля и управления доступом;

– масштабируемость и модернизация системы видеонаблюдения при необходимости;

– текущее наблюдение и управление всей системой из одной точки, в том числе организация видеонаблюдения через интернет.

Комплекс CCTV представляет собой сложную техническую систему, состоящую из видеокамер, объективов, мониторов, регистраторов и другого дополнительного оборудования.

При классификации систем видеонаблюдения используют различные классификационные признаки.

В зависимости от типа используемого оборудования системы видеонаблюдения делят на аналоговые и цифровые.

Аналоговые системы видеонаблюдения используются там, где необходимо организовать видеонаблюдение в небольшом количестве помещений и сигнал с видеокамер записывать на видеомагнитофон: в небольших офисах, складских помещениях, автостоянках и других объектах. Основу аналоговых систем видеонаблюдения составляют камеры видеонаблюдения. Эти камеры представляют собой оптические устройства, ПЗС-матрицы которых формируют видеосигнал из светового потока, проходящего через объектив и группу линз и попадающего на матрицу. Аналоговые видеокамеры можно модернизировать, используя блок преобразования аналогового видеосигнала в цифровой. Такие модернизированные видеокамеры можно использовать и в цифровых системах видеонаблюдения. В аналоговых системах видеонаблюдения используются также видеомониторы, видеокоммутаторы, видеоквадраторы, видеомультиплексоры, детекторы движения, видеомагнитофоны и другие устройства.

Преимущества аналоговых систем видеонаблюдения заключаются в невысокой стоимости оборудования, высокой надежности, простоте конструкции и эксплуатации, что позволяет использовать их персоналом невысокой квалификации.

Недостатками таких систем принято считать необходимость постоянного обслуживания (замена видеокассет, архивирование отснятого материала, обслуживание видеомагнитофонов) и некоторую функциональную ограниченность, обусловленную использованием аналоговой аппаратуры.

Цифровые системы видеонаблюдения используются для обеспечения безопасности особо ответственных или территориально-распределенных объектов. Эти системы могут интегрироваться в комплексные системы безопасности.

Преимущества цифровой записи очевидны: это неограниченное время хранения записи, практически мгновенный доступ к любому сюжету из архива, возможность простой передачи видеоинформации по локальным и глобальным вычислительным сетям, возможность обработки кадров с использованием различных алгоритмов фильтрации и повышения качества изображения с последующей распечаткой на обычном принтере. При этом, аппаратная часть цифровых систем видеонаблюдения сокращается до трех компонентов: цифровой видеокамеры, платы видеоввода (видеозахвата,

видеообработки) и персонального компьютера со специальным программным обеспечением (видеосервер).

Видеокамера – это устройство, которое преобразует оптическое изображение наблюдаемого объекта (сцены) в электрический видеосигнал определенного стандарта. Видеокамера является важнейшим элементом системы, так как именно с нее в систему поступает первичная информация об объекте и именно ее характеристиками определяется качество изображения в целом. Видеокамера состоит из светочувствительного устройства (фотоэлектрического преобразователя), устройства формирования видеосигнала, видеоусилителя, системы автоматической регулировки уровня сигнала и источника питания (рис. 7.1).

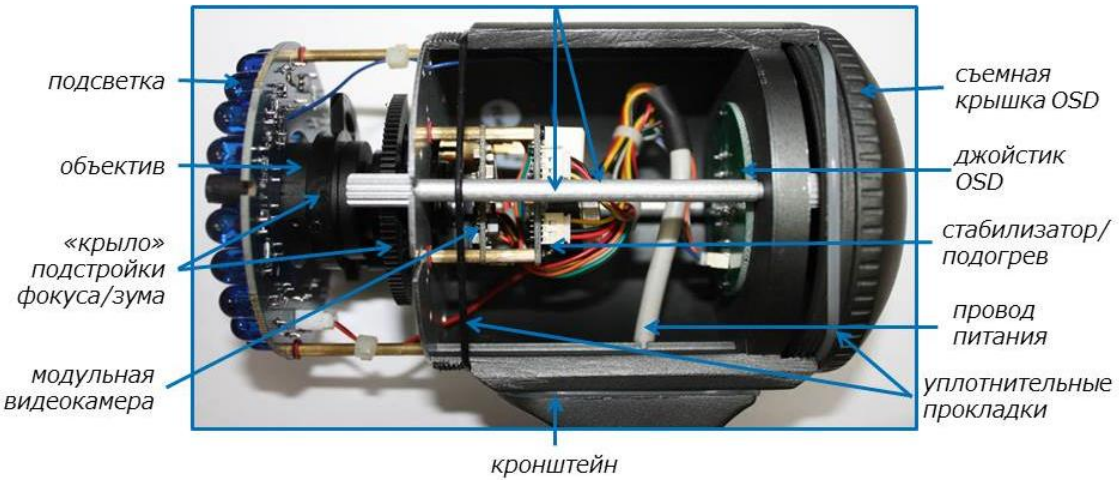


Рис. 7.1. Функциональная схема видеокамеры

Конструктивно видеокамера представляет собой плату с электронными компонентами, на которой размещены чувствительный элемент – матрица, выполненная на приборах с зарядовой связью (ПЗС-матрица), и объектив. Более простые (и, соответственно, более дешевые) видеокамеры оснащаются, как правило, простейшими встроенными объективами, более дорогие – сменными объективами с улучшенными характеристиками и широкими функциональными возможностями.

В качестве светочувствительного устройства в большинстве систем ввода изображений используются ПЗС-матрицы, состоящие из приборов с зарядовой связью. Принцип работы ПЗС-матрицы состоит в следующем. Каждый светочувствительный элемент на основе кремния обладает свойством накапливать заряды пропорционально числу попавших на него фотонов. Таким образом, за некоторое время (время экспозиции) получается двумерная матрица зарядов, пропорциональных яркости исходного изображения. Накопленные заряды строка за строкой передаются на выход матрицы. Используются также КМОП-матрицы (комплементарная структура

металл-оксид-полупроводник), имеющие более высокую скорость считывания, что важно при формировании изображения высокого качества.

Видеокамеры различают:

– корпусные и бескорпусные;
– черно-белого и цветного изображения;
– обычной и повышенной чувствительности;
– обычного и высокого разрешения;
– для внутреннего и наружного наблюдения;
– для скрытого наблюдения.

Качество видеокамеры определяется целым рядом *показателей*.

Видеоаналитика – аппаратно-программное обеспечение или технология, где используются методы компьютерного зрения для автоматизированного сбора данных на основании анализа потокового видео (видеоанализа). Видеоаналитика опирается на алгоритмы обработки изображения и распознавания образов, позволяющие анализировать видео без прямого участия человека. Видеоаналитика используется в составе интеллектуальных систем видеонаблюдения, управления бизнесом и видеопоиска.

В зависимости от целей, ***видеоаналитика может реализовать как одну, так и несколько базовых функций***:

1) *Обнаружение объектов*. Как правило, обнаружение объектов в поле зрения камеры производится при помощи видеодетекторов движения. Основное отличие видеоаналитики от ИК-датчиков движения состоит в возможности локализации (выделении) и независимого анализа сразу нескольких объектов. Если движение не является достаточным признаком для локализации объекта в кадре, то обнаружение может производиться при помощи шаблонов. Например, обнаружение лиц людей, номерных знаков автомобилей или обнаружение малоподвижных морских целей.

2) *Слежение за объектами*. Алгоритмы слежения (сопровождения) позволяют получить частную траекторию движения объекта как в поле зрения одной камеры, так и обобщенную траекторию по данным сразу нескольких камер. Слежение необходимо, чтобы проанализировать поведение объекта по его траектории, например, определить движение человека против потока или движение с повышенной скоростью. Кроме этого, слежение необходимо для исключения повторных срабатываний систем видеоаналитики на одни и те же объекты. Профессиональные системы работают по правилу «один тревожный объект – одно срабатывание» для достижения высокой продуктивности оператора.

3) *Классификация объектов*. Некоторые системы видеоаналитики классифицируют объекты для фильтрации оперативных уведомлений или результатов поиска. Например, типовой классификатор объектов, используя признаки формы и абсолютные размеры, распределяет объекты на группы: человек, группа людей, транспортное средство. Более сложные

классификаторы в системах видеоаналитики могут определить пол или возвратную группу человека.

4) *Идентификация объектов*. Идентификация объектов является наиболее сложным компонентом систем видеоаналитики. Современные системы позволяют идентифицировать людей по биометрическим признакам лица или транспортные средства – по номерным знакам. Идентификация может быть реализована при помощи дополнительных средств за рамками видеоаналитики: на основе отпечатков пальцев, банковской карты, билета, пропуска или идентификатора мобильного устройства.

5) *Обнаружение (распознавание) ситуаций*. Видеоаналитика позволяет не только выделять объекты из потокового видео, но и распознавать тревожные ситуации на основе анализа поведения данного объекта, что не дает сделать обычная система видеонаблюдения. Также ситуационная видеоаналитика может автоматически детектировать пересечение сигнальной линии, падение людей, запрещенную парковку и возникновение пожара.

Методические указания по отработке учебных вопросов

1. Создание конфигурации видеоверификации

Сетевой модуль «Видеоидентификация» устанавливается на рабочее место сотрудника службы охраны и позволяет производить идентификацию карты доступа, сравнивая личность проходящего сотрудника или изображение с видеокамеры и его фото, хранящееся в базе данных системы. Сетевой модуль позволяет отображать информацию о владельце предъявленной карты доступа, отображать и записывать видеоинформацию, полученную с выбранных камер. Модуль содержит раздел «Журнал верификации», который автоматически ведет запись для дальнейшего просмотра всех действий операторов, информации о предъявлении карт доступа, видеоинформации. Программный модуль «Видеоидентификация» позволяет одновременно контролировать до 4 точек прохода и 4 камер видеонаблюдения на одну созданную конфигурацию. На одном компьютере создавать несколько конфигураций верификации по 4 точки прохода и на нескольких мониторах запускать несколько консолей с различными конфигурациями, что дает возможность верифицировать более 4 точек. Для возможности работы модуля PERCo0SM09 с видеокамерами требуется установка модуля PERCo-SM01 «Администратор».

Для того чтобы начать работать с модулем, необходимо создать конфигурацию верификации. Каждая конфигурация верификации создается на той машине, на которой она будет использоваться, то есть конфигурация хранится локально.

1.1. Создайте конфигурацию верификации.

Для создания конфигурации нажмите иконку «Создать», введите название и нажмите «Ок». Первый этап – выбор считывателей, которые

необходимо контролировать (рис. 7.2).

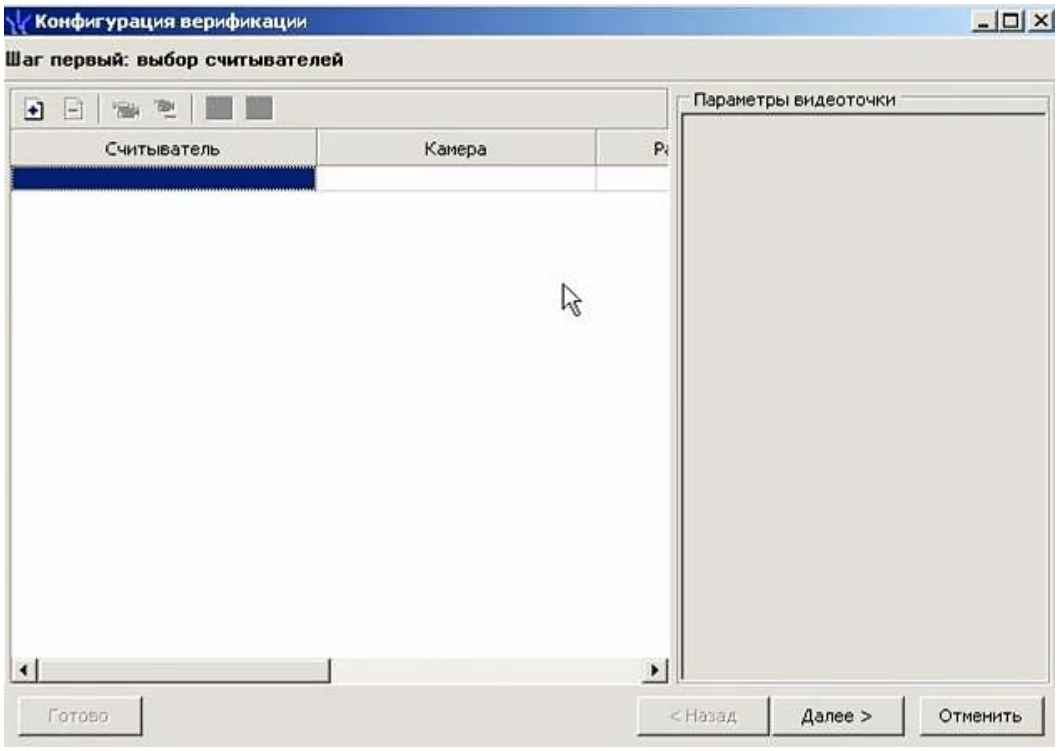


Рис. 7.2. Окно выбора считывателей

Можно выбрать до 4 считывателей. Для каждого считывателя выберите видеокамеру, и нажмите «Ок».

2. Настройка параметров видеоточки

Изучите общие параметры видеоточки:

– количество записываемых видеокадров – количество кадров видеозаписи, которые будут сохраняться в архив. По умолчанию – 5 кадров;

– частота записи видеокадров также относится к качеству видеозаписи. По умолчанию – 2 кадр/с;

– режим отображения информации – «Постоянный» и «не более чем». В первом варианте фотография будет находиться на экране до момента поднесения следующей карты к считывателю. Во втором варианте с момента поднесения карты фотография отображается определенное время;

– таймаут верификации отвечает за время, которое дается оператору для принятия решения пропускать сотрудника/ посетителя или нет. Время начинается с момента поднесения карты к считывателю. В течение всего периода турникет заблокирован, ожидая подтверждения от оператора.

Далее в системе настраиваются параметры по событиям:

– сотрудников; – посетителей; –уведомляющие.

Изучите данные параметры.

Проход. Устанавливается возможность отслеживать или не отслеживать проход, т. е. сохранять событие в журнал или не сохранять. Далее устанавливается возможность записи кадров видеокамеры в журнал верификации.

Верификация. Отвечает за подтверждение прохода. Если выбран параметр «Нет», то проход осуществляется сразу после предъявления разрешенной карты. Если параметр выбран «Да», то проход возможен только после подтверждения от оператора с максимальной задержкой открытия турникета равной таймауту верификации. При отсутствии действий от охранника (например, отсутствие на рабочем месте), проход будет автоматически разрешен при выборе параметра «Разрешить», в противном случае проход будет заблокирован. По окончании настройки всех параметров требуется нажать кнопку «Далее».

3. Настройка отображаемых данных сотрудников

Для настройки отображаемых данных сотрудников (рис. 7.3) выберите доступные текстовые данные из карточки сотрудника для отображения на мониторе охранника. Данные выбираются с использованием иконок «зеленый треугольник» (по одной позиции) и «двойной зеленый треугольник» (все позиции). Нажмите кнопку «Далее».

Настройка отображаемых данных посетителей производится аналогичным образом. После нажатия кнопки «Готово» создание конфигурации завершается.

Поднеся карточку к считывателю, видны кадры с камеры в режиме реального времени, фотография и текстовые данные из карточки.

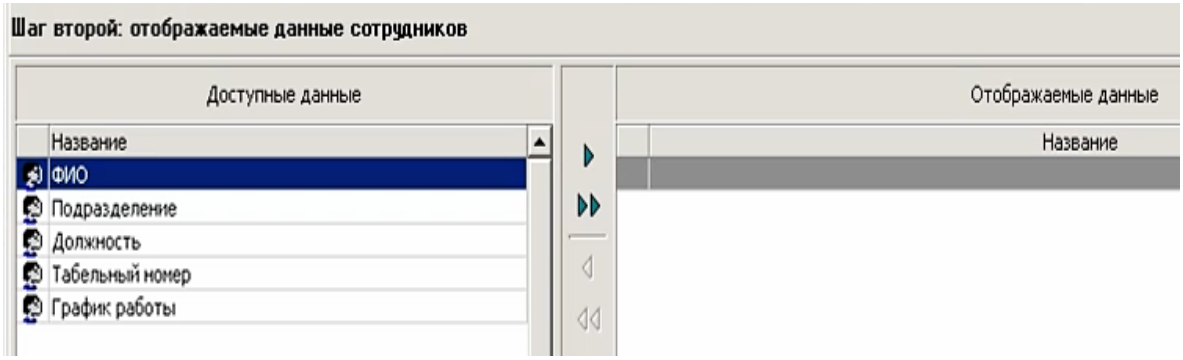


Рис. 7.3. Окно отображения данных сотрудника

Так же становятся активными кнопки «Разрешить проход» и «Запретить проход». Установка флажка «Протокол» создает в папке с программой лог файл модуля с системными событиями для отправки в сервисную службу в случае некорректной работы модуля.

В разделе «Журнал верификации» отображаются все события в текстовом виде с дополнением в виде фотографии из базы данных, кадров с

видеокамеры и текстовыми данными из карточки сотрудника.

Существует возможность выбора временного периода и различные возможности фильтрации данных, вывод в Excel и печати.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.

2. Скриншоты ПО «Видеоидентификация» по выполнении каждого этапа практических заданий с пояснениями.

3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Каково назначение и функциональные возможности видеоподсистемы системы безопасности и повышения эффективности PERCo-S-20?
2. Для чего предназначен программный модуль «Видеоидентификация»?
3. Какое количество точек прохода и камер видеонаблюдения позволяет контролировать программный модуль «Видеоидентификация»?
4. Какие условия необходимо выполнить для начала работы с модулем?
5. По каким событиям настраиваются параметры системы?
6. Из каких основных элементов состоит видеокамера?
7. Назовите основные технические параметры видеокамер.

Задания для самостоятельной работы

1. Отразите в рабочей тетради схему расположения средств видеонаблюдения совместно с системой контроля и управления доступом на объекте (отдел полиции).

2. Составьте структурную схему разработанной в первом задании системы безопасности, используя рекомендуемые условно-графические обозначения.

ПРАКТИЧЕСКАЯ РАБОТА № 8

Программирование компонентов системы безопасности
и повышения эффективности PERCo-S-20
с использованием WEB-интерфейса

Цели занятия:

Образовательные: формирование умений программирования и диагностики контроллеров системы безопасности и повышения эффективности PERCo-S-20 через WEB-интерфейс.

Развивающие: актуализация опорных знаний обучающихся по дисциплине, а также межпредметных связей; развитие внимания, памяти, логического мышления, профессиональной лексически и терминологически грамотной речи.

Воспитательные и личностно-формирующие: стимулирование активной познавательной деятельности и мотивации к самообразованию, способствование формирования у обучающихся убежденности в важности освоения рассматриваемых вопросов для практической деятельности.

Учебно-материальное обеспечение:

1. Методические рекомендации обучающимся по выполнению практической работы.
2. Лабораторный стенд «Система безопасности и повышения эффективности PERCo-S-20».

Задания обучающимся для подготовки к занятию:

1. Повторить материалы лекции по теме № 2.4 «Конфигурирование оборудования, настройка параметров и реакций в системе».
2. Ознакомиться с рекомендованной литературой.
3. Сделать запись в отчете о теме, цели, учебных вопросах и учебно-материальном обеспечении занятия.
4. Подготовить экспликацию объекта в формате *.jpeg.

Учебные вопросы:

1. WEB-интерфейс. Главная страница и разделы.
2. Добавление карт доступа.

Литература

Нормативно-правовая:

1. О безопасности : Федеральный Закон Российской Федерации от 28.12.2010 г. № 390-ФЗ.
2. О полиции : Федеральный Закон Российской Федерации от 07.02.2011 г. № 3-ФЗ (с изменениями и дополнениями).

3. ГОСТ Р 52551-2006. Системы охраны и безопасности. Термины и определения.

4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

5. Р 064-2017. Выбор и применение систем контроля и управления доступом. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с.

Основная:

1. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

2. Винокуров, С. А. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2019. – Текст : электронный.

Дополнительная:

1. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание. Книга 1 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. 4-е изд./ В. Г. Олифер, Н. А. Олифер. – Санкт_ Петербург : Питер, 2010. – 944 с. – Текст : непосредственный.

Краткие теоретические сведения

Система PERCo состоит из целого ряда компонентов и программных продуктов, которые рассмотрены ниже.

Подсистема СКУД и охранной сигнализации

Подсистема ***СКУД PERCo-S-20*** с элементами охранной сигнализации предназначена для организации контроля и управления доступом сотрудников, посетителей и ТС на территорию и в помещения предприятия.

Доступ может осуществляться по пропускам на основе бесконтактных карт через специально оборудованные точки прохода. Каждая карта обладает уникальной информацией – *идентификатором***.** В БД системы идентификатор связан с данными сотрудника, посетителя или ТС, которому она выдана. В качестве идентификатора в системе также могут выступать и биометрические признаки человека, в частности, в системе *PERCo-S-20* предусмотрена интеграция с биометрическими контроллерами *Suprema***,** которые осуществляют биоидентификацию по отпечаткам пальцев.

Контроллеры всех точек прохода связаны по сети Ethernet между собой и с единой БД системы. Каждое событие предъявления идентификатора фиксируется в БД с указанием места и времени предъявления. Это поз-

воляет отслеживать время пребывания и перемещения пользователей по территории и в помещениях предприятия.

Для каждого контролируемого направления через исполнительные устройства точек прохода может быть установлен один из режимов контроля доступа (РКД): «Открыто», «Закрыто», «Контроль». Это позволяет при необходимости обеспечить свободный проход в данном направлении или полностью его перекрыть. РКД «Контроль» используется для прохода по идентификаторам.

Для точек прохода типа «дверь» доступна возможность конфигурирования ОЗ. В зависимости от модели контроллера в ОЗ может входить ИУ и ШС. Эту ОЗ можно перевести в режим «Охрана» и снять с охраны при помощи идентификатора – бесконтактной карты доступа, которой выдан соответствующий тип прав, или оператором через ПО. При постановке на охрану для считывателей точки прохода устанавливается РКД «Охрана». Поддержка ШС позволяет контролировать не только вход в помещение, но также и весь его объем.

Подсистема ОПС (охранно-пожарная сигнализация)

Подсистема ***ОПС PERCo-S-20*** предназначена для обнаружения случаев возникновения пожара или проникновения на территорию и в помещения предприятия с возможностью включения светового и звукового оповещения, передачи извещений на ПЦН. Подсистема также может взаимодействовать с подсистемой ***СКУД PERCo-S-20,*** что позволяет управлять ИУ.

Подсистема может устанавливаться как автономная или централизованная ОПС на различных объектах: промышленных и торговых предприятиях, офисах, складах, квартирах, гаражах, дачах, и т. д.

ОПС системы строится на базе ППКОП. Они соответствуют требованиям государственного стандарта и нормам пожарной безопасности, обладают повышенной надежностью и рассчитаны на непрерывную круглосуточную работу.

В охраняемых помещениях размещаются неадресные охранные и пожарные извещатели. Автоматические извещатели позволяют обнаруживать на ранней стадии факт возникновения пожара или проникновения. Ручные извещатели позволяют любому сотруднику при необходимости подать сигнал вручную. ППКОП поддерживает возможность контроля вскрытия корпуса извещателей. Извещатели подключаются к ППКОП при помощи двухпроводных ШС.

ППКОП осуществляет прием сигнала от ШС о пожаре, проникновении или неисправности (КЗ и обрывы). При получении сигнала ППКОП включает индикацию номера нарушенного или неисправного ШС и, в соответствии с заданной конфигурацией, активизирует звуковые, световые оповещатели и подает сигнал на ПЦН.

Все регистрируемые события (прием сигналов «Пожар», «Тревога»,

неисправность, отключение питания и т. д.) сохраняются в энергонезависимой памяти ППКОП.

Конфигурация ППКОП после монтажа осуществляется по сети Ethernet от ПК с установленным ПО системы. ПК может также использоваться как устройство дополнительной индикации и управления.

Описание работы подсистемы ОПС PERCo-S-20 и основные технические характеристики ППКОП приводятся в эксплуатационной документации ППКОП.

Видеоподсистема

Подсистема видеонаблюдения ***PERCo-S-20*** состоит из камер наблюдения, АРМ операторов и одного или нескольких программных серверов видеонаблюдения.

В системе могут использоваться IP-видеокамеры и аналоговые видеокамеры, подключенные к lP-видеосерверам. Поддерживается работа камер в качестве детекторов движения. Система ***PERCo-S-20*** полностью совместима с видеокамерами стандарта ***ONVIF*.**

Список поддерживаемых видеоподсистемой камер наблюдения представлен на сайте компании ***PERCo,*** по адресу www.perco.ru, в разделе **Главная> Поддержка> Программное обеспечение** на вкладке **ПО PERCo-S-20**. Для поддержки некоторых моделей камер требуется установка дополнительных драйверов.

Для записи видеоархива данных, получаемых с IP-видеокамер и IP-видеосерверов, необходимо установить сервер видеоподсистемы. В системе может быть установлено несколько серверов. Для управления сервером и файлами видеоархива вместе с сервером видеоподсистемы устанавливается модуль ***«Центр управления видеоподсистемой».***

Подключение камеры к тому или иному серверу, а также настройка параметров камеры, производится в расширенной версии раздела ***«Конфигуратор»,*** входящей в модуль ***SM01 «Администратор».***

В состав видеоподсистемы входят следующие компоненты:

– ***«Видеонаблюдение»*** **–** модуль ПО, предназначен для организации АРМ оператора видеонаблюдения. Модуль позволяет отображать в режиме реального времени видеоинформацию с камер наблюдения видеоподсистемы и просматривать видеоархив, записанный с камер. Видеоинформация с камер передается непосредственно в модуль. Запись с камер производится по команде оператора или ПО.

– ***«Прозрачное здание»*** **–** модуль ПО, предназначен для организации АРМ руководителя или контролера. Модуль позволяет отображать в режиме реального времени видеоинформацию с камер наблюдения и просматривать видеоархив, записанный с камер. Видеоинформация в модуль поступает через сервер видеоподсистемы. В модуле доступны только те камеры, для которых установлен параметр **Использовать в «Прозрачном здании»**. Запись с отмеченных камер производится непрерывно.

– ***«Камеры СКУД»*** **–** компонент видеоподсистемы, позволяющий при предъявлении карты доступа считывателю производить автоматическую запись с камеры, связанной с этим считывателем. Камера устанавливается в точке прохода таким образом, что в ее поле зрения попадает место предъявления карт доступа считывателю. Для использования компонентом доступны только те камеры, для которых установлен параметр **Использовать, как камеру СКУД**. Длительность записи определяется параметром **Время предзаписи для камер СКУД**.

– ***«Верификация», «АТП: Верификация»*** **–** модули ПО, предназначены для организации АРМ оператора службы безопасности. Модули позволяют усилить контроль доступа через точки прохода за счет проведения оператором процедуры верификации. При организации точек верификации доступна возможность использования камер видеоподсистемы. Видеоинформация с камер передается непосредственно в модуль.

– ***«Прием посетителей»*** **–** модуль ПО, предназначен для организации АРМ сотрудника,

ведущего прием посетителей. При организации точки верификации доступна возможность использования камер видеоподсистемы. Видеоинформация с камер передается непосредственно в модуль.

– ***«Центральный пост охраны»*** **–** модуль ПО, предназначен для организации поста охраны и наблюдения. В модуле доступны возможности видеонаблюдения и верификации.

Сервер видеоподсистемы по сети Ethernet производит запись с камер видеоподсистемы. Запись начинается по команде оператора или ПО. Управление сервером видеоподсистемы и создание файлов видеоархивов производится из модуля ***«Центр управления видеоподсистемой»***.

АРМ

Автоматизированное рабочее место (АРМ) **–** программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Установка и лицензирование сетевого ПО системы производится по модульному принципу. То есть одновременно приобретаются все разделы, входящие в один модуль. Модуль может состоять из одного или нескольких разделов. При этом разделы одного модуля могут входить в разные АРМ.

Организация АРМ в системе производится выдачей полномочий оператору. При запуске ***«Консоли управления»*** под своей учетной записью оператору доступны только те разделы, на которые ему даны полномочия (при условии, что на данном ПК установлены модули, в которые входят эти разделы). Системой отслеживается количество АРМ с установленными разделами, одновременно подключенных к серверу системы. Оно не должно превышать количество предусмотренных лицензией рабочих мест.

Условно в системе можно выделить следующие возможные типы

АРМ (указаны необходимые для их организации модули):

1) АРМ «Администратор»

– PERCo-SN01 «Базовое ПО»
– PERCo-SM01 «Администратор»

2) АРМ «Служба безопасности»

– PERCo-SM08 «Мониторинг»
– PERCo-SM09 «Верификация»
– PERCo-SM012 «Видеонаблюдение»
– PERCo-SM013 «Центральный пост»

3) АРМ «Бюро пропусков»

– PERCo-SM03 «Бюро пропусков»
– PERCo-SM04 «Управление доступом»
– PERCo-SM014 «Дизайнер пропусков»

4) АРМ «Бухгалтерия»

– PERCo-SM05 «Дисциплинарные отчеты»
– «Интеграция с 1С»

5) АРМ «Отдел кадров»

– PERCo-SM02 «Персонал»

6) АРМ «Руководитель»

– PERCo-SM07 «Учет рабочего времени»
– PERCo-SM010 «Прием посетителей»
– PERCo-SM015 «Прозрачное здание»

Специализированные АРМ при установке соответствующих модулей:

– PERCo-SM016 «Кафе»
– PERCo-SM017 «АТП»

«Базовое ПО»

Модуль сетевого ПО ***PERCo-SN01 «Базовое ПО»*** предназначен для:

– подключения и конфигурации устройств системы;
– создания списка структурных подразделений предприятия;
– создания единого списка должностей;
– создания списка помещений (пространственных зон) с указанием точек прохода между ними и расположения на плане территории предприятия;
– создания графиков работы сотрудников;
– создания и ведения списка сотрудников;
– выдачи и изъятия карт доступа сотрудников;
– назначения прав доступа сотрудников в помещения предприятия;
– регистрации событий системы;
– задания автоматической реакции системы на регистрируемые события;
– оперативное управления устройствами системы.

В состав модуля входят следующие разделы:

– «*Конфигуратор»* – предназначен для конфигурирования системы, т. е. для задания необходимых значений параметрам как всей системы, так и параметрам входящих в нее устройств и их ресурсов.

– *«Помещения и мнемосхема»* – предназначен для составления единой схемы помещений и устройств, поэтажных планов и точек прохода между ними.

– «*Назначение прав доступа операторов»* – предназначен для ввода учетных данных операторов системы и выдачи им полномочий.

– «*События устройств и действия пользователей»* – предназначен для создания отчетов о событиях, зарегистрированных в системе.

– «*Управление устройствами»* – предназначен для оперативного управления устройствами системы.

– «*Сотрудники»* – предназначен для ведения списка сотрудников; организации отправки SMS-сообщений сотрудникам.

– «*Графики работы»* – предназначен для создания графиков работы сотрудников.

– «*Учетные данные»* – предназначен для задания структуры подразделений предприятия и списка используемых на предприятии должностей. Эти данные используются при вводе учетных данных сотрудников.

– *«Доступ сотрудников»* – предназначен для выдачи / изъятия карт доступа для сотрудников предприятия и назначения им прав доступа в помещения.

– *«СТОП-лист»* – предназначен для работы с запрещенными к использованию (заблокированными) картами доступа.

Дополнительные модули
ПО PERCo-SM01 «Администратор»

Модуль сетевого ПО ***PERCo-SM01 «Администратор»*** предназначен для организации АРМ администратора системы. В состав модуля входят следующие разделы:

– *«Конфигуратор»* (расширенная версия) – предназначен для добавления в конфигурацию устройств системы и для настройки их параметров. В отличие от базовой версии раздел данного модуля позволяет: описать параметры функционирования подсистемы пожарной сигнализации, описать параметры функционирования подсистемы видеонаблюдения, задать реакции системы на регистрируемые события.

– *«Планировщик заданий»* – предназначен для задания последовательности команд управления устройствами, выполняемых сервером системы, а также автоматической отправки SMS-сообщений в рамках выполнения заданий.

– *«Отчет по SMS»* – предназначен для генерирования отчетов по отправке и доставке SMS-сообщений.

PERCo-SM02 «Персонал»

Модуль сетевого ПО ***PERCo-SM02 «Персонал»*** предназначен для АРМ сотрудника отдела персонала, позволяет сократить объем рутинной работы и повышает эффективность работы. В состав модуля входят следующие разделы:

– *«Сотрудники»* (расширенная версия) – предназначен для автоматизации ведения списка сотрудников предприятия. В отличие от базовой версии раздел данного модуля позволяет: вводить фотографии сотрудников предприятия, заполнять расширенный список учетных данных в текстовом и графическом виде

– *«Учетные данные»* (расширенная версия) – предназначен для составления справочников учетных данных используемых на предприятии. В отличие от базовой версии раздел данного модуля позволяет расширять список учетных данных путем добавления дополнительных полей. В качестве данных могут быть использованы текстовые и графические значения.

PERCo-SM03 «Бюро пропусков»

Модуль сетевого ПО ***PERCo-SM03 «Бюро пропусков»*** используется для выдачи и изъятия карт доступа сотрудникам предприятия и посетителям. Модуль необходим для задания параметров доступа карт сотрудников и посетителей. (Для настройки критериев доступа по времени дополнительно необходим модуль ***PERCo-SM04 «Управление доступом»).*** В состав модуля входят следующие разделы:

– *«Доступ сотрудников»* (расширенная версия) – предназначен для выдачи карт доступа сотрудникам предприятия и назначения им прав доступа в выбранные помещения. В отличие от базовой версии раздел данного модуля позволяет: назначать параметры доступа карты (Antipass, доступ по времени, комиссионирование, верификация), назначать сотрудникам права по постановке на охрану (снятию с охраны) помещений.

– *«Автозамена параметров доступа»* – предназначен для временных замены прав доступа сотрудников (например, на время отпуска, выполнения специальных работ и др.), без изменения штатных прав доступа.

– *«Доступ посетителей»* **–** предназначен для выдачи временных карт доступа посетителям предприятия, назначения им прав и параметров доступа в выбранные помещения.

– *«Доступ в помещение»* **–** предназначен для оперативного разрешения / запрета прохода в выбранное помещение для одной или нескольких карт доступа.

– *«СТОП-лист»* (расширенная версия) – предназначен для работы с картами доступа, которые были занесены в СТОП-лист по причине изъятия карты, невозвращения карты сотрудником при увольнении, утере карты.

– *«Заказ пропусков для посетителей»* **–** служит для заказа карты доступа посетителей для последующей выдачи в разделе «Доступ посетителей».

PERCo-SM04 «Управление доступом»

Модуль сетевого ПО ***PERCo-SM04 «Управление доступом»*** предназначен для настройки критериев доступа по времени. Создаваемые в этом разделе критерии в дальнейшем могут быть использованы для разграничения доступа по времени сотрудников и посетителей. В состав модуля входят следующие разделы:

– *«Временные зоны»* – предназначен для создания критериев контроля доступа по времени в рамках суток.

– *«Недельные графики»* – предназначен для создания критериев контроля доступа по времени в рамках недели.

– *«Скользящие посуточные графики»* – предназначен для создания критериев контроля доступа по времени для скользящих посуточных графиков.

– *«Скользящие понедельные графики»* – предназначен для создания критериев контроля доступа по времени для скользящих понедельных графиков.

– *«Типы праздников»* – предназначен для задания в системе праздничных дней за текущий год.

PERCo-SM05 «Дисциплинарные отчеты»

Модуль сетевого ПО ***PERCo-SM05 «Дисциплинарные отчеты»*** предназначен для контроля руководителями подразделений трудовой дисциплины сотрудников, позволяет формировать отчеты о нарушениях трудовой дисциплины: опозданиях, прогулах, уходах раньше. В состав модуля входят следующие разделы:

– *«Дисциплина труда*» – предназначен для получения отчетов о нарушениях дисциплины труда во всех или выбранных подразделениях с участием всех или отдельных сотрудников за определенный интервал времени. Интервал времени, за который просматриваются события, задается с точностью до дня. Нарушения трудовой дисциплины определяются относительно установленных графиков рабочего времени.

– *«Время присутствия»* – предназначен для получения отчетов о количестве времени, проведенном сотрудником на территории предприятия.

– *«Местонахождение»* – предназначен для получения отчетов о местонахождении сотрудника в определенный день и время суток.

PERCo-SM07 «УРВ» (Учет рабочего времени)

Модуль сетевого ПО ***PERCo-SM07 ««Учет рабочего времени»*** предназначен для организации АРМ сотрудника, формирующего отчеты по отработанному времени для начисления заработной платы (табельщика). В состав модуля входят следующие разделы:

– *«Журнал отработанного времени»* – предназначен для ведения табельного учета на предприятии.

– *«Отчеты»* – предназначен для формирования табелей учета рабо-

чего времени по формам Т-12 и Т-13.

– *«Оправдательные документы»* – предназначен для ввода и редактирования информации об уважительной причине отсутствия сотрудника на рабочем месте: оправдательных документов, влияющих на корректность расчета табелей учета рабочего времени.

– *«Временная замена учетных данных»* – предназначен для временного изменения подразделения и/или график работы сотрудников, без изменения штатных значений, установленных в разделе «Сотрудники».

PERCo-SM08 «Мониторинг»

Модуль сетевого ПО ***PERCo-SM08 «Мониторинг»*** устанавливается на АРМ сотрудника службы безопасности и предназначен для отображения информации о состоянии объекта и оперативного управления расположенными на нем устройствами.

В состав модуля входят следующие разделы:

– *«Управление устройствами и мнемосхемой»* – предназначен для отображения информации о состоянии объектов системы на графических планах и управления устройствами в целях оперативного реагирования в случае экстренной ситуации.

– *«Выбор событий мониторинга»* – предназначен для определения устройств и типов событий, информация о которых отображается на каждом конкретном посту охраны.

\PERCo-SM09 «Верификация»

Модуль сетевого ПО ***PERCo-SM09 «Верификация»*** устанавливается на АРМ сотрудника службы охраны и позволяет производить идентификацию владельца карты доступа, сравнивая внешность проходящего сотрудника (посетителя) или изображение с видеокамеры и фото владельца карты, хранящееся в БД системы.

В состав модуля входят следующие разделы:

– *«Верификация»* – предназначен для проведения процедуры верификации, то есть отображения информации о владельце предъявленной карты доступа, а также для отображения и записи кадров, полученной с выбранных камер.

– *«Журнал верификации»* – предназначен для автоматической записи с целью последующего просмотра всех действий операторов, информации о предъявлении карт доступа в разделе «Верификация».

PERCo-SM10 «Прием посетителей»

Модуль сетевого ПО ***PERCo-SM10 «Прием посетителей»*** предназначен для организации АРМ руководителя или другого лица, ведущего прием посетителей. Также модуль может использоваться для организации доступа в помещения с особым режимом доступа, например, в кассу.

В состав модуля входят следующие разделы:

– *«Прием посетителей»* – предназначен для проведения оператором процедуры верификации при автоматизированном приеме посетителей.

– *«Журнал приема посетителей»* – предназначен для просмотра данных о фактах предъявления карт доступа к контролируемым разделом «Прием посетителей» считывателям.

PERCo-SM12 «Видеонаблюдение»

Модуль сетевого ПО ***PERCo-SM12 «Видеонаблюдение»*** состоит из одного раздела и предназначен для организации АРМ сотрудника службы безопасности, являющегося оператором видеонаблюдения. Модуль позволяет выводить на монитор кадры с камер видеоподсистемы, производить запись с камер, просматривать видеоархив.

PERCo-SM13 «Центральный пост»

Модуль сетевого ПО ***PERCo-SM13 «Центральный пост»*** устанавливается на АРМ сотрудника службы безопасности и позволяет вести централизованное наблюдение за состоянием объекта. Модуль позволяет обеспечить взаимодействие технических и программных средств, в том числе в автоматическом режиме (включение видеокамеры в зоне сработавшего охранного датчика и т. д.), снижая негативное влияние человеческого фактора.

В состав модуля входят следующие разделы:

– *«Центральный пост охраны»* – предназначен для отображения информации о состоянии объектов на графических планах предприятия и в табличном виде; отображения информации с камер видеонаблюдения; управление устройствами, расположенными на графическом плане предприятия; проведения процедуры верификации при контроле доступа; автоматического отображения информации с камер видеонаблюдения и указания на мнемосхеме помещения, где произошло событие, в случае возникновении тревожной ситуации.

– *«Выбор событий центрального поста»* – предназначен для определения устройств и типов событий, информация о которых отображается на каждом конкретном посту охраны.

– *«Журнал центрального поста»* – предназначен для просмотра данных о событиях на объектах и о фактах предъявления карт доступа считывателям, контролируемым в режиме верификации.

PERCo-SM14 «Дизайнер пропусков»

Модуль сетевого ПО ***PERCo-SM14 «Дизайнер пропусков»*** состоит из одного раздела и предназначен для организации АРМ сотрудника бюро пропусков, занимающегося подготовкой шаблонов и печатью пропусков сотрудников и посетителей предприятия. Это позволяет автоматизировать работу по оформлению постоянных и временных пропусков. Предусмотрена возможность печати двухсторонних пропусков.

PERCo-SM15 «Прозрачное здание»

Модуль сетевого ПО ***PERCo-SM15 «Прозрачное здание»*** состоит из одного раздела и предназначен для организации АРМ руководителя или сотрудника, ведущего контроль выполнения сотрудниками производ-

ственных задач на рабочих местах с целью повышения трудовой дисциплины. Модуль позволяет выводить на монитор кадры с камер видеоподсистемы, просматривать видеоархив.

PERCO-SM16 «Кафе»

Модуль сетевого ПО ***PERCo-SM16 «Кафе»*** предназначен для организации учета безналичных и наличных расчетов оплаты питания персонала с использованием бесконтактных карт доступа на предприятиях, имеющих подразделения служебного питания (кафе, столовые, буфеты и т. п.). Модуль ***«Кафе»*** позволяет учитывать различные схемы льгот и компенсаций питания сотрудников. В состав модуля входят следующие разделы:

– *«Блюда и меню»* – предназначен для создания и хранения полного списка блюд кафе, формирования текущего меню на его основе.

– *«Касса»* – предназначен для организации АРМ кассира кафе и позволяет производить идентификацию сотрудника по карте доступа; формировать заказ из выбранных сотрудником блюд на основе текущего меню; рассчитывать стоимости заказа с учетом льгот и компенсаций; выбирать способ оплаты и производить расчет с сотрудником.

– *«Отчеты»* – предназначен для формирования отчетов по расчетам с сотрудниками и количеству и ассортименту проданных блюд.

– *«Справочники»* – предназначен для ведения справочников схем оплаты питания, графиков посещения кафе и предприятий общественного питания.

PERCo-SM17 «АТП» (Автотранспортная проходная)

Модуль сетевого ПО ***PERCo-SM17 «АТП»*** предназначен для организации работы автотранспортной проходной (АТП), построенной на базе контроллеров серии ***pERCo- CT/L04, CT/L04.2.*** Система АТП предназначена для использования на предприятиях (в организациях), которые располагают собственной территорией с контролируемыми въездами/выездами для автотранспортных средств. Состоит из следующих разделов:

– *«АТП: Транспортные средства»* – предназначен для ввода данных о ТС сотрудников и служебных ТС; выдачи карт доступа, назначения им прав доступа.

– *«АТП: Отчеты»* – предназначен для составления отчетов, основанных на анализе событий, регистрируемых контроллерами, о времени, проведенном ТС на территории или вне территории предприятия (организации).

– *«АТП: Верификация»* – позволяет организовать АРМ сотрудника службы безопасности для проведения процедуры верификации.

– *«АТП: Журнал верификации»* – предназначен для просмотра событий о фактах предъявления карт доступа к считывателям, которые контролируются разделом «АТП: верификация».

Кроме этого при установке модуля ***«АТП»*** в разделе ***«Доступ посе-***

тителей» модуля ***PERCo-SM03 «Бюро пропусков»*** появляется возможность вводить данные о транспортном средстве посетителя.

Методические указания по отработке учебных вопросов

1. WEB-интерфейс. Главная страница и разделы

Помимо программного обеспечения PERCo-S-20 настройку и диагностику контроллеров возможно производить через встроенный WEB-интерфейс. WEB-интерфейс применяется при необходимости удаленного администрирования, изменения сетевых настроек и проверки работоспособности оборудования без необходимости инсталляции дополнительного ПО. WEB-интерфейс позволяет создавать малые СКУД на несколько точек доступа с возможностью ввода карт доступа, формирования простых отчетов. Использование WEB-интерфейса возможно в любых операционных системах и платформах, включая мобильные.

Для того чтобы начать работу с WEB-интерфейсом контроллера, необходимо запустить браузер. Контроллер, к которому нужно получить доступ, должен быть работоспособным и подключен к локальной сети, либо напрямую к компьютеру, либо через роутер или любое другое сетевое устройство.

1.1. Убедитесь, что контроллер имеет связь с локальной сетью и контроллером.

Компьютер и контроллер должны находиться в одной подсети. Подсеть IP-адресов контроллеров, которые выходят с завода – это подсеть 10.0, то есть все контроллеры по умолчанию имеют IP-адрес, который начинается с 10.0. В адресной строке ввести IP-адрес контроллера, и таким образом становится доступным WEB-интерфейс контроллера. На главной странице (рис. 8.1) отображается текстовая информация: модель контроллера, вариант конфигурации, версия встроенного ПО, MAC-адрес, IP-адрес, шлюз, маска подсети и заводской IP-адрес.

Раздел «Главная» показывает текущие параметры контроллера, и дает возможность изменить текущий IP-адрес контроллера, изменить шлюз и задать новую маску посети (рис. 8.2). Также в этой вкладке находится синхронизация со временем, для этого существуют три варианта: ручная настройка, синхронизация с ПК и использование текущей даты и времени.

Раздел «Смена пароля» дает возможность установить пароль на контроллер, либо спросить пароль с контроллера (рис. 8.3). В случае если будет установлен пароль на контроллер, то при входе в WEB-интерфейс контроллера, он запросит пароль.

Раздел «Конфигурация» дает возможность настраивать параметры исполнительных устройств, считывателя и формата для ввода и хранения карт доступа.

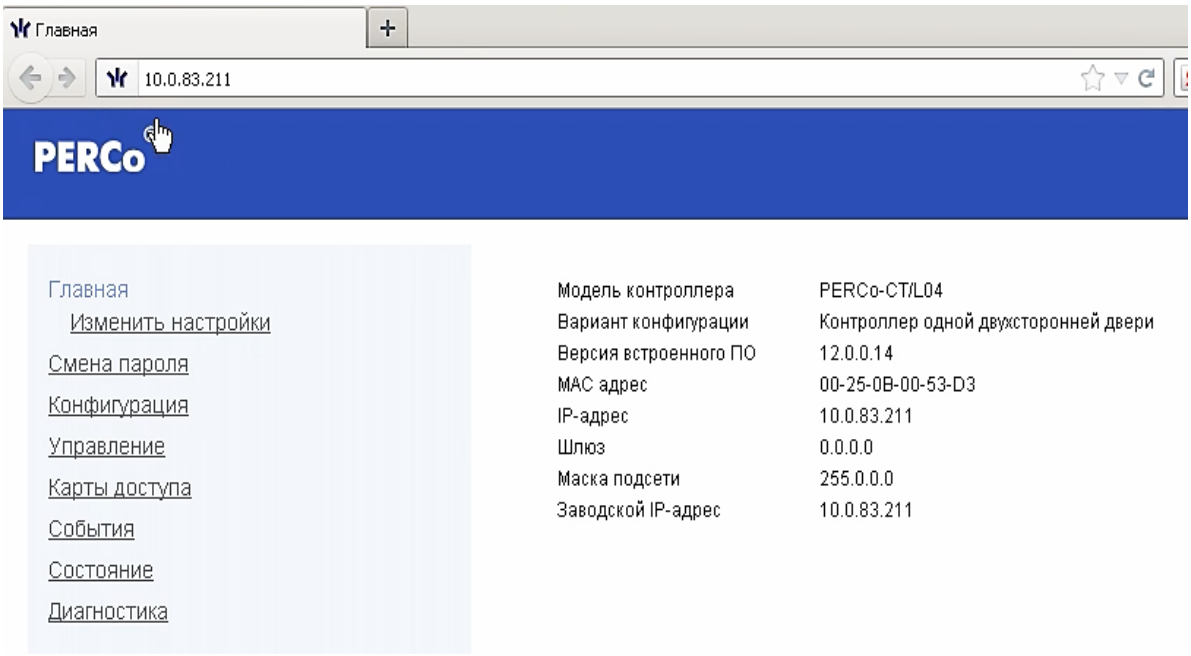


Рис. 8.1. Окно главной страницы

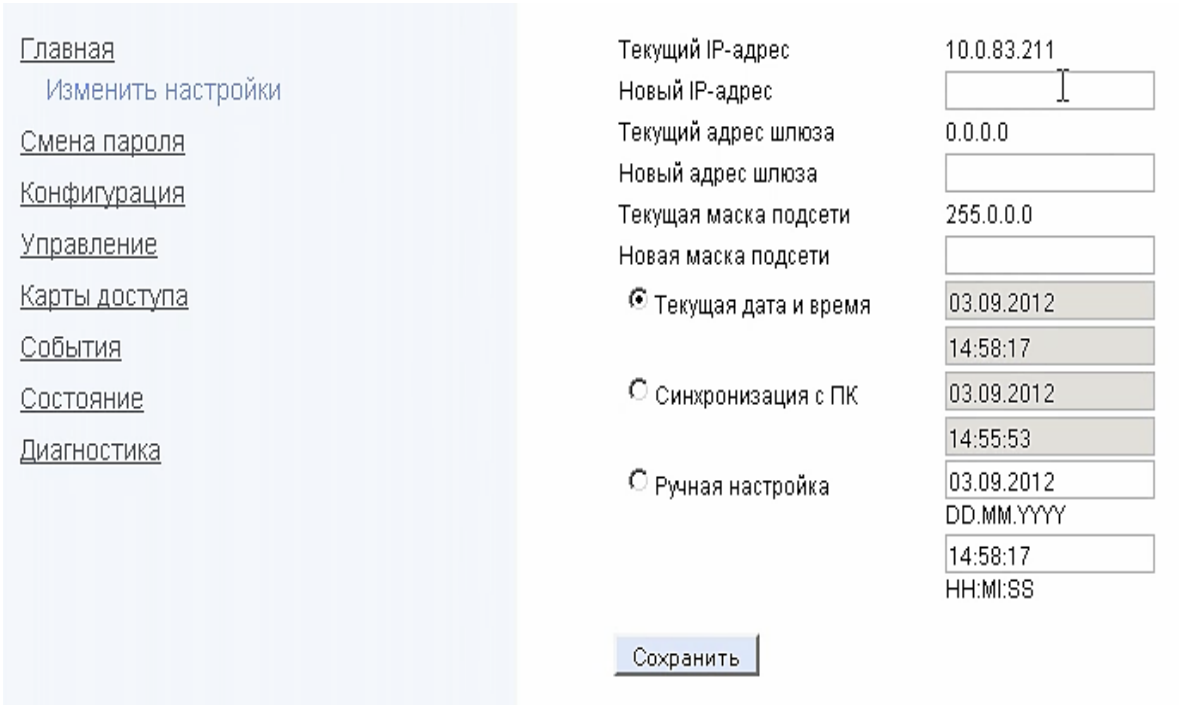


Рис. 8.2. Окно изменения сетевых настроек

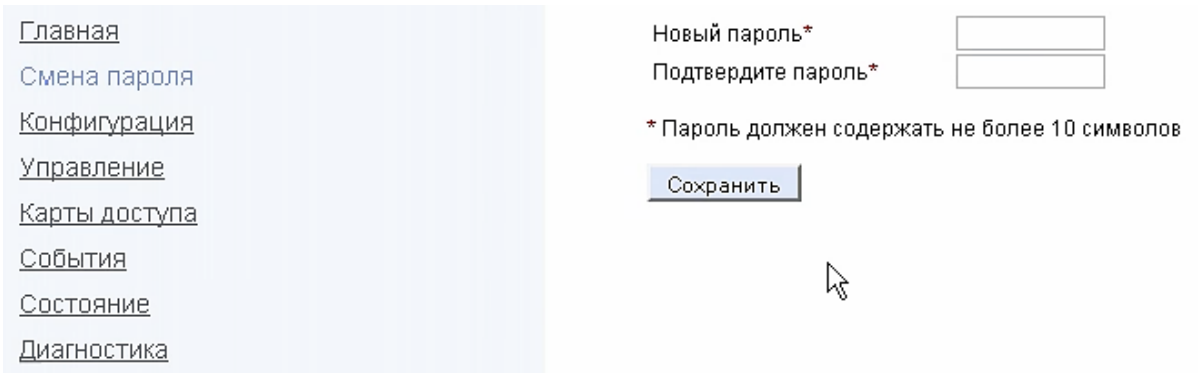


Рис. 8.3. Окно раздела смена пароля

Вкладка «Исполнительное устройство» дает возможность выбирать каждое из исполнительных устройств (рис. 8.4). Можно менять: предельное время разблокировки, время удержания в разблокированном состоянии, длительность импульса (для импульсного режима), нормальное состояние датчика, нормальное состояние выхода управления, нормализацию выхода управления, режим работы выхода управления, регистрацию прохода по предъявлению карты и направление прохода.

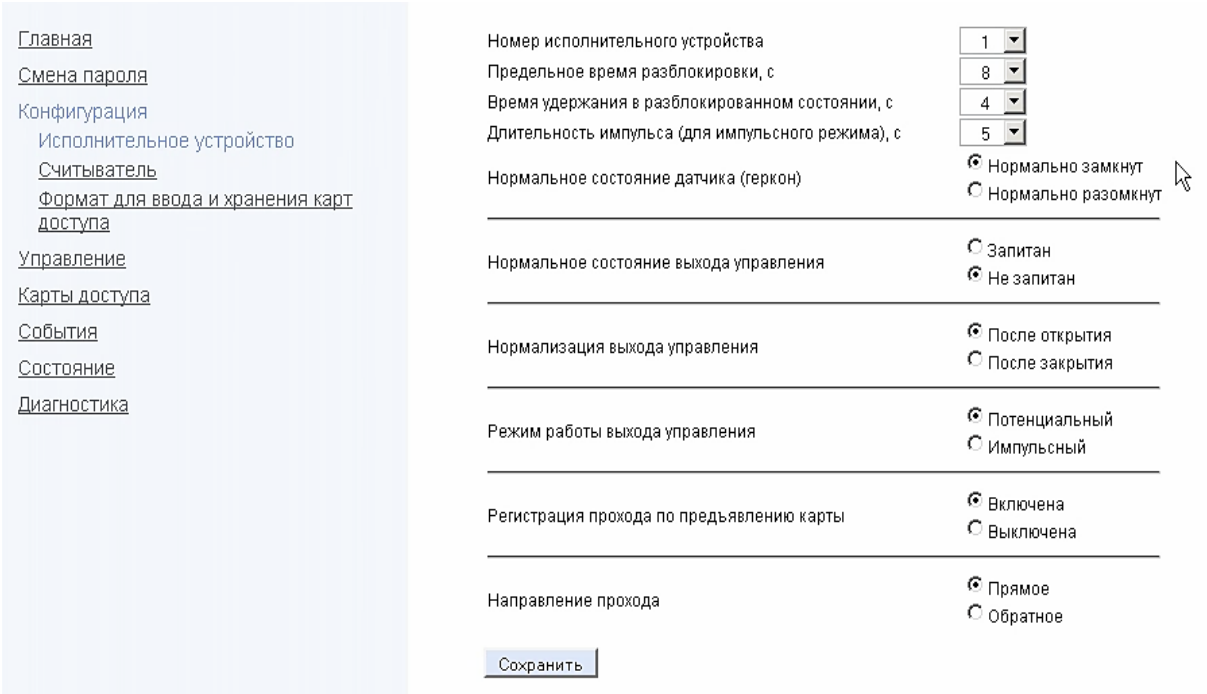


Рис. 8.4. Окно вкладки исполнительных устройств

Настройки во вкладке «Считыватель» дают возможность включать или отключать управление от дистанционного управления на каждый из считывателей (рис. 8.5).

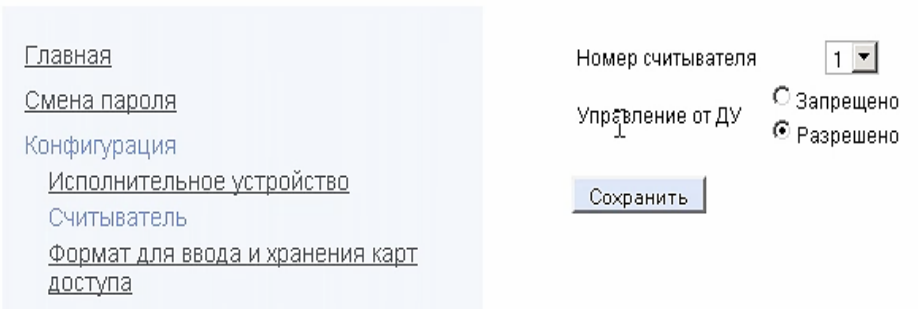


Рис. 8.5. Окно вкладки считывателей

Вкладка «Формат для ввода и хранения карт доступа» дает возможность выбрать выбрать формат универсальный (8 байт) или сокращенный (3 байта, Wiegand 26) (рис. 8.6).

Рис. 8.6. Окно вкладки формата
для ввода и хранения карт доступа

Раздел «Управление» дает возможность на каждое из считывателей устанавливать различные режимы: контроль, открыто, закрыто, охрана (рис. 8.7).

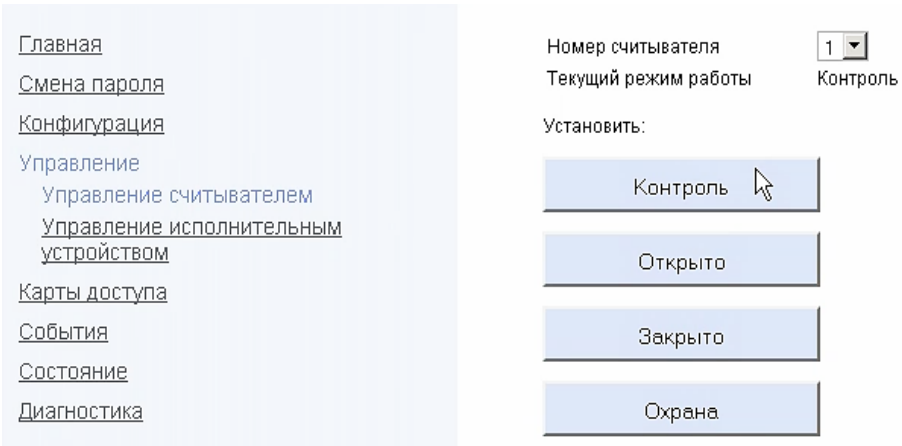


Рис. 8.7. Окно раздела управления считывателем

Также можно управлять исполнительным устройством (рис. 8.8).

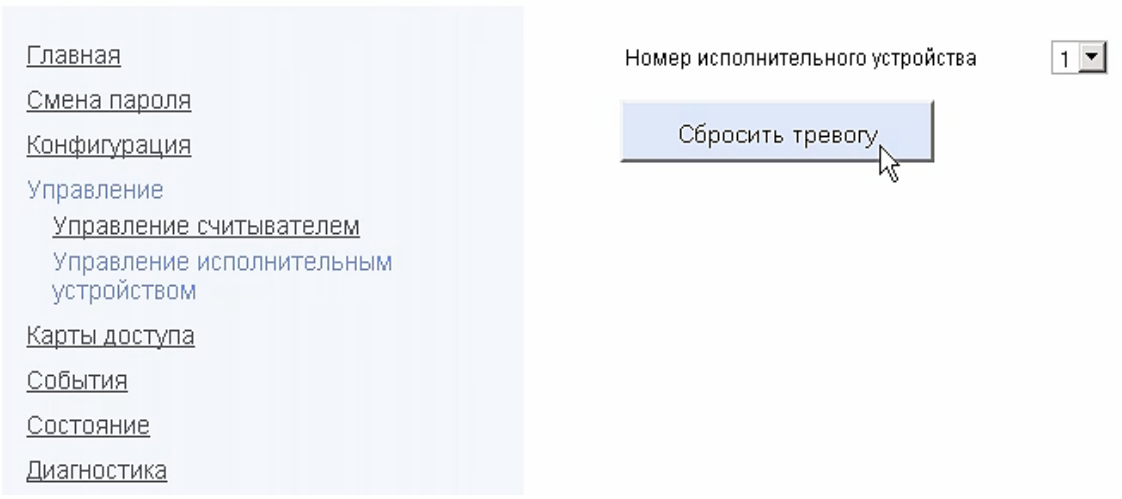


Рис. 8.8. Окно раздела управления исполнительным устройством

2. Добавление карт доступа

Раздел «Карты доступа» (рис. 8.9). На главной странице показано количество карт, загруженных в контроллер.

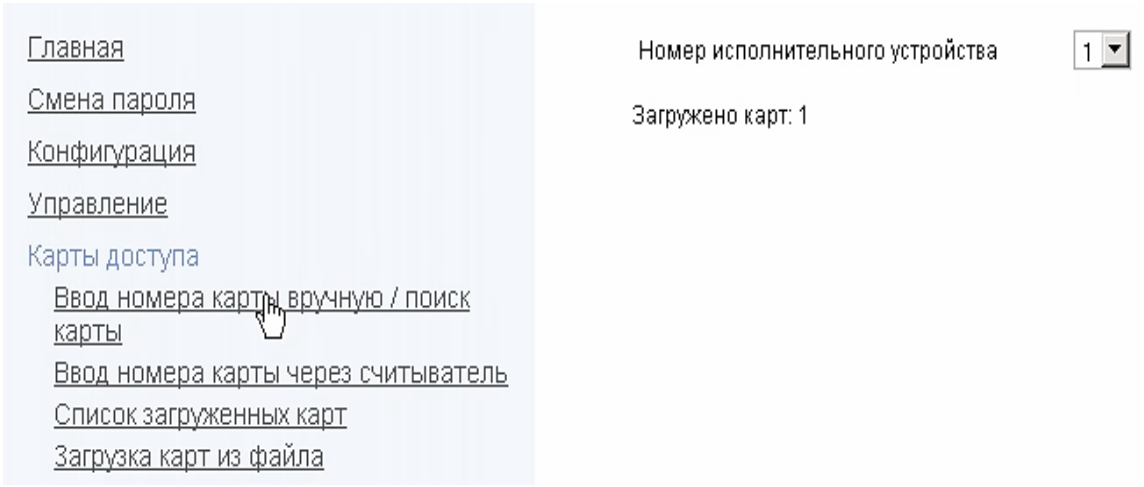


Рис. 8.9. Окно раздела карт доступа

Существует несколько способов добавления карты в контроллер.

1) Есть возможность ввести номер карты вручную, для этого необходимо ввести код семейства и номер пропуска (рис. 8.10). Система автоматически отображает введенные параметры карты в универсальном формате 8 байт.

2) Для того чтобы использовать считыватель для занесения карт, необходимо выбрать тот считыватель, который предполагается использовать (рис. 8.11). После этого нажать на иконку «Старт», и поднести карту

к считывателю. После поднесения всех карт, нажать «Стоп». Для подтверждения занесенных карт, необходимо нажать на иконку «Сохранить».

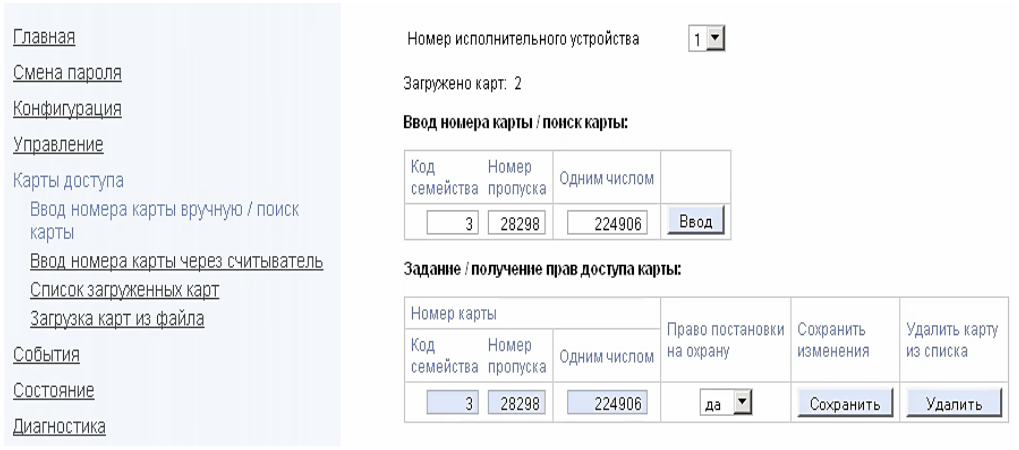


Рис. 8.10. Окно вкладки ввода карт вручную

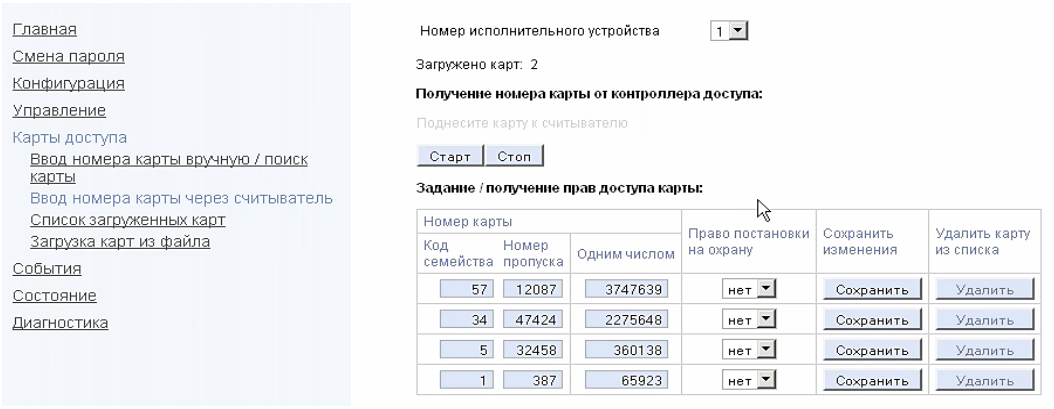


Рис. 8.11. Окно вкладки ввода номерка карты через считыватель

3) Также существует возможность загрузки карт из файла (рис. 8.12).

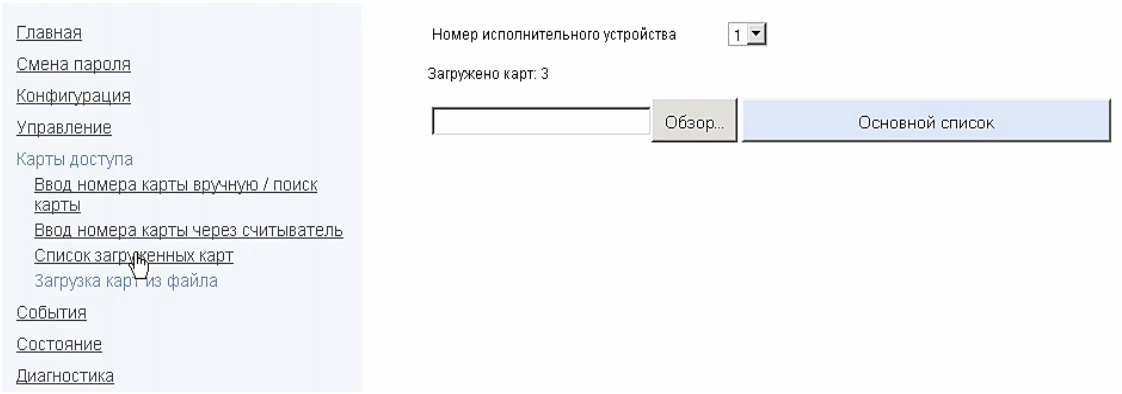


Рис. 8.12. Окно вкладки загрузки карт из файла

Для этого необходимо выбрать соответствующий файл, содержащий следующие параметры (рис. 8.13):

– номер карты, записанный в универсальном формате 8 байт;

– число 1 или 0, расположенное правее от номера карты и означающее соответственно наличие или отсутствие права пользователя на постановку под охрану;

– ФИО пользователя, которому предоставлена карта.

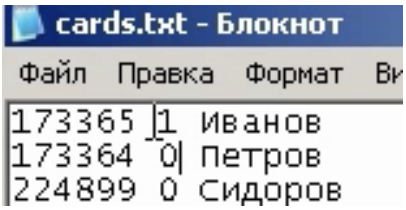


Рис. 8.13. Содержимое файла конфигурации карт, открытого в программе «Блокнот»

Также есть возможность просмотреть список загруженных карт и производить изменения в них (рис. 8.14).

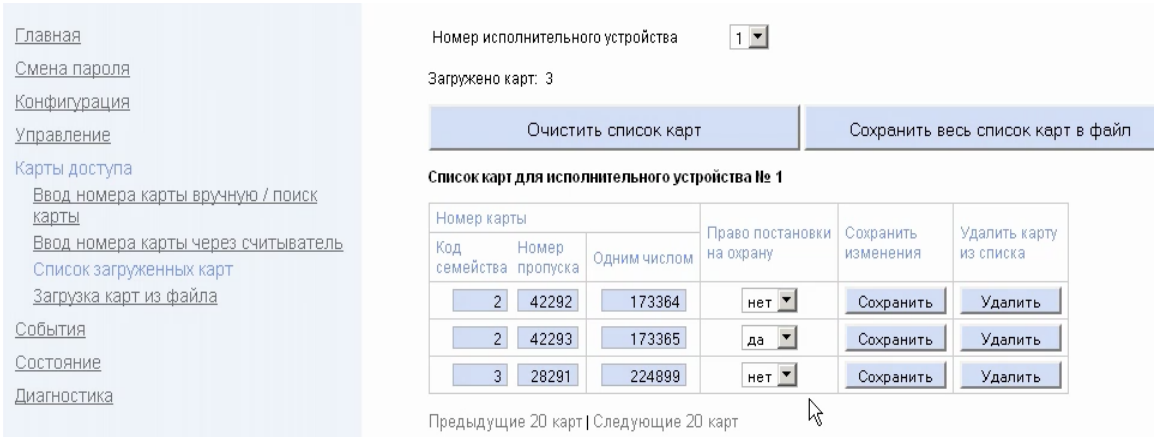


Рис. 8.14. Окно вкладки списка загруженных карт

При вводе карт, необходимо в первую очередь загружать карты из файла, и далее вводить карты вручную или через считыватель. Иначе карты, загруженные до загрузки карт из файла, будут удалены.

Раздел «События» дает возможность по определенному интервалу просмотреть все события на данном контроллере (рис. 8.15). Существует два варианта отображения журнала событий – краткий и полный. Во втором варианте (полном) отображаются все события, включая системные. При просмотре событий на контроллере журнал событий в контроллере не очищается. Есть возможность очистить журнал событий, чтобы обнулить память контроллера, и возможность сохранения журнала событий в файл.

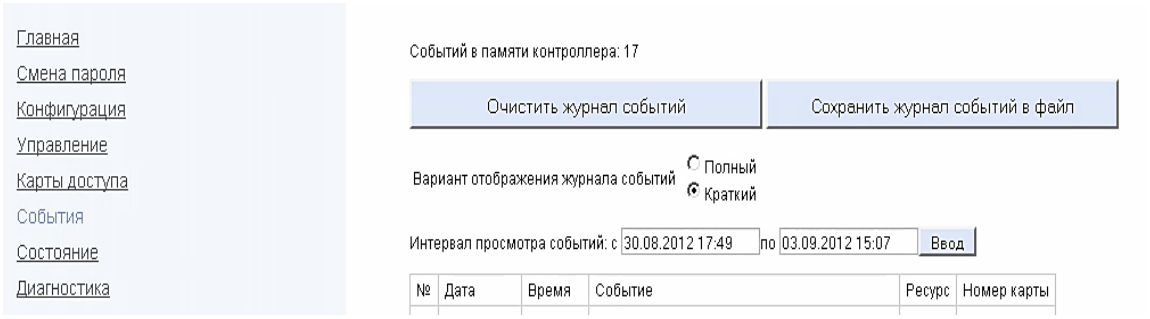


Рис. 8.15. Окно раздела события

Раздел «Состояние» показывает аппаратные неисправности, напряжение питания, режим прибора, есть ли вскрытие корпуса и режимы считывателей, и также исполнительные устройства (рис. 8.16).

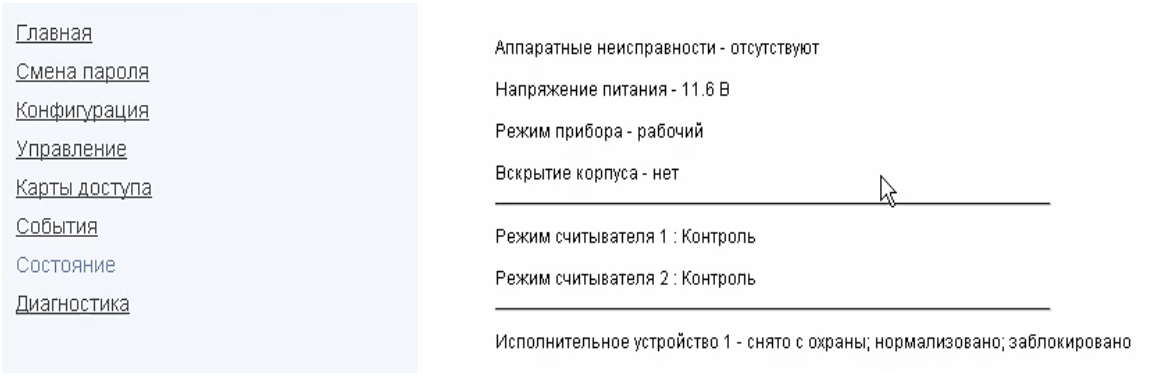


Рис. 8.16. Окно раздела состояния

Раздел «Диагностика» дает возможность провести тестирование контроллера (рис. 8.17).

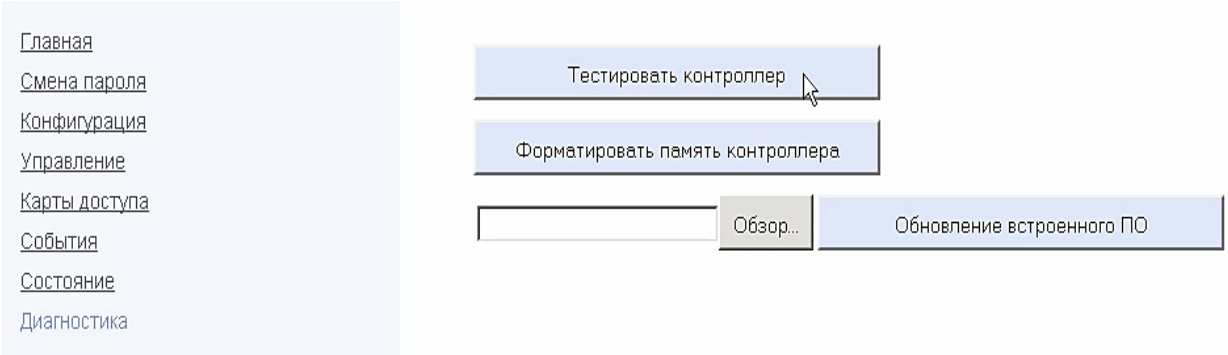


Рис. 8.17. Окно раздела диагностики

При запуске аппаратного теста контроллера будет удален журнал событий контроллера, и по окончании тестирования будет выведен отчет о его результатах. Форматирование памяти контроллера запускает форматирование внутренней памяти, и форматирование контроллера производится за одну минуту. При форматировании исчезают все данные по конфигурации, списки карт, журнала событий и пароль, установленный на контроллер. Также есть возможность обновления встроенного ПО.

Содержание отчета

1. Тема и цель работы, учебные вопросы, учебно-материальное обеспечение занятия.
2. Скриншоты веб-интерфейса системы PERCo-S-20 по выполнении каждого этапа практических заданий с пояснениями.
3. Выводы по результатам выполнения практической работы.

Контрольные вопросы

1. Поясните порядок входа в WEB-интерфейс.
2. Каковы особенности программирования компонентов системы через WEB-интерфейс?
3. Какие разделы WEB-интерфейса используются для настройки?
4. Принцип работы TCP/IP протокола?
5. Какие виды топологий локальных сетей Вам известны?
6. Раскройте определения терминов «протокол» и «интерфейс».
7. Назовите виды сетевого оборудования.
8. Сколько байт данных содержит в себе IP-адрес?

Задания для самостоятельной работы

1. Изучите и законспектируйте в тетради особенности организации локальных вычислительных сетей.
2. Составьте схему локальной вычислительной сети лаборатории систем автоматизированного проектирования с указанием IP-адресов, MAC-адресов оборудования.

ЗАКЛЮЧЕНИЕ

Система безопасности и повышения эффективности PERCo-S-20 – сетевая многофункциональная система, позволяющая осуществлять контроль и управление доступом всего объекта и удовлетворяющая расширенным требованиям безопасности.

Особенностями системы являются:

– работа в автономном режиме без постоянной связи с компьютером;

– энергонезависимое хранение списков доступа и списков событий в контроллерах системы (СКД);

– разграничение прав доступа по помещениям, по времени, по статусу карты;

– поддержка недельных и сменных графиков доступа;

– защита от передачи карты (Antipassback);

– постановка помещений на системную охрану.

Система PERCo-S-20 построена на основе сети контроллеров и компьютеров, связь между которыми осуществляется по интерфейсу Ethernet. Использование IP-технологии при построении современных систем безопасности позволяет использовать богатый опыт типовых решений, который накоплен в компьютерных сетях, дает ряд существенных преимуществ и обеспечивает надежность работы системы.

Преимуществом СКУД S-20 является использование одного и того же оборудования для решения разноплановых задач. Данные, получаемые от системы доступа, могут быть в дальнейшем использованы в системах повышения эффективности. Данные о фактах и времени прохода сотрудников через точку контроля сохраняются в памяти контроллера и могут быть использованы для составления отчетов по трудовой дисциплине и табеля учета рабочего времени, а также начисления заработной платы.

Учебное издание ориентировано на курсантов и слушателей радиотехнического факультета. Издание может быть полезно слушателям факультета профессиональной подготовки и факультета переподготовки и повышения квалификации, обучающихся по различным направлениям подготовки.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые источники:

1. О безопасности : Федеральный закон Российской Федерации от 28 декабря 2010 года № 390-ФЗ. – СПС «КонсультантПлюс» (дата обращения 12.02.2022). – Текст : непосредственный.

2. О полиции : Федеральный закон от 7 февраля 2011 года № 3-ФЗ. – СПС «КонсультантПлюс» (дата обращения 12.02.2022). – Текст : непосредственный.

3. О противодействии терроризму : Федеральный закон от 6 марта 2006 года № 35-ФЗ. – СПС «КонсультантПлюс» (дата обращения 12.02.2022). – Текст : непосредственный.

4. О безопасности объектов топливно-энергетического комплекса : Федеральный закон от 21 июля 2011 года № 256-ФЗ. – URL: http://docs.cntd.ru/document/ (дата обращения 12.02.2022). – Текст : электронный.

5. О войсках национальной гвардии : Федеральный закон от 3 июля 2016 года № 226-ФЗ. – URL: http://docs.cntd.ru/document/ (дата обращения 12.02.2022). – Текст : электронный.

6. Об антитеррористической защищенности объектов (территорий) (вместе с «Правилами разработки требований к антитеррористической защищенности объектов (территорий) и паспорта безопасности объектов (территорий) : постановление Правительства Российской Федерации от 25 декабря 2013 № 1244. – URL: http://base.garant.ru/70552494/ (дата обращения 12.02.2022). – Текст : электронный.

7. Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий) : постановление Правительства Российской Федерации от 11 февраля 2017 г. № 176. – URL: http://www.garant.ru /products /ipo/prime/doc/71511840/ (дата обращения: 12.02.2022). – Текст : электронный.

8. Об утверждении перечня объектов, подлежащих обязательной охране войсками национальной гвардии Российской Федерации (с изменениями на 26 июля 2018 года) : распоряжение Правительства Российской Федерации от 15 мая 2017 года № 928-р. – URL: http://www.garant.ru (дата обращения 12.02.2022). – Текст : электронный.

9. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств : приказ МВД России от 31.12.2014 № 1152. – URL: http://www.garant.ru (дата обращения 12.02.2022). – Текст : электронный.

10. СП 132.13330.2011. Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования. – URL: www.mchs.gov.ru/law/Svodi_pravil/item (дата обращения 12.2.2022). – Текст : электронный.

11. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний. – Москва : Изд-во стандартов, 2007. – 19 с. – Текст : непосредственный.

12. ГОСТ Р ИСО/МЭК 7810-2015 Карты идентификационные. Физические характеристики. – Москва : Изд-во стандартов, 2014. – 19 с. – Текст : непосредственный.

13. ГОСТ Р ИСО/МЭК 7816-1-2013 Карты идентификационные. Карты на интегральных схемах. Часть 1. Карты с контактами. Физические характеристики. – Москва : Изд-во стандартов, 2012. – 20 с. – Текст : непосредственный.

14. ГОСТ Р ИСО/МЭК 15693-1-2013 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты удаленного действия. Часть 1. Физические характеристики. – Москва : Изд-во стандартов, 2007. – 21 с. – Текст : непосредственный.

15. ГОСТ 14254-2015 (IEC 60529:2013) Степени защиты, обеспечиваемые оболочками (Код IP) (Издание с Поправкой). – Москва : Изд-во стандартов, 2014. – 29 с. – Текст : непосредственный.

16. Р 085-2019. Правила производства монтажа и технического обслуживания технических средств безопасности на объектах, охраняемых (принимаемых под охрану) подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации, а также порядка контроля за их проведением. Методические рекомендации. – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2019. – 47 с. – Текст : непосредственный.

17. Р 071-2017. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 20 с. – Текст : непосредственный.

18. Р 064-2017. Выбор и применение технических средств контроля и управления доступом. Методические рекомендации. – Москва : НИЦ «Охрана» Росгвардии. – 2017. – 92 с. – Текст : непосредственный.

19. ТП 78.36.005-2014. Система контроля и управления доступом. Административное здание. Типовой рабочий проект. – Москва : НИЦ «Охрана», 2014. – 37 стр. – Текст : непосредственный.

20. РМ 78.36.002-2012. Обзор запирающих устройств на отечественном рынке. – Москва : НИЦ «Охрана», 2012. – 155 с. – Текст : непосредственный.

Основные источники:

21. Организация охраны объектов особой важности, повышенной опасности и жизнеобеспечения : практикум / С. А. Винокуров [и др.] ; Воронежский институт МВД России ; Кафедра радиотехнических систем и комплексов охранного мониторинга. – Воронеж : ВИ МВД России, 2019. – 109 с. – Текст : непосредственный.

22. Ворона, В. А. Системы контроля и управления доступом : учебное пособие / В. А. Ворона, В. А. Тихонов – Москва : Горячая линия – Телеком, 2016. – 272 с.: ил. – Текст : непосредственный.

23. Аппаратно-программные комплексы охранного мониторинга : учебное пособие / С. А. Винокуров [и др.] ; Воронежский ин-т МВД России; Кафедра радиотехнических систем и комплексов охранного мониторинга. – Воронеж : ВИ МВД России, 2017. – 243 с. – Текст : непосредственный.

24. Проектирование технических систем безопасности и охранного мониторинга : практикум / С. А. Гречаный [и др]. – Воронеж: Воронежский институт МВД России, 2018. – 125 с. –Текст : непосредственный.

25. Организация комплексных систем мониторинга объектов охраны : курс лекций / С. А. Винокуров, С. А. Гречаный, Д. Ю. Калков. – Воронеж : ВИ МВД России, 2019. – Текст : электронный.

26. Организация комплексных систем оповещения с целью повышения эффективности безопасности объектов: методические рекомендации / С. А. Гречаный, А. В. Сидоров, Д. Ю. Калков [и др.]. – Воронеж : Воронежский институт МВД России, 2019. – 65 с. – Текст: непосредственный.

Дополнительные источники:

27. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч. 1 / С. А. Винокуров, С. А. Гречаный, М. Ю. Пакляченко. – Воронеж : ВИ МВД России, 2019. – 165 с. – Текст : непосредственный.

28. Организация интегрированных систем безопасности и охранного мониторинга : курс лекций. Ч. 2 / С. А. Винокуров, С. А. Гречаный, М. Ю. Пакляченко. – Воронеж : ВИ МВД России, 2019. – 158 с. – Текст : непосредственный.

29. Романов, М. С. Комплексные системы безопасности : методические рекомендации / М. Ю. Пакляченко, М. С. Романов, М. В. Таравков. – Воронеж : ВИ МВД России, 2018. – Текст : электронный.

30. Обеспечение безопасности на объектах спортивной инфраструктуры : методические рекомендации / С. А. Винокуров [и др.]. – Воронеж : ВИ МВД России, 2018. – Текст : электронный.

31. Ворона, В. А. Концептуальные основы создания и применения системы защиты объектов : справочное издание ; Книга 1 / В. А. Ворона, В.

А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с. – Текст : непосредственный.

32. Ворона, В. А. Инженерно-техническая и пожарная защита объектов : справочное издание ; Книга 4 / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 512 с. – Текст : непосредственный.

33. Системы контроля и управления доступом: методические рекомендации / С. А. Гречаный, М. С. Романов, М. В. Таравков, Д. Ю. Калков. – Воронеж : Воронежский институт МВД России, 2021. – 78 с.– Текст : непосредственный.

Учебное издание

Сергей Анатольевич Гречаный
Александр Викторович Сидоров
Дмитрий Юрьевич Калков

СИСТЕМЫ КОНТРОЛЯ
И УПРАВЛЕНИЯ ДОСТУПОМ

Практикум

Редактор А. Г. Лиопа
Компьютерный набор Д. Ю. Калкова

Подписано в печать 22.07.2022
Формат 60x84 1/16
Усл. печ. л. 6,28
Тираж 100 экз. Заказ № 178

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394065, Воронеж, просп. Патриотов, 53