Разработка проекта внедрения системы контроля и управление доступом

1. Теоретические основы контроля и управления доступом в помещение

1.1 Технологии контроля и управления доступом в помещение

Система контроля и управления доступом (СКУД) - совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.

Основная задача - управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию), включая так же:

– ограничение доступа на заданную территорию.

– идентификация лица, имеющего доступ на заданную территорию.

– учёт рабочего времени;

– расчет заработной платы (при интеграции с системами бухгалтерского учёта);

– ведение базы персонала / посетителей;

– интеграция с системой безопасности, например: с системой видеонаблюдения для совмещения архивов событий систем, передачи системе видеонаблюдения извещений о необходимости стартовать запись, повернуть камеру для записи последствий зафиксированного подозрительного события;

– с системой охранной сигнализации (СОС), например, для ограничения доступа в помещения, стоящие на охране, или для автоматического снятия и постановки помещений на охрану;

– с системой пожарной сигнализации (СПС) для получения информации о состоянии пожарных извещателей, автоматического разблокирования эвакуационных выходов и закрывания противопожарных

дверей в случае пожарной тревоги.

На особо ответственных объектах сеть устройств СКУД выполняется физически несвязанной с другими информационными сетями.

Положительные тенденции развития экономики страны в 2013 году позволяют прогнозировать дальнейшее увеличение спроса на СКУД. К основным традиционным потребителям - государственным режимным организациям, крупным промышленным предприятиям, банкам, бизнес-центрам - добавляются относительно новые: учреждения образования, культуры, медицины.

Общее увеличение потребления СКУД также будет, вероятно, обусловлено расширением функционала самих систем, тенденцией к возрастанию требований к оснащенности объектов техническими средствами обеспечения безопасности ввиду активизации противоправных действий, а также необходимостью модернизации систем, установленных более 5 лет назад.

Существует большое множество типов электронных систем защиты и контроля доступа в помещения. Все они отличаются друг от друга как степенью сложности и надежности, так и удобством обслуживания, что в свою очередь отражается на стоимости системы.

Как правило, все системы защиты сводятся к следующим функциям: обнаружение, опознавание, управление, контроль. Приведенная ниже блок-схема часто приводится в литературе и хорошо отражает функции систем защиты.

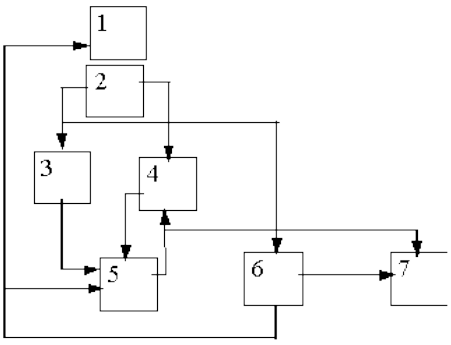

Рисунок 1.1 Схема системы контроля и управления доступом

В данной схеме:

-выявление подлежащих анализу признаков воздействия;

-сравнение выявленных признаков с эталонными;

-выработка запроса статистики опасных воздействий;

-сбор и хранение опасных признаков воздействий;

-выработка управляющих воздействий;

-контроль;

-исполнительный блок;

Выполняемые функции: 1-обнаружение, 2-опознавание 3,5 - управление, 4,6 - контроль, 7-коммутация доступа (или его ограничение).

При выработке подходов к решению проблем безопасности предприятия-производители, как правило, исходят из того, что конечной целью любых мер противодействия угрозам является защита владельца и законных пользователей системы от нанесения им материального или морального ущерба в результате случайных или преднамеренных воздействий на нее. И здесь нужно решить три основные задачи. Это:

) идентификация-процесс распознания определённых компонентов системы, обычно с помощью уникальных, воспринимаемых системой имен (идентификаторов).

) аутентификация-проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы.

) авторизация-предоставление доступа пользователю, программе или процессу.

До сих пор основным средством идентификации являются или магнитные карточки или механические ключи, которые сейчас удачно подделываются и не обеспечивают надежной безопасности объекта защиты. Сейчас начинают получать распространение электронные ключи защиты. Как показывает

мировой опыт в качестве надежного средства распознавания пользователей в настоящее время служат электронные идентификаторы Touch Memory производства фирмы Dallas Semiconductor, Inc. Благодаря гарантированной производителем не повторяемости ключа обеспечивается высокий уровень защищенности объекта защиты.

Анализ литературы приводит к выводу, что для обеспечения эффективной системы защиты и контроля доступа в помещения важно организовать комплексную систему безопасности. Один из лидеров в организации обеспечения систем безопасности фирма «Advance Sucurity Systems» предлагают различное оборудование для ограничения прохода людей и перемещения ценностей. Туда могут входить:

оборудование систем контроля доступа - считыватели, различные типы идентификаторов, сетевые контроллеры, подстанции управления, подстанции сбора информации с датчиков, компьютерные платы и программное обеспечение;

оконечные исполнительные устройства - электромагнитные замки, электрозащелки, электромоторы блокировки дверей;

датчики охраны и сигнализации - инфракрасные датчики (принцип действия - регистрация изменения уровня теплового излучения людей и животных, передвигающихся в охраняемой зоне), вибрационные датчики, ультразвуковые датчики изменения объема, датчики массы и др., сирены, громкоговорители, все различные индикаторы.

системы видеонаблюдения - мониторы, видеокамеры, объективы, коммутаторы, устройства цифровой обработки видеосигнала, знакогенераторы, системы сканирования.

контрольно-пропускное оборудование-турникеты, шлюзы, шлагбаумы, ворота и т.д.

охранно-пожарные системы-извещатели охранные, приборы

приемоконтрольные, аппаратура пожарной сигнализации и др.

системы персонального вызова (пейджеры).

бронированные двери для хранилищ.

центральные пульты-концентраторы и пульты управления.

Перечисленные элементы системы безопасности предлагаемые этой фирмой, а также аналогичными фирмами такими как «BAUER» (Германия-Швейцария), «INTERNATIONAL ELECTRONICS» (США) соответствуют европейским и мировым стандартам, имеют высокую степень надежности, но являются очень дорогими. Поэтому средние и мелкие организации вынуждены искать менее дорогие системы защиты, имеющие невысокую степень надежности.

Среди Российских лидеров в организации обеспечения систем безопасности выделяется компания «КОДОС».

«КОДОС» - российский бренд систем безопасности, завоевавший широкое признание не только у себя на родине, но и за рубежом. Ориентация на потребителя и постоянное внедрение инновационных технологий позволили компании «КОДОС» занять лидирующую позицию на российском рынке технических средств безопасности.

Под брендом «КОДОС» производится продукция для организации систем контроля и управления доступом, охранно-пожарной сигнализации, а также цифрового видеонаблюдения. Основное преимущество продукции «КОДОС» в том, что все системы могут быть интегрированы в единый комплекс безопасности.

Многофункциональность и безупречное качество оборудования и программного обеспечения «КОДОС» позволяют построить надежную систему безопасности на объектах любого масштаба и назначения: от небольшого офиса до крупных предприятий, имеющих сложную многофилиальную структуру.

Результат непрерывного технологического развития компании -

уникальные, часто не имеющие аналогов не только в России, но и за рубежом продукты.

Системы «КОДОС» надежны - качество изделий и программного обеспечения контролируется и на стадии разработки, и при производстве. Вся продукция имеет необходимые сертификаты соответствия требованиям безопасности российских и европейских стандартов.

Система менеджмента качества компании сертифицирована на соответствие требованиям международного стандарта ISO 9001:2008.

Консультации по техническим вопросам и оперативное решение проблемных ситуаций обеспечивает служба технической поддержки клиентов. Подразделение сервисной поддержки компании «КОДОС» осуществляет послепродажное обслуживание оборудования и гарантийный ремонт.

Исходя из вышесказанного можно сделать вывод, что комплексная система безопасности позволяет при помощи мощной центральной процессорной станции осуществлять высоконадежную защиту и эффективный контроль доступа на объект защиты.

Структура технических средств системы контроля и управления доступом в помещения (СКУД) должна представлять собой двухуровневую централизованную систему, работающую в реальном времени. На верхнем уровне - пульт управления (ЭВМ, совместимая с IBM PC), с блоком связи и локальной сетью передачи данных. На нижнем уровне - N контролируемых пунктов (КП). КП - контролируемый пункт, в задачу которого входит защита и контроль контролируемого пункта.

На верхнем уровне пультом управления выполняются функции:

- сбора;
- документирования;
- архивирования;
- представления на видеотерминал информации.

Для этих целей лучше всего подходит ПЭВМ совместимая с IBM PC. Применение ПЭВМ по сравнению со специализированным пультом удобнее тем, что ПЭВМ обеспечивает широкие функциональные возможности и гарантирует гибкость и удобство в эксплуатации. Кроме того, при дальнейшей модернизации системы или ее расширения не потребуется дополнительных аппаратных затрат на пульт управления, а нужно изменить только управляющую программу.

На нижнем уровне выполняются функции сигнализации, управления, регулирования и контроля. Функцию контроллера выполняет однокристальный микропроцессор, который имеет физическую и логическую раздельность памяти программ и памяти данных. Структурная организация, набор команд и аппаратурно-программные средства ввода / вывода информации такого микропроцессора очень хорошо приспособлены для решения задач управления и регулирования в приборах, устройствах и системах автоматики, а не для решения задач обработки данных. Кроме того, массовый выпуск однокристальных микропроцессорных наборов БИС с их широкими функциональными возможностями, их низкая стоимость, гибкость и точность цифровых методов обработки информации превратили МП в системные элементы, на основе которых создаются системы промышленной автоматики, связи, измерительной техники и т.д.

Можно сказать, что назначение системы, это обеспечение безопасности. Под безопасностью СКУД будем понимать ее свойство, выражающееся в попытках нанесения ущерба владельцам и пользователям системы при различных возмущающих (умышленных и неумышленных) воздействиях на нее. Обеспечение безопасности СКУД в целом предполагает создание препятствий для любого несанкционированного вмешательства в процесс ее функционирования, а также попыток хищения, модификации, выведения из строя или разрушения ее компонентов, то есть защиту всех компонентов

системы: оборудования, программного обеспечения, данных и персонала.

По мере развития и расширения применения средств вычислительной техники острота проблемы обеспечения безопасности систем и хранящейся в них информации от различных угроз все возрастает. Основная из них - возросший уровень доверия к автоматизированным системам обработки данных. То есть система помимо выполнения функции защиты и контроля должна быть сама защищена, как на нижнем уровне, так и на верхнем. Доступ к ресурсам системы, а особенно к ПЭВМ должен быть максимально ограничен и надежно защищен. Вероятность подбора индивидуального кода должна быть не менее 10-6. Как показывает мировой опыт при такой вероятности подбора, система, в плане подбора идентификационного номера пользователя, практически надежна. Такую вероятность может обеспечить электронный идентификатор.

Первичным источником электропитания пульта управления и контролируемого пункта должна быть однофазная сеть переменного тока напряжением 220 вольт и частотой 50 герц. При кратковременных авариях в системе энергоснабжения должен быть обеспечен перезапуск и восстановление предаварийного состояния пульта управления и контролируемого пункта.

Так как СКУД предусматривает персональный вызов (ситуация - к пользователю пришел гость, который не идентифицируется системой), то система должна обеспечить надежную радиосвязь и работоспособность между передатчиком на входе КПП и пейджерами, установленными в удаленных помещениях. Максимальное удаление охраняемых помещений, где установлены пейджеры от передатчика, должно быть не менее 200 метров.

Электрическая составляющая электромагнитного поля помех в помещениях не должна превышать 0.3В на 1 метр согласно ГОСТ 16325-88.

Должна быть предусмотрена автономная шина заземления технических средств для подключения корпусов устройств, экранов, кабелей. Контур

заземления должен быть автономным, то есть несвязанным гальванически с контуром заземления каких-либо промышленных помещений. Сопротивление заземляющего устройства между клеммой земли контролируемого пункта, пульта управления и землей (грунтом) не должно превышать 4-ех ом в любое время года.

В линиях связи должны использоваться приемники с высоким входным сопротивлением, малой входной емкостью и предпочтительно с гистерезисной передаточной характеристикой для увеличения помехозащищенности. Шины питания и земли должны обладать минимальной индуктивностью. Кроме того, линия связи должна быть защищена от паразитных импульсных токов в оплетке кабеля из-за связи с источником помех через паразитную емкость между источником помех и оплеткой.

В проектируемой системе компьютер должен взаимодействовать с внешними устройствами (контроллерами). Для этой цели в мировой практике используется несколько стандартов и множество устройств, которые работают со стандартными интерфейсными схемами. Один из наиболее распространенных интерфейсных стандартов называется RS-232C (Reference Standart N232 Revision C), сигналы которого приведены в приложении. Благодаря очень небольшому расстоянию (несколько сантиметров) между различными узлами внутри контроллера шлюза уровни сигналов, используемых для предоставления двоичных данных, зачастую весьма малы. Например, распространенным логическим семейством, используемым в контроллере шлюза, является транзисторно-транзисторная логика (ТТЛ), в которой для представления двоичной единицы используется сигнал напряжением от 2 до 5 В, а для представления двоичного нуля - сигнал напряжением от 0,2 до 0,8 В. Напряжения вне этих диапазонов порождают неопределенное состояние: в худшем случае, если уровень напряжения близок к одному из этих пределов, то воздействие даже небольшого понижения сигнала или небольшой

электрической помехи может привести к ошибке. Поэтому при подключении контроллеров к компьютеру уровни напряжений обычно выше тех, которые используются для соединения отдельных элементов внутри некоторого узла. На практике фактически используемые уровни зависят от источников напряжений, подаваемых на схемы интерфейса; в проектируемой системе предполагается использовать напряжения +12 В. Схемы передачи преобразуют низкие уровни сигналов в более высокие, тем самым обеспечивая связь по моноканалу между компьютером и контроллерами шлюзов. Приемные схемы выполняют обратную функцию. Схемы согласования интерфейса также выполняют необходимые преобразования напряжений.

Относительно высокие уровни напряжений в интерфейсе значительно уменьшают влияние электрических помех по сравнению с их воздействием на уровни ТТЛ.

Предполагается использовать стандартную скорость передачи в стандарте RS-232C равную 9600 бит/сек.

1.2 Компоненты системы контроля и управления доступом

Система контроля и управления доступом обычно состоит из следующих основных компонентов:

- устройства идентификации (идентификаторы и считыватели);
- устройства контроля и управления доступом (контроллеры);
- устройства центрального управления (компьютеры);
- устройства исполнительного (замки, приводы дверей, шлагбаумов, турникетов и т.д.).

В зависимости от применяемой СКУД на объекте, отдельные ее устройства могут быть объединены в один блок (контроллер со считывателем) или вообще отсутствовать (персональный компьютер).

Устройство идентификации доступа (идентификаторы и считыватели) считывает и расшифровывает информацию, записанную на идентификаторах разного типа и устанавливает права людей, имущества, транспорта на перемещение в охраняемой зоне (объекте). Контролируемые места, где непосредственно осуществляется контроль доступа, например, дверь, турникет, кабина прохода, оборудуются считывателем, устройством исполнительным и другими необходимыми средствами.

Идентификатор - предмет, в который (на который) с помощью специальной технологии занесена кодовая информация, подтверждающая полномочность прав его владельца и служащий для управления доступом в охраняемую зону. Идентификаторы могут быть изготовлены в виде карточек, ключей, брелоков и т.п.

Считыватель - электронное устройство, предназначенное для считывания кодовой информации с идентификатора и преобразования ее в стандартный формат, передаваемый для анализа и принятия решения в контроллер.

Наиболее широкое распространение получили следующие виды идентификаторов и считывателей.

Карточка перфорированная - карточка из двухслойной недеформируемой пластмассы. Информация записывается на ней с помощью пробивки специальных отверстий один раз при изготовлении. Считывание информации осуществляется оптическим или механическим считывателями. Данная карточка самый простой и дешевый тип идентификатора, но который практически не обеспечивает секретность кода и легко подделывается. Срок службы карточки 1-2 года.

Карточка со штриховым кодом - карточка с нанесенными на поверхность полосами иного цвета, чем остальная поверхность, ширина и расстояние между которыми представляют собой кодовую последовательность. Кодовая последовательность наносится на карточку при ее изготовлении (обычно она

определяется генератором случайных чисел), и в дальнейшем не может быть изменена. Код считывается оптическим считывателем (инфракрасным или лазерным). Самые распространенные системы штрихового кодирования, код 39 (3 из 9) и код 25 (2 из 5).

Карточка магнитная - карточка с магнитной полосой, на которой записан код. Данный тип носителя является самоочищающимся и не оставляет окислов на считывателе. При желании код, записанный на дорожках магнитной полосы может быть легко перепрограммирован, а при утере карточки можно быстро, дешево и без проблем закодировать новую карточку. Код с карточки считывается магнитным считывателем, принцип работы которого аналогичен считывателю обычного магнитофона: информация считывается при перемещении карточки между магнитными головками считывателя. Карточки с магнитной полосой являются дешевыми, но не очень надежными, так как существует вероятность их подделки. К их недостаткам можно также отнести наличие механического контакта при считывании с головками считывателя, который сокращает срок службы (средний срок службы 1 год) и необходимость очень аккуратного обращения, связанного с возможностью искажения или уничтожения записанной информации в относительно слабых магнитных полях и температур окружающего воздуха свыше 80 °С.

Виганд-карточка - карточка с содержащимися внутри обрезками тонких металлических проволочек, расположенных в определенном порядке, представляющем собой кодовую комбинацию. Расположение проволочек на карточке фиксируется специальным клеем, после этого переориентация проволочек не возможна. При перемещении данной карточки в магнитном поле считывателя проволочки создают магнитный импульс, несущий информацию записанную на карточке. Такой тип карточек не подвержен воздействию электромагнитных полей и высоких температур окружающего воздуха. Подделка практически исключена. Считыватели могут работать вне помещений,

так как все их электронные компоненты залиты специальным защитным компаундом. Недостатком является то, что карточки хрупкие и могут быть повреждены при изгибе. Кроме того, код каждой карточки записывается в нее при изготовлении и не может быть изменен. В настоящее время один из самых перспективных типов идентификаторов.

Карточка бесконтактная (Proximity) - карточка, внутри которой расположена микросхема (чип) с записанной в ней информацией. Информация с таких карточек считывается радиочастотным способом на расстоянии от 5 до 90 см (для автомобильных идентификаторов данного типа расстояние считывания достигает 2 м). Карточки делятся на активные и пассивные. В пассивных карточках информация записывается один раз на все время действия карточки, а в активных существует возможность изменения информации в микросхеме. Пассивные карточки питаются энергией, получаемой от считывателя, срок службы их неограничен и они не могут быть подделаны. Активные - имеют встроенные, незаменяемые батарейки, срок работы которой обычно достаточно велик - до 10 лет. В надежности эти карточки уступают Виганд-карточкам, но они более удобны в применении. Считыватель может быть скрытно размещен за не металлической стенкой. Эта технология идеально сочетает эффективный контроль со свободой перемещения. Информация с карточки может быть считана, даже если она находится в кошельке или кармане. Недостатком является невозможность работы при воздействии сильных электромагнитных полей. Эта карточка незаменима для случаев, когда необходимо обеспечить высокую пропускную способность, скрытность места установки считывателя или дистанционный контроль доступа.

Электронные ключи «Touch Memory» выполнены в виде брелоков. Все необходимые данные записываются на заключенную в них микросхему. Запись, добавление или стирание ключа осуществляется мастер-ключом из контроллера. Считывается информация при касании ключом считывателя.

Микросхема, как правило, питается от вмонтированной в ключ батарейки. Срок ее работы достаточно велик - несколько лет, но рано или поздно ключ подлежит замене. Ключ очень надежен в работе, устойчив к механическим, электромагнитным воздействиям. Широко применяются в небольших СКУД, когда необходимо контролировать большое количество дверей при малом количестве пользователей.

Кроме перечисленных выше могут использоваться идентификаторы следующих типов:

с использованием цифровой клавиатуры (PIN-код). Носителем информации является пользователь, набирающий на клавиатуре замка личный код (условное число) и, если он верен, то получаете право доступа. Это наиболее простое и дешевое средство контроля доступа, но которое легко обходится. Хотя, в последнее время, появились клавиатуры, у которых после каждого нажатия, изменяется порядок цифр на клавиатуре по случайному закону, что исключает возможность «подсмотреть» порядок нажатия кнопок или определить наиболее часто используемые кнопки;

биометрические - считывание индивидуальных физических признаков личности (отпечатки пальцев, рисунок ладони, голос и т.д.). Основное преимущество биометрического контроля - это полное решение задачи контроля доступа - идентифицируется личность человека, а не какой-либо предмет (карточка). По причине очень высокой стоимости, малой оперативности и большого объема машинной памяти, занимаемой одним таким «слепком ключа» они применяются чрезвычайно редко, в основном в учреждениях с повышенной секретностью. Для повышения быстродействия биометрического контроля, как - минимум на порядок, совместно с ним используется любой другой способ идентификации.

Контроллеры - электронные устройства, контролирующие работу считывателей и управляющие устройствами исполнительными.

Контроллеры бывают однофункциональными и многофункциональными.

Основное функциональное назначение - это хранение баз данных кодов пользователей, программирование режимов работы, прием и обработка информации от считывателя, принятие решений о доступе на основании поступившей информации, управление исполнительными устройствами и средствами оповещения.

Наиболее существенными дополнительными функциями контроллеров являются:

защита от повторного использования карточки, т.е. повторный вход по данной карточке возможен только после «ее выхода»;

наличие и возможности программирования временных зон;

наличие релейных выходов для подключения средств оповещения, телевизионного оборудования и т.д.;

возможность подключения охранной сигнализации;

возможность установки двух и более считывателей на одну дверь для организации двухстороннего прохода или многоуровневого контроля.

На практике применяются контроллеры, рассчитанные на управление до 8 считывателями. Все контроллеры, используемые на объекте, в свою очередь могут быть объединены в единую систему и подключаться либо к ведущему контроллеру (мастер-контроллеру), либо к компьютеру, управляющему работой всех контроллеров. Обычно ведущий контроллер отличается от остальных только заложенной программой. К нему же может подключаться управляющий компьютер, принтер и другие периферийные устройства. Однофункциональные контроллеры являются интеллектуальным аналогом кодового замка и работают только в автономном режиме.

Многофункциональные контроллеры не только управляют доступом, но и обладают функциями мониторинга состояния устройств исполнительных и вывода данных на компьютер и печать. С помощью многофункциональных

контроллеров можно создавать сложные комплексы, интегрированные с другими подсистемами безопасности, например, с охранно-пожарной сигнализацией и телевизионными системами видеоконтроля. Связь контроллеров между собой в единую сеть осуществляется через стандартный интерфейс RS-485. Для связи ведущего контроллера с компьютером используется стандартный интерфейс RS 232. Многофункциональные контроллеры работают в основном в сетевом режиме (централизованный контроль и управление доступом).

Персональный компьютер предназначен для программирования СКУД, получения информации о пользователях системы, дате и времени прохода пользователей через контрольные устройства, срабатывании средств охранно-пожарной сигнализации, видеоконтроля, попыток, несанкционированного прохода, аварийных ситуациям и т.п.

Для работы в СКУД может использоваться любой персональный IBM - совместимый компьютер. Наряду с работой в составе СКУД он может выполнять и другие функция, т. к. компьютер нужен в основном лишь для программирования системы и получения отчетов о работе системы. Персональный компьютер, используя специально разработанное для охраняемого объекта программное обеспечение (желательно русифицированное), осуществляет общее управление и программирование СКУД, собирает информацию с контроллеров, создает общий банк данных, формирует различные отчеты и сводки. Русифицированное программное обеспечение под MSDOS и Windows позволяет осуществлять автоматическую запись данных по всем операциям входа / выхода. В любой момент можно запросить разнообразные сведения, например, о местонахождении сотрудников и посетителей. Текущее состояние СКУД отображается в удобной графической форме. В компьютер вводится план охраняемого объекта, на котором стандартными значками указываются считыватели, замки, технические средства

охранно-пожарной сигнализации, видеоконтроля и т.п. На плане система автоматически в реальном масштабе времени показывает состояние всех нанесенных объектов контроля - открыта или закрыта дверь, какой именно извещатель сработал в случае тревоги. Таким образом, в любой момент времени можно быстро оценить ситуацию и в случае внештатной ситуации оперативно и эффективно принять меры предосторожности.

Устройства исполнительные принимают команды управления с контроллеров и обеспечивают блокировку возможных путей несанкционированного проникновения через устройства заграждения (двери, ворота, турникеты, кабины прохода и т.п.) людей, имущества, транспорта в помещения, здания и на территорию.

В устройствах исполнительных применяются исполнительные механизмы электромеханического и электромагнитного принципа действия.

Электромеханический принцип действия исполнительного механизма основан на перемещении закрывающих элементов (запоров, ригелей замков и т.п.) с помощью включения на время их передвижения электромотора или электромагнита.

В исполнительных механизмах с электромагнитным принципом действия отсутствуют движущиеся механические закрывающие элементы, т.е. блокировка устройств заграждения, например дверей, осуществляется с помощью сил магнитного притяжения, создаваемых мощным магнитом.

Часто в устройствах исполнительных применяется электромагнитная блокировка (магнитные защелки, задвижки и т.п.) закрывающих элементов с возможностью перемещения их вручную при открывании или закрывании в экстремальных условиях.

Для возвращения устройств заграждения в закрытое состояние, они дооборудуются специальными устройствами - доводчиками, без которых СКУД теряют свою основную функцию - ограничения доступа, так как без них

устройство заграждения может находиться в любом состоянии. По виду исполнительного механизма доводчики подразделяются на пружинные, пневматические, гидравлические и электромеханические.

Функция доводчика - не только гарантировать закрытие устройства заграждения (например, двери), но и оберегать замок от механических ударов, а при пожаре автоматически раскрывать двери и помогать эвакуации. В некоторых типах доводчиков используется, так называемая «система торможения с подтягом» - вначале доводчик дает разогнаться, потом тормозит движение и уже в конце, у самой дверной коробке, резко подтягивает дверь, обеспечивая гарантированное ее закрытие. Кроме того некоторые доводчики могут иметь встроенный режим безопасности, исключающий случайное придавливание человека в момент прохождения через устройство заграждения.

Критериями оценки СКУД являются основные технические характеристики и функциональные возможности.

К основным техническим характеристикам относятся:

уровень идентификации;

количество контролируемых мест;

пропускная способность;

количество пользователей;

условия эксплуатации.

По уровню идентификации доступа СКУД могут быть:

одноуровневые - идентификация осуществляется по одному признаку, например, по считыванию кода карточки;

многоуровневые - идентификация осуществляется по нескольким признакам, например, по считыванию кода карточки и биометрическим данным.

Но количеству контролируемых мест СКУД может быть:

малой емкости (до 16);

средней емкости (от 16 до 64);

большой емкости (более 64).

По условиям эксплуатации различают системы (части систем) для работы:

в закрытых отапливаемых помещениях;

в закрытых неотапливаемых помещениях;

под навесом на улице в условиях умеренно-холодного климата;

на улице в условиях умеренно-холодного климата;

в особых условиях (повышенная влажность, запыленность, вибрации и т.п.).

К основным функциональным возможностям относятся:

возможность оперативного перепрограммирования;

схемно-техническая и программная защита от вандализма и саботажа;

высокий уровень секретности;

автоматическая идентификация;

разграничения полномочий сотрудников и посетителей по доступу в помещения и на объект в целом;

надежное механическое запирание контролируемых мест с возможностью аварийного ручного открытия;

автоматический сбор и анализ данных;

выборочная распечатка данных.

По техническим характеристикам и функциональным возможностям СКУД условно подразделяются на четыре класса. В зависимости от особенностей объекта, конфигурации СКУД, фирмы изготовителя набор функций в каждом классе может изменяться и дополняться функциями из других классов.

2. Анализ деятельности ООО «Новые информационные технологии»

.1 Организационно-управленческая характеристика ООО «Новые информационные технологии»

Общество с ограниченной ответственностью «Новые Информационные Технологии» является коммерческой организацией, учрежденной участниками общества для ведения предпринимательской деятельности в сфере разработки и монтаже видеонаблюдения и других систем безопасности. Общество создано в соответствии с Гражданским Кодексом Российской Федерации, федеральным законом «Об Обществах с ограниченной ответственностью» и осуществляют свою деятельность на основе самофинансирования и самоокупаемости, в соответствии с настоящим указом и действующим законодательством Российской Федерации.

Общество имеет в собственности обусловленное имущество, учитываемое на его самостоятельном балансе, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде.

ООО «Новые Информационные Технологии» может иметь гражданские права и нести гражданские обязанности, необходимые для осуществления любых видов деятельности, не запрещённых действующим законодательством Российской Федерации, если это не противоречит предмету и целям, деятельности, определённым уставом.

ООО «Новые Информационные Технологии» в праве в установленном порядке открывать банковские счета (в т.ч. валютные) на территории Российской Федерации и за её пределами.

ООО «Новые Информационные Технологии» имеет круглую печать, содержащую ее полное фирменное наименование на русском языке и указание

на место нахождения.

ООО «Новые Информационные Технологии» вправе иметь штампы и бланки со своим фирменным наименованием, собственную эмблему, а также зарегистрированный в установленном порядке товарный знаки другие средства индивидуализации.

Компания «Новые Информационные Технологии» была основана в 2009 году командой профессионалов, долгое время проработавших на рынке высоких технологий. Основными направлениями деятельности стали поставки розничным и корпоративным клиентам компьютерной и оргтехники, услуги по обслуживанию компьютеров и специализированного программного обеспечения.

Основные принципы работы - это профессионализм специалистов компании в сочетании со стремлением предложить клиенту наиболее выгодные условия сотрудничества, обеспечение качественного гарантийного и пост гарантийного обслуживания наших клиентов.

За относительно недолгое время работы Компания «Новые Информационные Технологии» стала основным поставщиком услуг и оборудования для таких известных организаций как:

- Автосалон 2000;
- Аппарат уполномоченного по правам человека;
- Бюро медико-социальной экспертизы по Оренбургской области;
- Государственное бюджетное учреждение культуры «Оренбургский областной музей изобразительных искусств»;
- Оренбургоблгаз;
- Оренбургский государственный университет;
- Оренбургская таможня;
- Управление Федеральной службы государственной регистрации, кадастра и картографии по Оренбургской области;

- Оренбургский государственный областной театр кукол;
- Управление жилищной политики администрации города Оренбурга;
- Управление образования администрации города Оренбурга и Оренбургского района;
- Управление финансового обеспечения Министерства обороны Российской Федерации по Оренбургской области;
- Фабрика Оренбургских пуховых платков;
- Южно-Уральский филиал ОАО «Федеральная пассажирская компания РЖД»;
- Финансовое управление администрации г. Оренбурга;
- Центр по обеспечению мероприятий ГО и ЧС;
- МРСК Волга Центральные Электросети;
- МРСК Волга Городские Электросети;
- Банк Пушкино;
- Главное управление по делам и центра обеспечения МЧС Оренбургской области;
- Министерство и управление образования;
- Оренбургграждансторой;
- Управление Федеральной службы государственной регистрации, кадастра и картографии по Оренбургской области;
- Завод Инвертор;
- Южно-Уральский филиал ОАО «Федеральная пассажирская компания РЖД»;
- Оренбургэнерго МРСК Волга ГЭС;
- Юничел-Оренбург;
- МТС-банк;
- УФСИН России по Оренбургской области;

Динамичному развитию компании, совершенствованию предлагаемых

нами решений и внедрению новых технологий способствуют надежные партнерские отношения с крупнейшими фирмами-производителями в области информационных технологий.

Специалисты компании осуществляют индивидуальный подход к каждому клиенту, учитывая его возможности и предпочтения.

ООО «Новые Информационные Технологии» работает на рынке информационных технологий с 2009 года и, не смотря на такой короткий промежуток времени, специалисты компании научились оказывать партнерам, высокое качество сервиса по продаваемой продукции и услугам. ООО «Новые Информационные Технологии» многопрофильная организация и может полноценно удовлетворять потребности клиентов и решать любые возникающие вопросы в области IT.

Отдел продаж работает по наличному и безналичному расчету, предоставляет гибкие цены, скидки, быстрые сроки поставки, принимает к оплате карты MasterCard, VISA, Maestro, оформляет кредит на покупку по выгодным условиям.

Отдел Информационных Технологий оказывает информационную поддержку и полное сопровождение системы электронного документооборота казначейской программы СЭД. Выполняет IT-аутсорсинг (абонентское и разовое обслуживание парка компьютеров, оргтехники, сетей и программного обеспечения). Выполняет услуги по автоматизации и обслуживанию различных конфигураций 1С.

Сервисный центр заправляет картриджи, ремонтирует любую офисную технику. Занимается антивирусным лечением, ремонтом компьютеров, ноутбуков и мониторов любой сложности.

ООО «Новые Информационные Технологии» предлагает услуги по отправлению бухгалтерской отчетности через интернет (ИФНС, ПФР, ФСС) по выгодным ценам.

Компанией «Новые Информационные Технологии» налажено собственное производство компьютеров, сертифицированное по международному стандарту ISO 9001-2000. Компания готова предложить собственные модели, в которых используются только самые надежные комплектующие известных брендов. Специалисты компании всегда следят за развитием компьютерного рынка и своевременно меняют модельный ряд. Консультанты помогают подобрать необходимую комплектацию. Компания «Новые Информационные Технологии» наиболее полно удовлетворит потребности в поставке новой техники с учетом ее совместимости с ранее приобретенным оборудованием.

Каждому корпоративному клиенту предоставляется персональный менеджер, помогающий в решении всех возникающих проблем и при необходимости привлекающий к их решению других специалистов Компании.

ООО «Новые Информационные Технологии» отличается гибкостью при работе с клиентами, предоставляя им персональные скидки, различные формы оплаты и отсрочки платежей.

При участии ООО «Новые Информационные Технологии» клиенты компании обеспечат себе успешное участие в тендерах.

Юридический адрес ООО «Новые Информационные Технологии»: 460000, Российская Федерация, Оренбургская область, г. Оренбург, ул. Комсомольская д. 28.

Директором ООО «Новые Информационные Технологии» является Тюрин Дмитрий Алексеевич.

Дата регистрации ООО «Новые Информационные Технологии» 05.05.2009.

Регистратор: Межрайонная инспекция ФНС России 10 по Оренбургской области.

Телефон: 8 (3532) 305-500.

Факс: 8 (3532) 305-101.

Часы работы с понедельника по пятницу: с 09-00 до 19-00.

Часы работы с субботы по воскресенье: с 10-00 до 17-00.

Перечень некоторых услуг:

Информирование об объявленных закупках - поиск и предоставление информации об объявленных государственных и муниципальных закупках;

Подготовка конкурсных, аукционных, котировочных заявок - оформление необходимых документов для участия, предложений о функциональных (качественных) характеристиках, о сроках, о гарантиях и им подобных документов в полном объеме;

Экспертиза - анализ причин результатов размещенного заказа, анализ условий тендерной документации, анализ тендерных заявок участников;

Высококачественное обслуживание корпоративных клиентов - одна из составляющих успеха и процветания компании. Для корпоративного рынка Оренбургской области в сфере ИТ-Индустрии характерна самая высокая конкуренция, поэтому компания «Новые Информационные Технологии» с повышенным вниманием и заботой относится к своим корпоративным клиентам;

Корпоративным партнером является клиент, регулярно закупающийся в компании по безналичному и наличному расчету;

Возможна доставка товара до склада корпоративного партнера;

Предоставление индивидуального менеджера;

Цена товара определяется индивидуально менеджером компании и подлежит обсуждению с клиентом с возможной корректировкой в меньшую сторону;

При необходимости партнеру предоставляется отсрочка платежа;

Гарантийное обслуживание корпоративных партнеров, как правило, осуществляется в течение от 1 до 3 дней в зависимости от сложности поломки.

Также компания осуществляет другие работы и оказание других услуг, не

запрещенных и не противоречащих действующему законодательству РФ. Отдельными видами деятельности, перечень которых установлен действующим законодательством, общество вправе заниматься на основании разрешения (лицензии).

Финансовой основой деятельности общества является уставный капитал, который определяет минимальный размер имущества общества, гарантирующего интересы его кредиторов. Размер уставного капитала общества не может быть менее суммы, определенной действующим законодательством.

По виду выполняемых работ - комплексно-специализированная, т.е. выполняющая комплекс работ.

Так же можно сказать что по численности работающих организацию можно отнести к малым организациям так как численность рабочего персонала не превышает ста человек.

Одно из направлений деятельности ООО «Новые Информационные Технологии» - абонентское обслуживание компьютерной техники. Сегодня многие организации столкнулись с проблемой поддержки парка техники в работоспособном состоянии устройств, в необходимости сборки, монтажа и настройки серверов, сетей и программного обеспечения. Конечно, ряд компаний имеют в своём штате системного администратора, но это не единственное верное решение. По ряду причин порой наем специалиста по обслуживанию компьютеров нецелесообразен. Во-первых, хороший специалист не будет работать за невысокую оплату труда. Во-вторых, абонентское обслуживание компьютеров - мероприятия, скорее, эпизодические, чем постоянные. Чего не скажешь о заработной плате нанятого сотрудника: она, как раз, будет и постоянной, и регулярной. Однако без администрирования и обслуживания компьютерных сетей нормальное их функционирование просто невозможно. Поэтому есть два выхода. Либо держать в штате высокооплачиваемого специалиста, либо воспользоваться предложением Компании «Новые

Информационные Технологии».

Специалисты компании предлагают выгодное решение в области обслуживания компьютеров и техники, которое позволит клиентам значительно сэкономить средства:

- Администрирование локально-вычислительной сети;
- Оптимизация и мониторинг работы локально-вычислительной сети;
- Помощь в выборе, закупке и доставке необходимого оборудования;
- Устранение физических неисправностей в локально-вычислительной сети;
- Регулярный аудит IT-инфраструктуры;
- Консультации в выборе программного обеспечения;
- Установка и инсталляция программного обеспечения с дистрибутивов заказчика;
- Поддержка работоспособности программного обеспечения;
- Установка и консультирование по использованию стандартного ПО.

По мере достижения зрелости и укрупнения бизнеса перед компаниями встает вопрос упорядочивания внутреннего и внешнего документооборота, и перевода его на современную технологичную платформу. Примерно так случилось и в Федеральном казначействе РФ (ФК РФ), где внедрение единой системы электронного документооборота (СЭД) и учетной системы («Центр-КС») имело целью свести все разрозненные учетные системы воедино, чтобы в максимально короткие сроки решать задачи по переходу на обслуживание бюджетов всех уровней. В соответствии с положениями части 1 статьи 215 Бюджетного кодекса РФ с 1 января 2006 бюджеты субъектов РФ и местные бюджеты должны были в обязательном порядке перейти на централизованное кассовое обслуживание именно в ФК РФ. Конечно, это был

постепенный и запланированный процесс, но анализ ситуации показал: за один-два квартала объем документооборота через региональные подразделения Казначейства России увеличится примерно в шесть раз. Чтобы повысить эффективность работы сотрудников территориальных органов ФК на местах, было решено внедрить единую технологию учета всех бюджетных средств на основе программных комплексов «Центр-КС» и специальной системы электронного документооборота СЭД в территориальных органах и центральном аппарате Федерального казначейства. Исполнителем проекта (доработка и внедрение «Центра-КС», создание и внедрение СЭД, и дальнейшее сопровождение до конца 2008 г.) выступила компания ОТР.

Использование ППО СЭД ФК значительно упрощает процесс документооборота с УФК. Однако СЭД является сложной программной системой требующей квалифицированного сопровождения.

Компания «Новые Информационные Технологии» предлагает абонентское обслуживание данного программного продукта. Специалисты компании помогают в решении технических проблем, которые могут возникнуть в ходе работы. Возникшие вопросы обрабатываются квалифицированными специалистами горячей линии, с помощью средств удаленного администрирования. В случае если затруднение невозможно устранить средствами горячей линии, то в организацию направляется специалист для оказания помощи на месте.

Решаемые задачи:

- Настройка и отладка СЭД;
- Обновление СЭД;
- Генерация ЭЦП и подготовка документации в Казначейство;
- Защита вашей базы данных СЭД на случай поломки компьютера;
- Настройка транспортного сертификата;

- Электронные торги;
- Своевременное отслеживание всех изменений связанных с программным продуктом СЭД;
- Тесное сотрудничество с УФК и ОФК по Оренбургской области.

С: Предприятие 8.2 позволяет организовать бухгалтерский, оперативный, кадровый, торговый, складской и производственный учет, а также расчет заработной платы сотрудников. Пользователи могут применять конфигурации, входящие в новую комплексную поставку, как по отдельности, пользуясь средствами обмена данных, так и совместно, подобрав для себя подходящий вариант работы с системой.

Выбор конфигурации зависит, прежде всего, от решаемых задач, от типа деятельности и структуры конкретного предприятия, уровня сложности ведения учета и других условий. Бухгалтерский учет, а также учета зарплаты и кадров, в значительной степени универсальны - они подходят большинству предприятий всех видов деятельности. А торговый учет, в соответствии со своим названием, делает конфигурацию ориентированной на предприятия, занимающиеся торговой деятельностью.

В рамках 1С сопровождения выполняются следующие виды работ:

- Обновление релизов конфигураций программных продуктов и форм регламентированной отчетности (для подписчиков ИТС);
- Консультации и обучение пользователей по использованию продуктов семейства 1С: Предприятие;
- Выполнение регулярных профилактических работ: резервное копирование, тестирование и исправление базы данных;
- Настройка интерфейсов и разграничение прав доступа к базе данных системы «1С: Предприятие»;

А также дополнительные виды работ в рамках 1С:

- Разработка руководства пользователя по использованию программного обеспечения для выполнения конкретных бизнес операций;
- Настройка продуктов 1С: Предприятие под особенности Вашего предприятия: разработка и модификация существующих справочников, отчетов, документов, внесение изменений в план счетов и т.д.
- Помощь пользователям в обнаружении и устранении допущенных ими ошибок при вводе данных, в т.ч. в не типовых (изменённых) конфигурациях.

Возможность самостоятельного выбора тарифного плана, исходя из реальных потребностей организации. Обладая информацией о затраченном времени и оценив реальные потребности организации в ежемесячном сопровождении, клиент сможет выбрать тарифный план, оптимально подходящий, реально экономящий издержки на сопровождении любых программных продуктов системы «1С: Предприятие».

Тарифные планы

Наименование	Тариф 1 4000 р	Тариф 2 6500 р	Тариф 3 8000 р
Консультирование по телефону и удаленное администрирование, которое включает в себя настройку отчетов, отладку, оптимизацию и обновление. Первые 10 мин бесплатно (Инцидент не фиксируется).	Не более 5 Инцидентов	Не более 7 Инцидентов	Не более 10 Инцидентов
Плановый абонентский выезд. Время выезда определяется исполнителем и согласовывается с заказчиком.	1 выезд	1 выезд	1 выезд
Внеплановый выезд. Время выезда определяется заказчиком и согласовывается со специалистом службы поддержки отдела автоматизации. Не использованные вызовы на следующий месяц НЕ переносятся.	1 выезд	2 выезда	3 выезда
Пребывание специалиста у заказчика	Не должно превышать 3 часа в рамках рабочего дня	Не должно превышать 5 часов в рамках рабочего дня	Не должно превышать 8 часов в рамках рабочего дня
Время прибытия специалиста	В течение 3 дней	В течение 2 дней	В течение 1 дня

Реальная возможность прогнозировать свои платежи по абонентскому обслуживанию программных продуктов системы «1С: Предприятие», четкий контроль над текущими платежами и их планирование.

Закрепление за клиентской организацией конкретного ответственного специалиста, знающего специфику организации, особенности работы программы для бухгалтерии и других продуктов 1С. На все вопросы и замечания сможет ответить специалист, реально владеющий ситуацией и историей автоматизации клиентской организации.

Каждый поступающий звонок в зависимости от характера возникшего вопроса направляется специалистам Компании, или закрепленному за организацией специалисту отдела внедрения, который в кратчайшие сроки решит все возникшие вопросы.

Монтаж ЛВС

Монтаж локально-вычислительных сетей (ЛВС) обеспечивает пользователей рядом преимуществ:

- Получение и отправка любого вида информации с любого рабочего места;
- Добавление, перемещение или удаление рабочих мест внутри офиса в свободном порядке;
- Быстрые темпы наращивания системы оборудования без дополнительных финансовых затрат на кабельную сеть.

Создание локальной сети и комплексное использование ее ресурсов дает возможность значительно снизить расходы организации на приобретение дополнительного периферийного оборудования и модернизацию структуры в дальнейшем. Кроме того, монтаж локальных сетей существенно повышает уровень безопасности хранения различных данных, имеющих особую важность для предприятия.

Создание локальной сети обеспечит непрерывность доступа пользователей к особо важным данным, соответственно сократив затраты времени на выполнение поставленных задач и обмен служебной информацией. Как следствие, уровень продуктивности рабочего персонала повышается в несколько раз.

Для команды специалистов компании практически не существует невыполнимых задач. Многолетний опыт успешной работы в сфере своей деятельности позволяет выполнять монтаж ЛВС любых объемов и уровня сложности. Услуги компании ориентированы как на крупные предприятия, так и на частных лиц.

Монтаж видеонаблюдения

Системы видеонаблюдения предназначены для получения телевизионных изображений с охраняемого объекта. Выполняют функцию защиты объектов от краж, вандализма, несанкционированного проникновения, иных противоправных действий, а также функцию защиты от пожаров и чрезвычайных ситуаций.

Современная техника видеонаблюдения достаточно сложна, для её оптимального подбора и правильной установки требуется опыт и профессиональный подход. Специалисты компании обладают навыками и опытом установки систем различной сложности и выполнят работы качественно, в оптимальные сроки.

Сотрудники ООО «Новые Информационные Технологии» подбирают для клиентов оптимальное решение, помогают в выборе камер видеонаблюдения, подсказывают, что следует и чего не следует покупать, объясняют все нюансы и тонкости того или иного оборудования.

Сервисный центр компании предлагает услуги по комплексному обслуживанию компьютерного оборудования.

ООО «Новые Информационные Технологии» предлагает оперативное

решение всех технических вопросов, возникающих в гарантийный и постгарантийный периоды: консультирование, ремонт, частичная или полная модернизация оборудования, установка ПО, проведение профилактических работ, поставка комплектующих, запасных частей и расходных материалов.

Специалисты компании проводят сервисное и техническом обслуживание оргтехники, копиров, принтеров, ксероксов, факсов, мониторов, ИБП.

Также проводиться заправка картриджей для факсов, копиров, принтеров, ремонт оргтехники копиров, принтеров, факсов, МФУ таких фирм производителей, как Xerox, HP, Sharp, Mita, Canon, Epson, Panasonic, и т.д.

Ремонт ноутбуков.

В компании ремонтируют опытные мастера, в следствии чего клиенты получают качественный ремонт ноутбуков.

Виды работ:

- ремонт и замена матрицы ноутбука (замена экрана, ремонт экрана ноутбука);
- замена лампы подсветки, ремонт инвертора ноутбука (ремонт подсветки ноутбука);
- любой ремонт материнских плат, в том числе VGA-чипов (ремонт видеокарты ноутбука, ремонт видео-чипа ноутбука);
- ремонт и замена клавиатуры ноутбука;
- ремонт и замена корпусных частей ноутбука;
- ремонт разъемов ноутбука (ремонт гнезда питания ноутбука);
- ремонт системы охлаждения ноутбука (ремонт вентилятора ноутбука);
- замена модулей памяти и жесткого диска ноутбука;
- ремонт и замена внешних блоков питания (ремонт питания

ноутбуков, ремонт зарядного устройства ноутбука);

- замена аккумулятора ноутбука;
- ремонт / замена CD-DVD дисковода ноутбука;
- снятие пароля BIOS ноутбука;
- полный комплекс услуг по настройке ПО, драйверов ноутбука.

Специалисты могут выполнить следующие работы:

- комплексная диагностика работы компьютера;
- замена неисправных модулей в компьютере;
- апгрейд (увеличение производительности компьютера);
- обнаружение и удаление вирусов с зараженного компьютера;
- установка любого лицензионного программного обеспечения.

Компания может предложить для вашего предприятия различные схемы обслуживание парка оргтехники. В случае подписания договора на обслуживание, клиенту будет предложена дилерская колонка на закупку расходных материалов. Данная услуга поможет оптимизировать расходы на поддержание техники в рабочем состоянии по следующим пунктам:

- затраты на IT(айти) специалистов;
- закупка расходных материалов и комплектующих.- аутсорсинг компании включает полную гарантированную поддержку для своих клиентов, поэтому производится регулярный мониторинг, а также предоставляются соответствующие консультации:
- установка и настройка серверов;
- прокладка и настройка локальных сетей;
- проектирование и монтаж сетей;
- заправка и ремонт картриджей;

- ремонт оргтехники;
- ремонт компьютеров и ноутбуков;

Все это позволяет обеспечить эффективность работы - результат достигается качественной работой и гарантированной поддержкой.

Сервисный центр компании «Новые Информационные Технологии» предлагает новый вид услуг - выдача актов технического заключения о не ремонтопригодности и утилизации электронного оборудования.

Компания предоставляет все необходимые документы, разрешающие производить технический осмотр комплектующих, предоставлять экспертную оценку о нецелесообразности ремонта (в случае если эксплуатация невозможна и ремонт превышает стоимость деталей). В результате Сервисный центр предоставляет акт технического заключения. Далее клиент передает пакет документов в свою бухгалтерию, которая производит списание основных средств с баланса предприятия.

Компания «Новые Информационные Технологии» является официальным представителем утилизирующей компании, которая зарегистрирована в Пробирной палате.

Когда списание произведено, при желании заказчика можно приступить к процессу утилизации. Процесс включает в себя этап разборки оборудования и передача частей этой техники на переработку и аффинаж. Переработке будут подвергнуты те компоненты, которые могут быть вновь использованы в качестве исходного сырья (черные и цветные металлы, пластик). Аффинажный завод ожидает детали, содержащие драгоценные металлы. Эти металлы после будут переданы в государственный фонд драгоценных металлов и драгоценных камней. На основании всех данных, переданных на аффинаж, выдается паспорт о содержании драгметаллов.

Все необходимые документы (лицензии, акты, счета фактуры и др.) предоставляются.

Перечень услуг:

- Выдача акта технического заключения - 250 руб.;
- Утилизация системного блока - 200 руб.;
- Утилизация монитора - 250 руб.;
- Утилизация ПЭВМ - 400 руб.;
- Утилизация сервера - 500 руб.;
- Утилизация копировального аппарата А4 / принтера А4 - 300 руб.;
- Утилизация копировального аппарата А3/ принтера А3 - 500 руб.;
- Утилизация АТС - 400 руб.;
- Утилизация факса - 200 руб.;
- Утилизация ИБП - 200 руб.;
- Утилизация активного сетевого оборудования - 150 руб.;
- Утилизация картриджа - 50 руб.

ООО «Новые Информационные Технологии» при согласовании с директором в пределах средств, направляемых на оплату труда, определяет численность работников, ставки, оклады, размеры надбавок, премий и других выплат стимулирующего характера, а так же размеры и порядок выплаты авторского, постановочного и исполнительского вознаграждения в соответствии с Законом РФ» Об авторском праве и смежных правах».

ООО «Новые Информационные Технологии» - организация с вертикальной структурой управления, т.е. имеет несколько уровней управления. Организационная структура, показывает область ответственности каждого отдельного сотрудника и его взаимоотношения с другими сотрудниками, если все взаимосвязи организационной структуры применены правильно, то они ведут к гармоничному сотрудничеству и общему стремлению выполнить поставленные перед организацией цели и задачи. Структура предприятия ООО

«Новые Информационные Технологии» - это деление организации на отдельные элементы, каждый из которых имеет свою четко определенную, конкретную задачу и обязанности, т.е. модель, предусматривает деление персонала на группы, в зависимости от конкретных задач, которые выполняют сотрудники.

Во главе ООО «Новые Информационные Технологии» стоит директор, которому подчиняются все работники.

В процессе анализа информационных потоков предприятия служба контроллинга изучает процессы возникновения, движения и обработки информации, а также направленность и интенсивность документооборота на предприятии.

Цель анализа информационных потоков - выявление точек дублирования, избытка и недостатка информации, причин ее сбоев и задержек.

Наиболее распространенный и, по-видимому, самый практичный метод анализа информационных потоков - составление графиков информационных потоков. Для построения графиков информационных потоков следует знать (или выработать самим) определенные правила их составления и условные обозначения отдельных элементов.

Каждый информационный поток - единичное перемещение информации - имеет следующие признаки:

– документ (на чем физически содержится информация);

– проблематику (к какой сфере деятельности предприятия относится информация);

– исполнителя (человека, который эту информацию передает).

К графику информационных потоков прилагают расшифровку информационных связей на организации или в подразделении.

Составленный график информационных потоков имеет существенный недостаток - большое количество информационных связей затрудняет его чтение и анализ, но именно анализ информационных потоков и являлся целью

составления графика. Поэтому целесообразно разрабатывать графики, изображающие не статические связи между отделами, а поток документов, связанный с выполнением какой-то определенной рабочей задачи.

2.2 Анализ существующей системы технического и программного обеспечения ООО «Новые информационные технологии»

Средние параметры имеющихся в наличии ПК (в целом компьютеры мало различаются по производительности, но конфигурация подобранна специально для комфортной работы сотрудников):

- Процессор AMD Athlon II X2 245 2.9 GHz 2Mb Socket-AM3 OEM;

материнская плата: Asus SOCKET-FM2 F2A55-M LE A55;

ОЗУ: DRR3 2 Гб;

HDD SSD 2.5» SATA-3 250Gb Samsung 840 [MZ-7TD250BW] Samsung_MDX (R530, W240MB, s);

дисковод: Привод SATA DVD±RW LiteOn (iHAS120, 122, 124) Black DVD-20x, 8x, 20x, R9-8x, DL-8x, CD48x, 32x, 48x;

- монитор: Acer 19» V196Lbd.

Файл-сервер обеспечивает хранение больших объемов информации и распределенный доступ к ней. Этот компьютер запускает операционную систему и управляет потоком данных, передаваемых по сети. Через него осуществляется выход в интернет.

Характеристики сервера:

) Корпус: Miditower INWIN EAR002 <Black-Silver> ATX 450W (24+2x4+6 пин).

) Центральный процессор: Intel Core i5-3470 3.2 ГГц/4core/SVGA HD Graphics 2500/1+6Мб/77 Вт/5 ГТ/с LGA1155.

3) RAM: Crucial <CT51264BA160B> DDR-III DIMM 4Gb <PC3-12800>

CL11 (2 шт.).

) HDD: 1 Tb SATA 6Gb/s Seagate Barracuda <ST1000DM003> 3.5» 7200 rpm 64Mb (2 шт.).

) CD ROM: DVD RAM & DVD±R/RW & CDRW Optiarc AD-7280S <Black> SATA (OEM).

) Материнская плата: GigaByte GA-H77-DS3H rev1.0/1.1 (RTL) LGA1155 <H77> 2xPCI-E+Dsub+DVI+HDMI+GbLAN SATA RAID ATX 4DDR-III.

Все устройства локальной сети объединены UTP кабелем через общий коммутатор D-Link <DES-3552> Switch 52 port (48UTP 10 / 100Mbps + 2UTP1000BASE-T+ 2Combo 1000BASE-T / SFP).

Работа на всех компьютерах осуществляется в среде Windows 7 Максимальная, и сервера на Windows server 2008R2.

На всех компьютерах компании установлен стандартный набор программного обеспечения:

- Microsoft Office System Professional 2007 и 2010;

«1С Бухгалтерия»;

WinRAR;

Skype;

AIMP3;

QuickTime;

Adobe Acrobat Reader;

Adobe finereader;

- User gate;

Доступ в Internet в организации осуществляется через оптоволоконный кабель. Для доступа к интернет ресурсам используются стандартные программные средства Windows: Internet Explorer. Интернет в организации предоставляется по средствам оптоволоконной связи и раздаётся через файловый сервер, также в организации установлена мощная точка доступа

D-link.

Для безопасности хранимой информации используется антивирус kaspersky endpoint security для бизнеса стандартный - комплексная защита, включающая в себя: антивирус, анти шпион, анти спам, персональный файервол, а также приложение, которое обеспечивает обновление и централизованное администрирование в корпоративных сетевых средах или глобальных сетях.

3. Разработка проекта внедрения системы контроля и управления доступом «Кодос» в ООО «Новые информационные технологии»

.1 Обоснование выбора системы контроля и управления доступом

На сегодняшний день количество производителей систем контроля и управления доступом достаточно большое. Производством занимаются как иностранные, так и Российские компании. Проведем обзор некоторых систем контроля и управления доступом иностранных и отечественных производителей.

В России делают надежные и приемлемые по цене, для большой массы заказчиков, системы. Но когда речь идет о системах для больших распределенных объектов, когда необходимо обрабатывать огромные массивы данных с большим количеством событий, количеством посетителей в десятки тысяч, встает вопрос о производительности контроллеров, детальной проработке программного обеспечения, надежных алгоритмов интеграции с другими подсистемами.

Постоянный российский потребитель СКУД ведущих зарубежных производителей - это, в том числе, иностранные компании. Точнее, их представительства в Российской Федерации. Дело в том, что офисы большинства сетевых структур оборудуются в соответствии с достаточно жесткими корпоративными стандартами, которые распространяются и на технические средства безопасности. А для штаб-квартиры сетевой компании офис в Москве или Екатеринбурге ничем не отличается от любого другого офиса, будь он в Бразилии, Словении или Германии.

Для того чтобы оборудование того или иного производителя попало в корпоративный стандарт, мало делать качественную технику, хотя, как правило, известный и сильный бренд - по сути, синоним качества и надежности. Есть еще

одно непременное условие: производитель должен быть реальным участником международного рынка.

Международный бизнес - это когда у компании есть представительства и дистрибуторы в странах, являющихся серьезными потребителями СКУД, и когда она имеет не просто опыт работы в какой-то конкретной стране, а тот опыт, опираясь на который может успешно вести бизнес в любом регионе мира.

Надо отметить, что сегодня во многих российских компаниях также разработаны собственные корпоративные стандарты на применяемые в офисах и на других объектах технические средства безопасности. Заказчиками СКУД ведущих зарубежных производителей становятся, прежде всего, крупные компании: банки, промышленные предприятия, офисные центры.

Но далеко не всегда речь идет об инсталляции крупных систем. Очень гибкий западный рынок предлагает потребителям огромный ассортимент систем. Вам необходимо надежно закрыть от несанкционированного доступа две двери небольшого офиса? Выбрав СКУД одного из ведущих брендов, вы сделаете это легко, быстро и надежно. Для вашего объекта нужна сетевая СКУД? Можете быть уверены, что найдете среди предложений европейских и американских производителей лучшее решение. Проектируете интегрированную систему безопасности для крупного территориально распределенного объекта? Большинство из имеющихся на рынке зарубежных СКУД позволяют обеспечить построение на объекте интегрированной системы безопасности, включающей видеонаблюдение, а также охранную и пожарную и сигнализации.

Практически любая из систем имеет неограниченные возможности для наращивания. Даже автономные устройства зачастую имеют централизованный режим работы, который используется при необходимости расширения системы.(США)

Многоуровневая СКУД высшей степени надежности с интегрированной

ОС имеет древовидную, иерархическую структуру с выделенными центральными контроллерами: AAN-100, AAN-32 и интеллектуальными дверными модулями СКУД AIM-4SL/2SL/1SL. Обеспечивает аппаратное хранение карт и событий сразу на двух уровнях. Система может комплектоваться также охранными и релейными панелями AIO-168/16/8, панелями отображения состояния ASA-72, панелями управления автоматикой здания (лифты и проч.). Самые мощные контроллеры AAN-100 могут управлять 96 считывателями, помнят до 1'240'934 номеров карт, позволяют подключать до 512 охранных шлейфов и 608 релейных выходов на один контроллер.

Все контроллеры могут подключаться к компьютеру, с которого можно осуществлять их программирование, управление доступом и контроль событий с записью их на ПК. В тоже время все они могут работать полностью автономно, сохраняя протокол событий и выдавая его на компьютер по первому требованию. Соединение с компьютером осуществляется по RS-232/RS-485 или по Ethernet, соединение центральных контроллеров с подчиненными модулями и охранными панелями возможно как по RS-485, так и по Ethernet, что позволяет строить современные СКУД на основе IP технологий. Управляющие программные комплексы (ПК) для работы с оборудованием APOLLO - ПК APACS 3000 и ПК LyriX.

Оборудование позволяет организовать сложные режимы доступа: вход по двум картам, режим ограничения количества лиц в помещении или группе помещений, объединенных в одну зону, временной и зонный antipassback, ограничение попыток набора кода, «доступ под принуждением» и прочее.

В свою очередь, программные комплексы APACS 3000 и LyriX обеспечивают широкие сервисные функции, дополняющие возможности оборудования APOLLO. Среди них можно упомянуть учет рабочего времени, контроль всех событий в системе, прямое интерактивное управление оборудованием и системой с планов объекта, выдачу отчетов по заданным

критериям, интеграцию с оборудованием сторонних производителей для создания интегрированных систем безопасности (ИСБ) и прочее.

WIN-PAK Professional Edition (Honeywell)

WIN-PAK® Professional Edition - новейшая версия программного обеспечения Honeywell для систем контроля и управления доступом и комплексных интегрированных систем безопасности. Профессиональная версия поддерживает контроллеры СКУД серий PW-5000, PRO2200, N-1000, NStar NS2+, а также новые контроллеры со встроенным Web-сервером NetAXS. В отличие от программных продуктов других фирм-производителей, WIN-PAK реализован в виде набора служб Windows, работающих в фоновом режиме. Это обеспечивает исключительную устойчивость системы вне зависимости от действий оператора. Программа имеет Web-интерфейс для выполнения всех функций и поддерживает работу на нескольких мониторах.

Для каждого владельца карты можно фиксировать в базе данных не только фотографию, но и изображения документов, автомобиля или портативного компьютера. Это позволяет контролировать проход сотрудников и посетителей с оборудованием. В новую версию добавлены функции работы с электронной почтой, что позволяет автоматически формировать и рассылать отчеты и сообщения о событиях по E-mail. Отчеты о частоте использования карт дают возможность выявлять и деактивировать не используемые в системе карты.

Контроллеры PW-5000 и PRO2200 позволяют реализовать практически любые алгоритмы управления исполнительными устройствами благодаря встроенной программируемой логике, дающей возможность на аппаратном уровне контроллера связывать события и действия (процедуры), выполняемые в системе.помощью электронной системы учета посетителей LobbyWorks, также интегрированной в WIN-PAK, теперь можно управлять доступом посетителей и выдавать карты с ограниченным уровнем доступа, действительные только на

время визита. Карты автоматически становятся неактивными после окончания визита посетителя.PAK предоставляет полную интеграцию с цифровыми видеорегистраторами (например, Fusion), аналоговыми и IP-камерами. События, происходящие в различных подсистемах безопасности, связываются с фрагментами видео для возможности визуального контроля происходящих или уже произошедших событий. Функция слежения за перемещением позволяет отображать в реальном масштабе времени список людей, находящихся в любом помещении, и подсчитывать их количество.

Система контроля доступа Casi Rusco (GE)

Система контроля доступа Casi Rusco уникальна тем, что это единственная в своем роде система, которая устойчиво работает с очень большим количеством считывателей и поддерживает операционные системы как Windows, так и Linus/Unix, и базы данных не только SQL, но и Oracle, DB2. Практически все системы в мире, имеющие в своем составе 3000 и более считывателей, построены на Casi Rusco. Всего установлено более 10 000 систем на Windows и более 000 систем на Linus/Unix в 65 странах.

Большие системы Casi Rusco строятся на ОС Linus/Unix на платформе Picture Perfect 4.0, соответствующей запросам крупных корпораций с множеством объектов и высокими требованиями к производительности. Платформа Picture Perfect 4.0 - эксклюзивный Java-клиент, она устойчива к вирусным атакам, имеет неограниченную расширяемость. Пользовательские отчеты, настраиваемый интерфейс, интеграция/XMLAPI, резервирование серверов с использованием технологии PXNplus, поддержка платформ AIX и Linux - эти и другие функции системы неизменно привлекают пользователей.

Другое решение Casi Rusco - от малых до крупных распределенных систем - это Facility Commander для ОС Windows (FCWnx) с гибкими возможностями для интеграции видео и других подсистем.имеет единый пользовательский интерфейс, возможность предоставления информации от

систем в едином формате, уменьшения времени оценки и принятия решения. Снабжена такими функциями, как автоматическое событийное управление, открытая БД и API для интеграции.имеет три версии: Professional (до 5 клиентов и 256 считывателей), Enterprise (до 50 клиентов и 4000 считывателей), Global (до 64 региональных серверов уровня Enterprise).

При этом обе системы (Picture Perfect и FCWnx) имеют единую линейку контроллеров серии M (M5, M2000, M3000) с поддержкой до 16 считывателей и подключением по RS485 и Ethernet.

Кроме того, в Casi Rusco имеется сетевой IP-контроллер DirecDoor, который является надежной альтернативой IP-считывателям. Он устанавливается на каждую дверь, питается через Ethernet и поддерживает два считывателя, что позволяет создать распределенную недорогую систему, обладающую при этом всеми преимуществами Picture Perfect и FCWnx.

Система Casi Rusco имеет в своем составе специальные Transition Readers - переходные считыватели, поддерживающие четыре формата карт доступа: GE Proximity, HID, MIFARE, VICINITY. Все перечисленные форматы карт могут одновременно поддерживаться в единой базе данных СКД, это позволяет поддерживать в одной системе арендаторов с разными форматами карт.

Системы контроля и управления доступом Nedap-AEOS (Голландия)- это мощная, удобная для пользователя система контроля доступа и управления безопасностью, основанная на интеллектуальной сетевой технологии. В AEOS основные функциональные возможности формируются согласно пожеланиям конечного пользователя путем передачи информации между равноправными узлами сети и гибкими поведенческими компонентами. Используя новейшую информационную технологию, AEOS предлагает надежное и ориентированное на перспективу решение всех ваших вопросов безопасности в настоящее время и в будущем.

Легкая в использовании, доступная без ограничений AEOS основана на

интернет-технологии. Это означает, что вы можете подключиться к системе с помощью веб-браузера с любого компьютера: из другого офиса, с другого рабочего места, из дома или даже когда вы путешествуете.

Децентрализация информации AEOS основана на принципе децентрализованных данных. Все права доступа и программированные действия определяются и обрабатываются на самом низком уровне системы. Это означает, что управление системой и необходимый уровень безопасности гарантированы, несмотря на доступность сети или сервера. Система AEOS может функционировать независимо от сервера. Собственные IP-контроллеры AEOS (AEpu) могут напрямую связываться друг с другом и с другими IP устройствами, например, с камерами наблюдения.

Расширяемая AEOS создана из множества различных аппаратных модулей и программных компонентов, что позволяет изменять ее конфигурацию в соответствии с вашими требованиям, используя стандартные компоненты. В случае изменения ситуации вы можете быстро и легко адаптировать или расширить используемые аппаратные модули и поведенческие компоненты (встроенное программное обеспечение). Для передачи информации система AEOS использует существующую инфраструктуру ЛВС. Собственные IP-контроллеры AEOS могут подсоединяться из любого места к сети TCP/IP Ethernet 10/100 Мбит. Для связи между контроллерами и сервером используется VPN-соединение.была создана для того, чтобы предоставить возможность устанавливать систему управления безопасностью с наименьшими усилиями и затратами. Именно поэтому ПО лицензируется непосредственно по фактически используемым функциональным возможностям, т.е. заказчик платит только за те функции, которыми пользуется.

Российские профессиональные системы контроля доступа (СКУД) Parsec. Продукция Parsec широко известна и пользуется заслуженным авторитетом на рынке систем безопасности не только в России, но и за рубежом. Оборудование

и программное обеспечение под торговой маркой Parsec выпускается с 1997 года. Производитель профессиональных систем контроля и управления доступом Parsec - ООО «НПО Релвест».

Выпускаемый спектр продукции позволяет комплексно решать задачи по оснащению различных объектов, от небольшого офиса до крупных территориально-распределенных предприятий, системами контроля и управления доступа (СКУД) и, что самое главное, задачи обеспечения с их помощью высокого уровня безопасности.

Продукция Parsec отвечает самым высоким стандартам качества. Зачастую уникальные, не имеющие аналогов не только в России, но и за рубежом продукты, - результат непрерывного технологического развития компании. Успех продукции начинает формироваться уже на стадии разработки изделий и программных продуктов.

Высокотехнологичное производство и 100% выходной контроль изделий обеспечивает качество и надежность работы СКУД. Оперативное решение всех возникающих вопросов на протяжении всего срока службы систем обеспечивают компетентные специалисты технической поддержки.

На сегодняшний день компания специализируется на создании и производстве продукции по трем основным направлениям:

Системы контроля доступа ParsecNET.

Программно-аппаратные комплексы, предназначенные для решения задач безопасности на объектах любого типа, начиная от офисов небольших компаний, и заканчивая территориально и административно распределенными крупными объектами. Глубокая интеграция систем контроля доступа (СКД), охранно-пожарной сигнализации и видеонаблюдения позволяет обеспечить максимальную эффективность и удобство работы со всей системой.считыватели.

Продукция Parsec включает широкий спектр устройств для чтения

идентификаторов наиболее распространенных стандартов: с рабочей частотой 125 кГц и частотой 13,56 МГц. Считыватели Parsec совместимы с самыми популярными форматами идентификаторов: Em Marin, HID Corporation, Motorola (Indala Corporation), Mifare ® (NXP Semiconductors). Различные конструктивные исполнения, поддержка протоколов Wiegand 26 и Touch Memory, позволяют использовать данные устройства как в составе сторонней системы контроля доступа (СКД), так и для решения задач автоматизации в платежных и транспортных приложениях.

Система дальней идентификации.

Система, работающая на частоте 2,45 ГГц, обеспечивает уникальные в своем классе технические характеристики. Предназначена для решения широкого круга задач в самых разных областях: идентификация автотранспорта, обеспечение безопасности, логистика и складской учет, автоматизация производства и т.д. Техническая реализация считывателя и активных меток в сочетании с гибко программируемыми режимами и логикой работы выгодно отличают систему от аналогичных решений мировых производителей.

Система контроля и управления доступом TSS2000 Profi («Семь печатей»)

Программная часть СКУД TSS2000 Profi - совокупность модулей, взаимодействующих по TCP/IP протоколу по принципу клиент-сервер. Ядро системы реализовано как службы Windows. СУБД - Firebird.

Количество кодов ключей неограниченно, (автономный режим - 65 025). Объем журнала событий неограничен (автономный режим - 250 000). Число маршрутов доступа неограниченно. Число расписаний неограниченно (автономный режим - 16).

СКУД TSS2000 Profi может быть построена как локальная система с тремя способами подключения оборудования: непосредственно к серверу СКУД, к серверам оборудования, через ЛВС (число контролируемых пунктов

прохода от 1 до 2032). Второй вариант построения - распределенная система с синхронизацией баз данных неограниченного числа локальных СКУД (в том числе по медленным линиям связи), что позволяет вести единую систему регистрации персонала и формирования отчетов о рабочем времени (число контролируемых пунктов неограниченно).

В состав системы (кроме ядра и программ администрирования) входят модули «Бюро пропусков», «Проходная», «Мониторинг работы» (в текстовом и графическом виде), «Отчеты». Дополнительное ПО: «Создание и печать пропусков», «Учет рабочего времени», «Регистрация посетителей», сигнальная система, система видеонаблюдений, интеграция с внешними системами безопасности, система импорта-экспорта данных.СКУД Tempo Reale (ОАО НПП «Альфа-Прибор»)Reale - это универсальная система, базирующаяся на контроллерах серии АПДА и предназначенная для управления доступом абонентов в соответствии с назначенными правами, автоматизированного учета рабочего времени и контроля за трудовой дисциплиной.

Благодаря архитектурным особенностям СКУД Tempo Reale как IP-решения обеспечивается ее надежность, высокая пропускная способность, быстрое развертывание на объекте и легкое масштабирование.

Контроллеры серии АПДА могут использоваться как в автономном режиме, так и в составе сетевой СКУД под управлением ПО Tempo Reale. АПДА.21 и АПДА.41 рассчитаны на подключение соответственно до 2 и 4 считывателей с интерфейсом Weigand и обеспечивают управление исполнительными устройствами различных барьеров (дверей, ворот, турникетов, шлюзовых кабин и т.п.).

Благодаря наличию дополнительных входов и выходов контроллеры АПДА позволяют реализовать самые разнообразные режимы доступа и алгоритмы ответных реакций системы на возникающие внештатные ситуации (связи событий).

Несомненным преимуществом контроллеров АПДА является наличие сетевого порта Ethernet, что позволяет строить территориально распределенные системы с возможностью удаленного мониторинга и управления устройствами, входящими в состав системы.

Особого упоминания заслуживает новый IP-контроллер АПДА.21. Впервые для систем российского производства организация контроля повторного входа (anti-passback) и связей событий осуществляется на уровне «контроллер-контроллер», что увеличивает надежность и отказоустойчивость системы при потере связи с центральным сервером. Кроме того, разработчики наделили АПДА.21 внутренней памятью на 20 000 карт и 30 000 событий и возможностью питания по Ethernet (PoE).

Программная составляющая системы - ПО Tempo Reale - это клиент-серверное решение, которое предоставляет пользователю возможности контролировать события в системе в режиме реального времени, напрямую управлять оборудованием СКУД, автоматизировать учет рабочего времени, включая построение более 20 видов отчетов и унифицированного табельного листа по форме Т-13.

На программном уровне IP-СКУД Tempo Reale поддерживает интеграцию с IP-камерами AXIS, что позволяет выполнять видеоверификацию доступа абонентов в контролируемые зоны и осуществлять запись видеофрагментов, соответствующих системным событиям.

Система контроля и управления доступом GATE («Равелин»)

СКУД GATE представляет собой гибкий, легко масштабируемый программно-аппаратный комплекс на базе контроллеров GATE-4000, одного или нескольких компьютеров со специализированным программным обеспечением, считывателей, исполнительных и внешних устройств.

СКУД GATE была создана как универсальная система, которая имеет различные области применения: офисы в бизнес-центрах, промышленные

предприятия, учебные заведения, парковки, столовые крупных предприятий, спортивные комплексы. Система GATE - конструктор, имеющий огромный потенциал и способный решить задачи различной степени сложности.

СКУД GATE проста и удобна (система строится на базе единственного типового контроллера), сохраняет работоспособность при отказе компьютера или обрыве связи. Гибкость и масштабируемость системы дает возможность свободно расширять ее при необходимости. Система может быть интегрирована («Интеллект», Essel, Laguna, 1С др.), имеет европейский сертификат качества CE.

Система состоит из контроллеров GATE (до 255 в линии), компьютера со специализированным программным обеспечением, считывателей (HID, EM-Marine, Mifare, радиобрелоки), исполнительных устройств (замки, турникеты, шлагбаумы и др.)

Возможности GATE - это до 8144 пользователей и до 7 расписаний на каждую точку прохода, локальный буфер на 4095 событий в каждом контроллере (при пропадании связи события не теряются), сохранение всех событий в компьютере.

Система генерирует отчеты, имеет функцию непосредственного управления с компьютера, ведет мониторинг текущих событий системы в реальном времени. Есть также функции выдачи временных пропусков, поддержки фотоверификации, организации удаленных рабочих мест.

Программное обеспечение GATE предназначено для:

• Настройки и конфигурирования системы.

• Определения контроллеров, считывателей и расписаний.

• Работы с пропусками, изменения прав доступа.

• Мониторинга в реальном времени.

• Контроля за перемещениями.

• Чтения событий из памяти контроллеров и сохранения их в компьютере.

• Получения отчетов.

• Учета рабочего времени персонала.

• Фотоверификации.

• Контроля оставшихся сотрудников.

Системы контроля и управления доступом (СКУД) КОДОС - эффективные автоматизированные контрольно-пропускные системы, которые позволяют управлять безопасностью объекта и осуществлять контроль доступа. СКУД, собранная «под ключ», исполняет несколько функций:

разграничение доступа сотрудников;

регистрацию посетителей;

электронный учет посетителей;

учет рабочего времени персонала;

многое другое.

Правильный выбор контрольно-пропускной системы влияет и на безопасность предприятия, и на комфорт сотрудников. СКУД «КОДОС», благодаря многозадачности и возможностям модификации системы, способны удовлетворить эти потребности заказчика в полной мере.

Автоматизированная пропускная система контроля и управления доступом (СКУД) «КОДОС» - современный, удобный и эффективный инструмент обеспечения безопасности. В состав системы безопасности входит широкий спектр самых разных устройств контроля доступа:

считывателей

картоприемников

адаптеров

контроллеров

и т.п.

Специально разработанное ПО связывает между собой все элементы системы управления доступом.

СКУД «КОДОС» легко адаптировать под любой тип объекта, а кроме того, она может быть модифицирована в соответствии с изменениями на объекте без нарушений в работе системы. Использование автоматизированных пропускных систем в школе и на предприятии обеспечит постоянный контроль доступа всех посетителей независимо от типа объекта.

Система контроля и управления доступом «КОДОС» решает задачи множество задач, направленных на обеспечение безопасности:

разграничение доступа;

предотвращение несанкционированного проникновения на объект;

организация пропускной системы для сотрудников и гостей;

учет рабочего времени;

контроль действий операторов и охранников;

обеспечение порядка и дисциплины.

Установка пропускной системы «КОДОС» не только решит проблему несанкционированного проникновения на различные объекты предприятия, но и поможет максимально контролировать рабочее время всех сотрудников предприятия.

Программно-аппаратный комплекс СКУД «КОДОС» уже стал неотъемлемой частью корпоративного управления многих компаний. Благодаря СКУД «КОДОС» предприятия во многом оптимизировали рабочий процесс, за счет увеличения уровня безопасности и повышения контроля над персоналом предприятия в целом.

Одно из основных преимуществ системы контроля и управления доступом «КОДОС» - функциональная гибкость и возможность быстрой адаптации под условия конкретного объекта. Поэтапное наращивание системы происходит без демонтажа оборудования.

На базе оборудования «КОДОС» можно построить системы контроля и управления доступом как для небольших офисных помещений, так и для

крупных объектов с распределенной структурой и большим количеством точек доступа. В основе сетевой СКУД лежат контроллеры серий КОДОС RC, КОДОС EC и КОДОС PRO. Сочетание оборудования различных серий позволяет построить на любом объекте систему доступа с оптимальным соотношением цены и функциональности.

Контроллеры СКУД «КОДОС», помимо своего прямого назначения, обеспечивают управление исполнительными устройствами (считывателями СКУД, картоприемниками, турникетами) и контроль охранных шлейфов.

Особенностью комплексной системы обеспечения безопасности «КОДОС» является возможность задавать правила реагирования на те или иные события. К примеру, для автоматизированных систем контроля доступа при считывании запрещенной карты на входе можно предусмотреть команду «привести в действие исполнительное устройство звукового оповещения» (сирену) системы охранно-пожарной сигнализации.

К этому же событию можно «привязать» включение видеокамеры для записи или другие технологии безопасности, используемые на конкретном объекте. Работа ИКБ позволяет свести к минимуму влияние человеческого фактора, а внедрение автоматизированной пропускной системы в школе и на предприятии обеспечивает качественно новый уровень безопасности.

Плюсы лучших российских разработок очевидны: действительно высокое качество и надежность, проверенные многими сотнями инсталляций и годами интенсивной эксплуатации на объектах разной сложности. В силу географической близости к заказчику наши производители имеют гораздо больше, нежели их зарубежные коллеги, возможностей, организовать нормальную техническую поддержку. Тот, кто грамотно пользуется этой возможностью, получает очевидное конкурентное преимущество. Нельзя забывать и о том, что лучшие российские СКУД полностью адаптированы к условиям эксплуатации. А это не только суровый климат российских просторов,

но и состояние и возможности электрических сетей, IP-коммуникаций, пока еще далекий от идеала уровень подготовки монтажников и эксплуатационных служб.

Следующий фактор, который зачастую становится решающим при выборе системы, - относительно невысокая цена. Большинство российских СКУД занимают среднюю ценовую нишу, что в сочетании с высоким качеством во многом и объясняет столь значимую долю рынка, которую они занимают.

На шлагбаум Came Gard 4000 возможна установка кодовой клавиатуры или ключа-выключателя, фотоэлементов безопасности или сигнальной лампы непосредственно на корпус шлагбаума (рисунок 2.14), что упрощает монтаж и удешевляет систему. Особенностью всех моделей шлагбаумов серии GARD является самоблокирующийся редуктор, который блокирует стрелу как в открытом, так и в закрытом состоянии.

В случае отсутствия электропитания стрела шлагбаума может быть поднята или опущена вручную. При этом нет необходимости открывать корпус шлагбаума, поскольку механизм разблокировки находится снаружи.

Библиографический список

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник / В.Г. Олифер, Н.А. Олифер - СПб.: Питер, 2008.
2. Щербо В.К. Стандарты вычислительных сетей / В.К. Щербо. - М.: Кудиц-Образ, 2009.
. Основы построения беспроводных локальных сетей стандарта 802.11. Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11 / Педжман Рошан, Джонатан Лиэри. - М.: Cisco Press; пер. с англ. - «Вильямс», 2010.
. Современные технологии беспроводной связи / Шахнович И. - М.: Техносфера, 2011.
. Сети и системы радиодоступа / Григорьев В.А., Лагутенко О.И., Распаев Ю.А. - М.: Эко-Трендз, 2007.
. Анатомия беспроводных сетей / Сергей Пахомов // Компьютер Пресс, 2010. - №7.
. WLAN: практическое руководство для администраторов и профессиональных пользователей / Томас Мауфер. - М.: КУДИЦ-Образ, 2010.
. Беспроводные сети. Первый шаг / Джим Гейер. - М.: Вильямс, 2005.
. Секреты беспроводных технологий / Джек Маккалоу. - М.: НТ-Пресс, 2008.
. Современные технологии и стандарты подвижной связи / Кузнецов М.А., Рыжков А.Е. - СПб.: Линк, 2011.
11. Виталий Леонтьев Интернет. Справочник / Леонтьев Виталий, ОлмаМедиаГрупп, 2011.
12. Лапунов А.И. Интернет. Самоучитель / Лапунов А.И., Ульянов О.В., Прокди Р.Г. - М.: Наука и техника, 2009.
13. Крайзмер Л.П. Персональный компьютер на вашем рабочем месте / Л.П.

Крайзмер, Б.А. Кулик. - СПб.: Лениздат, 1991.

14. Епанешников А.М. Локальные вычислительные сети / А.М. Епанешников, В.А. Епанешников. - СПб.: Диалог-МИФИ, 2005 г. - 224 с.

. Чекмарев Ю.В. Локальные вычислительные сети / Ю.В. Чекмарев. - СПб.: ДМК Пресс, 2009. - 200 с.

. Поляк-Брагинский А. Локальные сети. Модернизация и поиск неисправностей / Александр Поляк-Брагинский. - М.: БХВ-Петербург, 2007. - 640 с.

. Майкл Уэнстром Организация защиты сетей Cisco / Майкл Уэнстром. - М.: Вильямс, 2003.

. Мерит Максим Безопасность беспроводных сетей / Максим Мерит, Полино Дэвид. - М.: Компания «АйТи», ДМК Пресс, 2004. - 288 с.

. Хачиров Т.С. Настраиваем сеть своими руками / Т.С. Хачиров. - СПб.: АСТ, Астрель, Полиграфиздат, 2010. - 96 с.

. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В.Г. Олифер, Н.А. Олифер. - 3-е изд. - СПб.: Питер, 2006. - 958 с.

. «Экономика» / под ред. А.С. Булатова. - М.: БЕК, 1997.

. «Экономика предприятия»: Учебник для вузов, под ред. Е.М. Куприянова. - М.: Банки и биржи, 1996.

. Рошан П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Рошан, Дж. Лиэри. - М.: Издательский дом «Вильямс», 2004. - 304 с.

. Зигуненко С. ОБЖ. Основы безопасности жизнедеятельности / С. Зигуненко. - М.: Изд.: АСТ, 2004.

. Диго С.М. Проектирование и использования баз данных / С.М. Диго. - М.: Финансы и статистика. 1985.

. Самоучитель создания локальной сети: Ю.В. Васильев. - М.: Триумф, 2008. - 160 с.

. Серопегин В.И. Радиотехнологии в сфере WLL / В.И. Серопегин // Технологии и Средства Связи. - №4. - 2000.

. Шахнович И. Современные технологии беспроводной связи: И. Шахнович - СПб.: Техносфера, 2006. - 288 с.

. Стюарт Мак-Клар. Секреты хакеров. Безопасность сетей - готовые решения / Мак-Клар Стюарт, Скембрей Джоэл, Курц Джордж. - 4-е изд. - М.: Вильямс, 2004.

. Уэнделл Одом Компьютерные сети. Первый шаг / Одом Уэнделл. - М.: Вильямс, 2005.

. Феер К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер, под ред. В.И. Журавлева. - М.: Радио и связь, 2000.

. Хизер Остерлох Маршрутизация в IP-сетях. Принципы, протоколы, настройка / Остерлох Хизер. - Изд.: ДиаСофтЮП, 2002.

. Стандарты вычислительных сетей / В.К. Щербо. - М.: Кудиц-Образ, 2000.

. «WLAN: практическое руководство для администраторов и профессиональных пользователей» / Томас Мауфер. - М.: КУДИЦ-Образ, 2005.

. «Анатомия беспроводных сетей» / Сергей Пахомов // Компьютер-Пресс. - №7. - 2002.

. «Базовые технологии локальных сетей» / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 1999.

. «Беспроводные сети. Первый шаг» / Джим Гейер. - М.: Издательство: Вильямс, 2005.

. «Основы построения беспроводных локальных сетей стандарта 802.11. Практическое руководство по изучению, разработке и использованию беспроводных ЛВС стандарта 802.11» / Педжман Рошан, Джонатан Лиэри. - М.: Cisco Press: пер. с англ. - Издательский дом «Вильямс», 2004.

. «Секреты беспроводных технологий» / Джек Маккалоу. - М.: НТ-Пресс, 2005.

. «Сети и системы радиодоступа» / В.А. Григорьев, О.И. Лагутенко, Ю.А. Распаев. - М.: Эко-Трендз, 2005.

. «Современные технологии беспроводной связи» / И. Шахнович. - М.: Техносфера, 2004.

. «Современные технологии и стандарты подвижной связи» / М.А. Кузнецов, А.Е. Рыжков. - СПб.: Линк, 2006.

. Wi-Fi. Беспроводные сети. Установка. Конфигурирование. Использование: Джон Росс - М.: НТ Пресс, 2006 г. - 312 с.

. Владимиров А.А. Wi-Фу: боевые приемы взлома и защиты беспроводных сетей / А.А. Владимиров, К.В. Гавриленко, А.А. Михайловский. - М.: NT Press, 2005.

. Советов Б.Я. Моделирование систем: учебное пособие / Б.Я. Советов. М.: Высшая школа, 2008.