

Пример реализации системы сбора и обработки информации "XVmatic" и интеграции с "ADEMCO", "ШРАК", "Northern Computers"

1. Цели, назначение и области применения системы

Система сбора и обработки информации предназначена для интеграции систем инженерно-технических средств охраны (ИТСО) в единый комплекс с целью повышения эффективности их использования и комплексного предоставления информации о работе систем ИТСО оперативному дежурному, ответственным должностным лицам отделения безопасности и защиты информации и руководству Предприятия.

Цели установки системы сбора и обработки информации:

- регистрация информации о работе систем ИТСО, рабочих мест и оборудования систем ИТСО, изменениях режимов работы систем ИТСО;
- информирование оператора дежурной службы о работе систем ИТСО, тревогах и внештатных ситуациях;
- обеспечение записи и фиксации информации о событиях систем ИТСО и работе системы ССОИ в электронных цифровых архивах хранения данных.
- автоматизированный контроль работы систем ИТСО, сверка с требуемыми параметрами работы систем ИТСО (эталонными) и информирование оператора дежурной службы об обнаруженных расхождениях.

Система была установлена в административном здании Предприятия общей площадью здания – 1900 кв. м. Штатная численность персонала – 120 человек.

На прилегающей территории расположены служебные помещения.

Объект оборудован следующими системами ИТСО:

- Система охранно-тревожной сигнализации (СОТС) на базе оборудования ADEMCO (панели VISTA-501);
- Система пожарной сигнализации (СПС) на базе оборудования ШПРАК;
- Система контроля и управления доступом (СКУД) на базе оборудования Northern Computers и программного обеспечения DSP;
- Электронный сейф ключей СК-24;
- Телевизионная система охраны и наблюдения (ТСОН) на базе оцифровщиков AXIS 240Q Blade, видеосерверов и программного обеспечения XViewision. Всего 86 камер;
- Система охранной сигнализации периметра (СОСП) на базе контроллера «Фокус»;
- Подсистема контроля прохода сотрудников и посетителей по разовым и временным пропускам IDmatic.

Последовательность реализации проекта

Система установлена в несколько этапов в соответствии с планами-графиками.

Общий порядок проведения работы на объекте:

- Поставка материалов.
- Прокладка кабельных трасс.
- Поставка оборудования и программного обеспечения.
- Монтажные работы по установке и подключению оборудования.
- Пуско-наладочные работы.
- Предварительные испытания.
- Опытная эксплуатация.
- Приемо-сдаточные испытания.
- Ввод в промышленную эксплуатацию.

2. Описание процесса деятельности системы

2. 1. Состав подсистем

Система сбора и обработки информации на уровне организации подсистем обеспечивает:

- сбор и обработку информации системы охранно-тревожной сигнализации (СОТС);

- сбор и обработку информации системы пожарной сигнализации (СПС);
- сбор и обработку информации системы охранной сигнализации периметра (СОСП);
- сбор и обработку информации, управление системой контроля и управления доступом (СКУД), включающую в себя подсистему управления аварийными выходами и электронные сейфы ключей.
- сбор и обработку информации, управление телевизионной системой охраны и наблюдения (ТСОН);
- организацию подсистемы контроля прохода сотрудников и посетителей по разовым и временным пропускам;
- фото-идентификацию сотрудников при проходе через шлюзовые кабины по радиокартам;
- организацию подсистемы мониторинга источников бесперебойного питания и контроля параметров окружающей среды в отдельных помещениях;
- автоматическую комплексную обработку информации, управление подсистемами и контроль выполнения регламентов работы персонала и систем объекта на основе программного обеспечения «XVmatic».

2.2. Состав технических средств

Система сбора и обработки информации строится на базе собственной локальной вычислительной сети (ЛВС) и включает в себя следующее оборудование:

- обрабатывающее оборудование (серверные блоки управления и архивации), компьютерные блоки мониторинга и связи с системами СОТС, СПС, СОСП, СКУД;
- оборудование связи и преобразования сигнала от видеокамер ТСОН;
- компьютерный блок мониторинга источников бесперебойного питания;
- серверное оборудование подсистемы контроля прохода сотрудников и посетителей, электронный терминал выдачи радиокарт-пропусков;
- АРМа поста охраны и АРМ администратора (с необходимым периферийным оборудованием);
- локальные источники бесперебойного питания для серверного оборудования и АРМов;
- необходимое оборудование преобразования интерфейсов для организации связи с системами ИТСО;

- активное сетевое оборудование;
- межсетевые экраны АПК Континент-К;
- аппаратные шкафы для установки оборудования;
- кабельные линии связи.

Все оборудование имеет соответствующие Российские сертификаты соответствия.

2.3. Функциональные характеристики системы

2.3.1. Взаимодействие с системами ИТСО

Система выполняет операции считывания или получения по цифровым интерфейсным каналам информации о работе систем ИТСО, обрабатывает полученные данные, записывает их в архивы хранения, отображает состояние систем ИТСО в интерфейсах программ рабочих мест (АРМ) ССОИ, по информации от систем ИТСО выявляет типовые ситуации на объекте с последующим оповещением рабочих мест ССОИ.

В системе ССОИ информация передается между внутренними компонентами в формате mail-smtp и SQL-запросах (в случае работы с базами данных).

Для сбора информации и управления отдельными функциями систем ИТСО используются различные методы подключения интерфейсов и передачи данных.

Система сбора и обработки информации обеспечивает:

- интеграцию систем СОТС, СПС, СОСП, СКУД, ТСОН объекта в единый комплекс;
- информационную связь с системами СОТС, СПС, СОСП, СКУД, ТСОН;
- информационную связь, по существующим оптоволоконным каналам связи, с сегментом ССОИ здания Предприятия;
- протоколирование (запись и хранение) информации поступающей от систем СОТС, СПС, СОСП, СКУД, ТСОН в течение требуемого времени;
- централизованное управление исполнительными устройствами СКУД (настройка полномочий доступа пользователей в помещения и к ключам по картам СКУД, блокирование локальных зон внутри объекта при поступлении сигнала Тревоги, разблокирование отдельных точек доступа и т.п.);
- круглосуточный, непрерывный и автоматический контроль систем СОТС, СПС, СОСП, СКУД, ТСОН источников бесперебойного питания с отображением

информации на мониторах автоматизированных рабочих мест (АРМ) системы, отображение рекомендаций по действиям дежурной службы Предприятия;

- анализ текущего состояния технических средств систем СОТС, СПС, СОСП, СКУД, ТСОИ, источников бесперебойного питания с отображением информации на мониторах АРМ системы;
- автоматический и автоматизированный анализ данных о функционировании ИТСО:
 - анализ и контроль правильности текущих режимов и настроек ИТСО и выдача извещений (сигналов) при выявлении ошибочных и/или неоптимальных режимов и/или настроек;
 - анализ и контроль реакций ИТСО в штатных ситуациях и при происшествиях;
 - расчет показателей надежности и качества технической эксплуатации ИТСО;
 - сравнительный анализ по выбранным параметрам (календарным периодам, техническим средствам, ситуациям, показателям и т.д.).
- автоматический текущий контроль функционирования программного обеспечения ССОИ;
- мониторинг работоспособности оборудования ССОИ;
- обработку и отображение полученной информации на АРМ администратора в виде унифицированных табличных отчетов;
- наглядный графический интерфейс пользователя для отображения ситуационной обстановки на графических планах и необходимой информации о штатных и тревожных событиях на мониторах АРМ с указанием места, даты, времени и характера событий, а также рекомендаций по действиям поста милиции и службы безопасности Предприятия в различных ситуациях;
- звуковое (в т.ч. голосовое) сопровождение при отображении критических состояний контролируемых объектов;
- простоту конфигурирования системы – изменение алгоритмов работы и параметров конфигурации системы без остановки действующей системы;
- дистанционное управление режимами работы и настройками оборудования ССОИ;
- внесение изменений, модернизацию, замену версий программного обеспечения без изменения настроенных алгоритмов работы системы;
- автоматическое резервное копирование баз данных и текущих установок;

- защита собственных ресурсов ССОИ и технических средств при попытках несанкционированного доступа к ним;
- синхронизацию внутренних часов АРМ и серверного оборудования системы по часам одного (центрального) сервера;
- синхронизацию часов центрального сервера с эталонными сигналами времени другого объекта Предприятия;
- разграничение доступа пользователей (операторов и администраторов) системы к функциям ССОИ;
- доступ к информации о состоянии систем СОТС, СПС, СОСП, СКУД, ТСОИ, протоколам событий в соответствии с категориями доступа к информации;
- протоколирование действий операторов и администраторов ССОИ во время работы;
- контроль присутствия операторов и администраторов ССОИ на рабочем месте (периодическое подтверждение с вводом пароля);
- отображение на экранах мониторов АРМ системы окон со служебными сообщениями о тревогах и внештатных ситуациях с указанием места расположения события на графическом плане, видеоизображения с расположенных рядом видеокамер, звуковым сопровождением;
- документирование (протоколирование) всей поступающей информации с указанием места происшедшего события, его характера, времени и даты;
- подготовка и печать отчетов по событиям ССОИ.

2.3.1.1. Взаимодействие с СОТС

Информация о событиях СОТС передается с панелей VISTA-501 (оборудование ADEMCO) системы охранной и тревожной сигнализации через интерфейсное соединение RS-232 на приемный порт Блока регистрации событий сигнальных панелей VISTA Fractal-C-010/КО. Программа регистрации событий СОТС, входящая в состав ПО Блока, обеспечивает прием информации в текстовом виде (ASCII-символы), разбор по событиям, перевод данных событий в формат mail-smtp и отправку сообщений в архив событий ССОИ и АРМ ССОИ.

Система сбора и обработки информации регистрирует следующие события СОТС:

- Информация о состоянии раздела сигнализации;
- Взятие и снятие раздела с охраны (с данными о пользователе СОТС);
- Взятие и снятие зоны с охраны;

- Раздел готов;
- Раздел не готов;
- Связь с панелью потеряна;
- Связь с разделом потеряна;
- Тревога сигнализации;
- Нарушение в зоне ОПС;
- Обход зоны ОПС;
- Запуск сервера;
- Остановка сервера;
- Информация о работоспособности сервера (с программируемым периодом).

2.3.1.2. Взаимодействие с СПС

Информация о событиях СПС передается из управляющего контроллера ШПРАК системы пожарной сигнализации по интерфейсу RS-232 на преобразователь интерфейса ПИ I-7188E3-232, а далее по ЛВС ССОИ на приемный порт контроллера мониторинга пожарной сигнализации Fractal-19"-002/КР. Программа регистрации событий СПС, входящая в состав ПО контроллера мониторинга пожарной сигнализации, обеспечивает прием информации в текстовом виде (ASCII-символы), разбор по событиям, перевод данных событий в формат mail-smtp и отправку сообщений в архив событий ССОИ и АРМ ССОИ.

Система сбора и обработки информации регистрирует следующие события СПС:

- Запуск сервера;
- Остановка сервера;
- Информация о работоспособности сервера (с программируемым периодом);
- Чтение конфигурации системы;
- Связь с панелью потеряна;
- Тревога (извещатель);
- Тихая тревога (извещатель);
- Ревизия тревоги (извещатель);
- Загрязнение извещателя;
- Аппаратная тревога (панель);
- Выход из строя (панель);
- Исследование (панель);

- Помеха (панель);
- Предупреждение (панель);
- Прогон бумаги (панель);
- Ревизия помехи, активации (панель).

2.3.1.3. Взаимодействие с СОСП

Система охранной сигнализации периметра СОСП построена на базе оборудования ПКП «Фокус-3М». Информация о срабатывании СОСП через преобразователи интерфейса АПК-01 и I-7188ЕЗ-232 по локальной сети поступает на блок управления, в архив событий и на АРМы ССОИ.

Оборудование «Фокус-3М» формирует два типа сообщений - канальное и общее.

Канальное сообщение формируется при:

- постановке любого канала на контроль;
- снятии с контроля любого канала;
- фиксации сигнала срабатывания по любому из каналов;
- получении изделием команды «Запрос состояния канала».

Общее сообщение формируется изделием при:

- получении изделием команды «Режим обмена»;
- получении изделием команды «Сброс»;
- обнаружении изделием ошибок в принятых командах.

От сервера оборудование ПКП «Фокус-3М» может получать следующие команды:

- режим обмена;
- сброс;
- контроль (ДК);
- повтор;
- начальная установка (НУ);
- запрос состояния канала.

2.3.1.4. Взаимодействие со СКУД

Информация о событиях СКУД передается из системы СКУД, реализованной на базе оборудования Northern Computers и программного обеспечения DSP, по сети ЛВС СКУД через сетевой коммутатор из состава СКУД поступает в ЛВС ССОИ и далее на контроллер мониторинга СКУД Fractal-19"-002/KS из состава ССОИ.

Там производится обработка полученных данных, перевод их в формат mail-smtp и дальнейшая передача в архив событий ССОИ и на АРМ ССОИ. Программа мониторинга и управления СКУД, входящая в состав ПО Контроллера мониторинга СКУД, обеспечивает также передачу команд в СКУД о блокировке и разблокировке дверей.

Система сбора и обработки информации регистрирует следующие события СКУД:

- Запуск сервера;
- Остановка сервера;
- Информация о работоспособности сервера (с программируемым периодом);
- Доступ по карте разрешен;
- Доступ по карте запрещен;
- Взлом двери;
- Нажата кнопка выхода;
- Отпущена кнопка выхода;
- Неправильный пин-код;
- Удержание двери;
- Панель вскрыта;
- Панель закрыта;
- Информация о питании панели;
- Отсутствие связи с панелью.

2.3.1.5. Взаимодействие с ТСОН

Система ТСОН построена на программном обеспечении XViewision, обеспечивающем связь с внешними системами на основе протоколов mail-smtp (для передачи событий и видеок кадров) и http (для передачи только видеок кадров). Программное обеспечение ССОИ поддерживает данные протоколы. Информация о событиях ТСОН передается по сети Ethernet напрямую в архив событий ССОИ (срабатывание датчиков движения и т.п.), архив видеоданных ССОИ (серия видеок кадров) и АРМы ССОИ. В ТСОН объекта используются, как IP-видеокамеры высокого разрешения, так и аналоговые видеокамеры. Видеосигналы от IP-видеокамер поступают в ССОИ напрямую, а от аналоговых камер – через Блок видеорегистрации (шасси с блоком питания, 4 модуля оцифровки AXIS 240Q Blade).

Видеосигнал от аналоговых телекамер ТСОН объекта поступает на усилители-разветвители. На выходе разветвителей получается по 2 канала на каждый видеоисточник. Один из этих каналов выводится на существующую телевизионную

систему охранного наблюдения, а второй поступает на блок видеорегистрации из состава ССОИ. Таким образом, при сохранении существующей ТСОИ появляется возможность цифровой обработки видеоизображений.

Блок видеорегистрации представляет собой шасси с блоком питания и 4 модулями оцифровки AXIS 240Q Blade. На блоке устанавливается программный модуль цифровой обработки видеосигнала, который выполняет оцифровку аналогового видеосигнала, поступающего с видеокамер, обсчитывает охранные зоны на оцифрованном изображении (обсчет зон), а в случае положительного результата записывает видеоинформацию в блок архива видеоданных, передает информацию на блок управления и оповещает АРМ ССОИ согласно текущему сценарию. Запись в архив может производиться также в периодическом режиме (согласно установок сценария).

Блок видеорегистрации является сетевым устройством ЛВС сегмента.

Команды управления из ССОИ в ТСОИ (например, задания на запись с отдельных камер) поступают с серверного оборудования ССОИ напрямую по сети Ethernet на оборудование ТСОИ.

Система сбора и обработки информации регистрирует следующую информацию ТСОИ:

- серия видеок кадров с заданной камеры начиная с заданного времени (для привязки к событиям систем ИТСО);
- серия видеок кадров с заданной камеры после сработки детектора движения для заданной зоны.

2.3.1.6. Взаимодействие с системами аналоговой сигнализации

Подсистема мониторинга аналоговой сигнализации обеспечивает считывание изменений состояния выходных реле аналоговых систем комплекса ИТСО. Подсистема предназначена для считывания информации кнопок управления дверями гостевого шлюза входа-выхода на проходной. Поскольку подсистема является многофункциональной, то дополнительно предоставляется возможность считывания показаний системы САГПТ «Гамма» и датчика затопления, установленных на объекте.

Кнопки управления дверями гостевого шлюза подключаются через устройства коммутации УК-1, обеспечивающие разделение аналогового сигнала от каждой из кнопок на два канала. Один канал подключается к соответствующим устройствам управления шлюзом, а второй поступает на 16-канальный модуль дискретного ввода I-7053_FG, и далее по интерфейсу RS-232 на преобразователь интерфейса I-7188E3-232. Последний

обеспечивает преобразование интерфейсов и передачу информации непосредственно в ЛВС ССОИ. Сигнальные панели САГПТ «Гамма» и датчик затопления также подключаются к системе через преобразователи интерфейса (I-7053_FG и I-7188E3-232).

Информация систем аналоговой сигнализации после преобразования интерфейсов по сети ЛВС ССОИ поступает на Контроллер мониторинга аналоговой сигнализации Fractal-19"-002/KR из состава ССОИ. Контроллер производит обработку полученных данных, перевод их в формат mail-smtp и дальнейшую передачу на блок управления ССОИ, в архив событий ССОИ и на АРМ ССОИ.

Контроллер мониторинга аналоговой сигнализации является сетевым устройством ЛВС сегмента.

Система сбора и обработки информации регистрирует следующую информацию систем аналоговой сигнализации:

- текущее состояние и информацию о сигналах кнопок управления дверями шлюза;
- дополнительно – текущее состояние датчика затопления;
- дополнительно – текущее состояние цепей внешних сигналов в штатном режиме и информацию о сигналах оборудования САГПТ.

2.3.1.7. Регистрация собственных событий системы

Система обеспечивает регистрацию следующих собственных событий:

- вход и выход пользователей АРМ в программное обеспечение;
- подтверждения пользователей АРМ при просмотре событий;
- действия пользователей АРМ (отправка управляющих команд);
- результаты мониторинга работоспособности оборудования ССОИ и других подключенных через сеть ЛВС аппаратных сетевых устройств систем ИТСО;
- результаты мониторинга работоспособности видеокамер ТСОИ;
- события и команды, генерируемые сценариями обработки информации;
- события начала и окончания процессов, переходы между их промежуточными состояниями;
- события нарушения регламента.

2.3.1.8. Хранение информации систем ИТСО

Архив событий ССОИ обеспечивает хранение событий в течение не менее 1 года, а для СКУД не менее 3 лет. При переполнении архива наиболее старые данные автоматически удаляются, а на их место записываются новые.

Длительность хранения видеок кадров зависит от емкости видеоархива ТСОИ. При этом кадры, ассоциированные с тревожными событиями, хранятся не менее 14 дней.

Система осуществляет автоматический контроль ведения записи информации в архивы (в том числе видеоархив) и, в случае обнаружения ошибок, сообщает об этом на пульт администратора и дежурного Предприятия.

2.3.2. Решение задач передачи информации

При информационном взаимодействии ССОИ и систем ИТСО, а также между отдельными частями ССОИ, все команды управления и информационные сообщения представлены в едином формате (в частности. mail smtp), передача бинарной информации (видеокадры, звук) производится стандартизованными методами (http протокол, SQL-запросы), информация баз данных представляется для просмотра по запросу в табличном виде.

Каналы передачи данных и средства обработки информации (СУБД, архивы хранения) обеспечивают вывод результатов запросов не более чем за 10 секунд с момента поступления запроса. Для больших объемов вывода результатов сначала выводится ограниченный начальный объем данных (фиксированное количество строк, видеок кадров и т.д.).

На случай временного отключения каналов связи с ССОИ проектом предусмотрено использование возможности буферизации данных и хранения информации в системах ИТСО с последующим скачиванием актуальной информации при восстановлении связи.

Объем буферной памяти для хранения событий должен обеспечивать хранение до 64 необработанных событий на 1 сервер и должен обеспечивать буферное хранение информации не менее 24 часов. Накопление данных должно проводиться последовательно в порядке поступления событий в архив.

Мониторинг каналов связи обеспечивается средствами ССОИ круглосуточно. При обрыве связи выдается предупреждение на АРМ ССОИ.

Время реакции на зарегистрированное в системе событие не превышает 5 секунд. Запросы к базам данных для формирования отчетов строятся на SQL-языке запросов.

В составе работ по созданию системы предусмотрено формирование базы данных конфигурации, являющейся необходимым компонентом ССОИ (планировки объекта, размещение оборудования комплекса ИТСО, параметры отдельных устройств систем ИТСО, отражение взаимосвязей и состояния оборудования, категории пользователей и

т.п.). На этапе пусконаладочных работ производится надлежащее начальное программирование ССОИ.

2.3.3. Подсистема контроля прохода сотрудников и посетителей по разовым и временным пропускам

Для обеспечения контроля выдачи пропусков-радиокарт и прохода сотрудников и посетителей через проходную здания используется существующий АРМ поста охраны, установленный в кабине поста охраны проходной.

На АРМ поста охраны реализованы следующие функции:

- вывод на монитор АРМ поста охраны информации о предъявляемых на считывателях шлюзовых кабин (турникетов) проходной пропусках-радиокартах и их владельцах, а также фотографии из базы данных бюро пропусков (для фотоидентификации персоны) и изображения отсканированного паспорта. В случае попытки несанкционированного или несвоевременного прохода по радиокарте на АРМ поста охраны выводится специальное предупреждение со звуковым сопровождением;
- считывание идентификатора пропуска-радиокарты и последующий вывод на экран АРМ информации о пропуске и персоне, фотографии из базы данных, изображение отсканированного паспорта;
- сканирование паспорта посетителя и поиск по паспорту пропуска на данного человека;
- хранение информации на локальном диске АРМа поста охраны;
- передача информации о событиях (включая изображения и отсканированные образы паспортов) для длительного хранения на сервер;
- передача информации о нарушениях пропускного режима оператору Бюро пропусков, дежурному Предприятия.

Подключение АРМ поста охраны к ЛВС ССОИ обеспечивает надежную защиту от доступа к сетевым ресурсам и базам данных ССОИ со стороны постовых милиционеров. Защита обеспечивается разграничением полномочий при организации доступа к ССОИ, а также парольной защитой.

Подключение АРМ поста охраны к ЛВС ССОИ обеспечивает возможность удаленного наблюдения администратором ССОИ за информацией выводимой на монитор

АРМ, для оказания практической помощи постовому милиционеру в случае возникновения нештатной ситуации.

2.3.3.1. Алгоритм прохода посетителей по разовому пропуску через пост охраны

Электронный пропуск добавляется в систему оператором Бюро пропусков на основании заявок утвержденных электронной цифровой подписью, далее данные автоматически помещаются базу данных АРМ поста охраны.

1) Получение пропуска-радиокарты и проход на объект

При получении разового пропуска-радиокарты должны выполняться следующие действия:

Постовой милиционер:

- пропускает посетителя в шлюзовую кабину, закрывает двери, берет документ, удостоверяющий личность посетителя;
- выполняет сканирование документа, удостоверяющего личность посетителя;
- при сканировании пропуска идет автоматическое распознавание данных паспорта и поиск действующего пропуска в системе;
- в случае успешного поиска пропуска посетителя на экран компьютера выводятся данные о пропуске. Если система автоматически не смогла найти пропуск, предлагается просмотреть все пропуска, действующие на текущий момент для объекта и выбрать нужный пропуск вручную;
- при отсутствии в системе действующего пропуска посетителя на вход, постовой милиционер возвращает удостоверяющий документ посетителя и открывает дверь выхода из шлюзовой кабины.
- по результатам положительной проверки документов, постовой берет любую пропуск-радиокарту из соответствующего набора разовых и временных пропусков-радиокарт и подносит к устройству считывания радиокарт «Вход»;
- постовой выдает пропуск-радиокарту посетителю и с помощью пульта управления открывает двери шлюзовой кабины, для прохода посетителя на объект.

2) Встреча посетителя представителем принимающей стороны.

-Представитель принимающей стороны у входного узла должен отметить своей радиокартой на специальном считывателе «Регистрации представителя подразделения, принимающего посетителя» время встречи и прохода посетителя. В случае отсутствия отметки встречающего, на экран АРМ поста охраны и дежурного Предприятия выводится информация о нарушении. Информация о встречающем сотруднике фиксируется в архиве системы.

3) Выход посетителя из здания

При выходе посетителя из здания должны выполняться следующие действия:

- Посетитель подносит имеющуюся у него радиокарту к считывателю входа в шлюз, дверь шлюза автоматически открывается. На экран АРМа поста охраны должна выводиться информация о пропуске посетителя (при предъявлении посетителем пропуска радиокарты на считыватель выхода из здания), а также в некоторых случаях информация о нарушении, т.е. отсутствии отметки прохода посетителя представителем принимающей стороны.
- После успешной проверки системой соблюдения установленного времени посещения, порядка входа и выхода, время отметки представителя принимающей стороны, постовой изымает радиокарту и подносит пропуск-радиокарту к устройству считывания радиокарт «Выход». Одновременно АРМ выводит набор признаков, характеризующих результаты проверки наличия информации о пропуске в базе данных, право выхода с объекта, а также фотографию зарегистрированного владельца пропуска и его персональные данные.
- С этого момента пропуск считается деактивированным, что означает невозможность повторного выхода посетителя с объекта по пропуску-радиокарте.
- Постовой нажимает кнопку выхода, при этом открывается дверь шлюза, посетитель выходит с объекта.

4) Контроль действий постового по управлению шлюзом

- Ручное управление шлюзом постовым автоматически анализируется и, при обнаружении нарушений последовательности действий, ответственным лицам передается сигнал о нарушении.

2.3.3.2. Алгоритм прохода посетителей по временному пропуску через пост охраны

Временный пропуск для прохода посетителей на объект выдается оператором Бюро пропусков, расположенном на специальном объекте Предприятия, в соответствии с внутренним регламентом работы бюро пропусков объекта.

При проходе посетителей по временному пропуску через пост охраны постовой сверяет информацию на экране с предъявленным паспортом, идентифицирует посетителя по фотографии и принимает решение об открытии внутренней двери шлюза, либо отказе. Сканирование паспорта посетителя при этом не производится, поскольку оно уже производилось при выдаче ему временного пропуска.

При проходе посетителя по временному пропуску через пост охраны объекта встреча посетителя представителем принимающей стороны по регламенту не предусмотрена, отметки представителя на специальном считывателе не требуется.

При выходе с объекта временный пропуск-радиокарта, согласно существующему регламенту пропускного режима, не изымается, а остается на руках у посетителя.

2.3.3.3. Особенности функционирования подсистемы

При реализации проекта предусмотрено выполнение следующих пунктов:

- в случае получения разового пропуска-радиокарты на проход в здание Предприятия и ухода с него без прохода в здание данная радиокарта исключается из СКУД;
- в случае если радиокарта разового пропуска не была востребована, заявка аннулируется;
- открытие дверей шлюза контролируется программно;
- осуществляется автоматический контроль разовых, временных и постоянных пропусков-радиокарт (контролируется дата, время, порядок входа и выхода);
- осуществляется автоматический контроль отметки принимающей стороны для разового пропуска;
- осуществляется автоматический контроль паспортных данных при сканировании;
- предусмотрена возможность сканирования документа и выдачи пропуска-радиокарты посетителю постовым;
- при обнаружении нарушений производится оповещение ответственных лиц;

2.3.4. Подсистема мониторинга электропитания и параметров среды

Подсистема мониторинга электропитания и параметров окружающей среды предназначена для контроля состояния системы гарантированного бесперебойного электропитания (СГЭ) объекта и температурного режима в трех помещениях.

Климатические датчики измерения температуры и влажности устанавливаются в трех помещениях здания. В каждом помещении устанавливается один основной датчик и один дополнительный, подключаемый к основному. Основной датчик подключается по специальному кабелю к контроллеру мониторинга климатических параметров EM-1, который, в свою очередь, подключается к сети Ethernet ССОИ. Контроллер мониторинга климатических параметров обрабатывает полученную от датчиков информацию и передает ее на блок управления, блок архива событий и на АРМ ССОИ.

Информация от источников бесперебойного питания систем ИТСО поступает на контроллер мониторинга электропитания и параметров среды непосредственно по локальной сети. При этом используются специальные сетевые карты UPS Network Management Cards.

Системой контролируются следующие параметры работы системы гарантированного бесперебойного электропитания (СГЭ):

- входное напряжение в сети;
- выходное напряжения источника (для потребителей);
- частота тока в сети;
- нагрузка (мощность потребителей);
- уровень заряда батарей;
- недостаточный ресурс батареи (необходима замена аккумуляторов);
- оставшееся время работы от батарей (в случае отключения входного напряжения);
- контроль температуры в помещениях.

В случае отключения входного напряжения в сети информация об этом отображается на АРМ оператора (и других АРМ – в соответствии с настройками сценариев).

Администратору ССОИ предоставлена возможность калибровки источников бесперебойного питания, как в ручном, так и в автоматическом режиме по расписанию.

В случае необходимости замены аккумуляторов ИБП на АРМ оператора ССОИ периодически выводится соответствующее сообщение (о неисправности).

Информация обо всех событиях подсистемы мониторинга электропитания и параметров среды записывается в архив событий ССОИ.

2.4. Решение задач комплексного взаимодействия систем ИТСО

Система сбора и обработки информации является программно-аппаратным комплексом для управления различными средствами обеспечения внутренней безопасности. ССОИ позволяет интегрировать в единое целое средства ТСОИ, СКУД, охранной и пожарной сигнализации, мониторинга сетевого оборудования.

Как было описано выше, ССОИ получает информацию о состоянии средств ИТСО и может реагировать на регистрируемые события. Если средства ИТСО допускают внешнее управление, то специализированные контроллеры ССОИ преобразуют цифровые команды ССОИ в формат данных средств. Иногда обратная связь со средствами ИТСО объекта осуществляется на уровне баз данных. ССОИ позволяет осуществить частичное или полное управление функциями средств ИТСО как ручное, так и автоматическое - на уровне сценариев.

Единый формат данных внутри ССОИ позволяет записывать данные о работе комплекса в единую базу данных и выполнять их анализ. Информация о конфигурации комплекса в целом и отдельных подсистем хранится в централизованной базе данных.

Система позволяет интегрировать охранные подсистемы различных поставщиков, уже имеющиеся на охраняемых объектах. ССОИ производит сбор данных от различных подсистем, а при наличии технической возможности осуществляет автоматическое управление подсистемами. Пользователи имеют возможность получения информации обо всех подсистемах одновременно или управления ими с одного или нескольких универсальных пультов управления.

Все угрозы, связанные с нарушением режима работы выявляются при непосредственном наблюдении изображения с видеокамер, установленных в охраняемых помещениях, и при просмотре тревожных сообщений средств управления сценариями.

Оператор с помощью системы видеонаблюдения осуществляет визуальный контроль за происходящим в помещениях. При обнаружении нарушений комплекс по команде оператора имеет возможность записать один кадр или несколько изображений в базу данных.

Осуществление функций охраны ССОИ производит на основе событий и сценариев, которые представляют собой совокупность неких данных в базе системы

Примеры событий:

-Нарушение кем-то охранной зоны видеокамеры.

- Выход из строя видеокамеры (обрыв сигнального кабеля или кабеля питания).
- Нарушение зоны, оборудованной датчиками охранной сигнализации.
- Выход из строя функционального блока системы.

При интеграции в систему «XVmatic» подсистем СКД, пожарной, охранной и других видов сигнализации возможна обработка тревожных или диагностических сообщений от этих подсистем.

В основе данных сценария лежит список значимых событий системы, обрабатываемые средствами ССОИ.

Некоторые события вызывают автоматическую реакцию той подсистемы, в которой событие возникло. Обработка таких событий и задание реакции на них определяется настройками самой подсистемы. Так, например, система контроля доступа при проходе сотрудника через терминал производит автоматическую запись информации об использованной карте-пропуске в собственную базу данных регистрации, а система автоматического видео наблюдения (обсчет контрольных зон) при обнаружении движения автоматически записывает серию кадров в архив видео данных.

Для каждого события, обрабатываемого в сценарии, определена реакция.

Примеры реакций:

- Записать в архив заданное количество видео кадров с определенной камеры;
- Развернуть управляемую камеру в сторону нарушения и сделать «наезд»;
- Выдать на экран оператору текстовое сообщение;
- Выдать на экран оператору план помещения с отметкой зоны нарушения;
- Выдать оператору речевое сообщение;

Система работает как с простыми (одиночными) событиями, так и со сложными (множественными) событиями.

Реакцией на простое или сложное событие может быть единственное действие - простая реакция, или совокупность (последовательность) действий - сложная реакция.

Различные варианты последовательности наступления событий от одного устройства (как одиночного, так и с партнером) называются сценами. Количество сцен во фрагменте сценария для одного устройства может быть произвольным.

Пример сценария

Ситуация

На 1 этаже охраняемого объекта имеется запасной выход. За дверью этого выхода с внутренней стороны «наблюдает» видеочамера №25. При попытке открыть эту дверь с внешней стороны или при подходе к двери с внутренней стороны требуется оповестить дежурного оператора системы.

Сценарий для ситуации

Источник события - камера №25 зона 1 - дверь.

Вид события - нарушение охранной зоны (от этой камеры могут прийти и другие события - например, выход камеры из строя, но эта ситуация в примере не рассматривается).

Реакция - (сложная)

1. Послать на пульт оператора безопасности текстовое сообщение «нарушение зоны», типа «тревога» (красный цвет сообщения на экране и в протоколе), с указанием устройства №3025 (камера №25).

2. Послать на пульт оператора безопасности, речевое сообщение №11 «тревога, нарушение охранной зоны на 1 этаже».

Конец сценария.

Для каждого обрабатываемого события (события, на которое сценарий должен реагировать) в сцене задается одна или более реакций. В зависимости от состава установленного на охраняемом объекте оборудования и от состава охранных подсистем можно задать следующие реакции:

- вывод текстового сообщения на пульт оператора. Вывод текстового сообщения совмещается с показом на пульте оператора расположения устройства, от которого пришло сообщение, на плане объекта. Некоторые текстовые сообщения общего назначения могут не сопровождаться показом плана, если невозможно (или не имеет смысла) определить устройство или если это устройство не привязано к конкретному плану в базе данных оборудования. Текстовые сообщения заранее заносятся в базу данных, и при разработке сценария выбираются из списка. На этапе создания сценариев новое сообщение определить нельзя. Сообщение с планом можно направить на один или несколько пультов управления по выбору.
- вывод звукового сообщения на пульт управления. Сообщение, это заранее записанный звуковой файл. Это может быть некоторый звук или дикторский текст. Все сообщения должны быть заранее зарегистрированы в базе данных. На

этапе разработки сценария новое звуковое сообщение ввести нельзя, но любое из сообщений можно прослушать для проверки. Звуковое сообщение можно направить на один или несколько пультов управления по выбору. В списке пультов управления присутствуют только те пульта, на которых есть звуковой адаптер.

- запись заданного количества видео кадров с заданным интервалом времени в видео архив. Указывается камера, с которой производится запись (обычно, не та, событие которой обрабатывается в данной сцене), и номер предустановки, если эта камера управляемая. С помощью этой реакции производится съемка места нарушения, когда "мастером" является датчик охранной сигнализации или считыватель СКД. Возможна съемка места нарушения с помощью управляемой камеры, которая разворачивается в нужном направлении (предустановка) и совершает "наезд". Следует иметь в виду, что для любой видео камеры, задействованной в сценарии (если для нее определена охранная зона), кадры во время нарушения пишутся в видео архив автоматически.

- отображение места нарушения на пульте оператора. Для этой реакции должна быть выбрана камера. Изображение с указанной камеры в полноэкранный режим выводится на все пульта управления, на которых в данный момент работает модуль "Видеонаблюдение". Пульт управления не выбирается.

Кроме перечисленных реакций по желанию заказчика и при наличии технической возможности могут быть определены дополнительные реакции. Например: блокировка или принудительное открывание дверей через СКД, блокировка пропуска в СКД, включение системы пожаротушения, включение/выключение вентиляции, кондиционирования и т.д.

2.5. Средства комплексной обработки информации и управления подсистемами

Средства комплексной обработки информации и управления подсистемами обеспечивают:

- работу сценариев обработки данных (событий) подсистем для автоматического выявления заранее определенных шаблонных ситуаций (штатных и нештатных), последующего оповещения на АРМах ответственных сотрудников и выполнения заданных действий средствами подсистем ССОИ и систем ИТСО объекта;

- логическую обработку поступающей информации от систем ИТСО и сверку с требуемыми значениями на определенное время.
- автоматическую сигнализацию и оповещение на АРМах ответственных сотрудников, при обнаружении нарушений.
- генерацию собственных простых (при выполнении одного условия) и сложных (при выполнении группы и последовательной цепочки условий) событий для фиксации моментов определения ситуаций и принятия решений;
- передачу в систему громкого оповещения управляющих воздействий для громкого оповещения объекта в случаях тревоги, эвакуации;
- взаимодействие по общим информационным протоколам с компонентами системы, отвечающими за сбор и обработку систем ИТСО объекта;
- взаимодействие по общим информационным протоколам с программным обеспечением АРМов системы ССОИ;
- взаимодействие по общим информационным протоколам с программным обеспечением АРМов системы ТСОИ с возможностью передачи информации на АРМы ТСОИ;
- отправку информации (событий) о своей работе на запись в архивы хранения данных ССОИ.

2.6. Контроль выполнения регламентов работы персонала и систем объекта

Контроль выполнения регламентов работы персонала и систем объекта предназначен для постоянного автоматического аудита параметров происходящих на объекте процессов.

Процесс представляет собой виртуальное описание конечного действия, выполняемого человеком или предметом. В системе описываются типы процессов, их параметры, условия начала и окончания.

Процессы создаются и заканчиваются автоматически с помощью специализированного программного обеспечения (система «XVmatic»). Начало процесса определяется совпадением заданных в описании процесса условий с параметрами текущих событий ССОИ.

Начало и конец фиксируются в архиве хранения данных процессов, с привязкой к событиям ССОИ, относящимся к данному процессу. Процесс может быть связан с другими процессами (например, переход одного процесса в другой).

Регламент представляет собой виртуальное описание действий (процессов), разрешенных или запрещенных на объекте. Регламент описывает условия протекания процессов, соответствие процессов заданным условиям, взаимное сочетание и взаимоисключение процессов.

Нарушением регламента считается несоответствие текущих процессов заданным регламентам.

Контроль выполнения регламентов обеспечивает выявление несоответствий происходящих (и описанных) процессов на объекте заданным регламентами правилам.

Случаи нарушения регламентов классифицируются по уровню важности (опасности).

Информация о текущих процессах и регламентах доступна в отдельном программном модуле, устанавливаемом на АРМ оперативного дежурного и других АРМ ССОИ.

2.7. Функции рабочих мест

2.7.1. АРМ администратора ССОИ

АРМ администратора ССОИ предназначен для отображения текстовой, графической и звуковой информации о состоянии систем ИТСО объекта в реальном времени, а именно:

- состояния охранных зон, разделов, реле релейных модулей и панелей систем СОТС;
- адресных датчиков, шлейфов и панелей СПС;
- точек прохода, режимов работы шлюзов и панелей СКУД;
- состояния работоспособности видеокамер ТСОН, видеокадров с места событий.
- В функции АРМ администратора ССОИ входит также:
- настройка алгоритмов работы технических средств и программного обеспечения ССОИ;
- администрирования доступа операторов к функциям ССОИ;
- подготовки и распечатки отчетов о работе систем ИТСО и ССОИ.

2.7.2. АРМ поста охраны

На АРМ поста охраны реализованы следующие функции:

- вывод на монитор АРМ поста охраны информации о предъявляемых на считывателях шлюзовых кабин (турникетов) проходной картах СКУД и их

- владельцах, а также фотографии из базы данных бюро пропусков (для фото-идентификации персоны). В случае попытки несанкционированного или несвоевременного прохода по карте выводится специальное предупреждение со звуковым сопровождением;
- считывание идентификатора пропуска-радиокарты и последующий вывод на экран АРМ информации о пропуске и персоне, фотографии из базы данных, изображения отсканированного паспорта (при необходимости);
 - сканирование паспорта посетителя и поиск по паспорту пропуска на данного человека;
 - хранение информации на локальном диске АРМа поста охраны;
 - передача всей информации о событиях (включая изображения и отсканированные образы паспортов) для длительного хранения на сервер;
 - передача информации о нарушениях пропускного режима оператору Бюро пропусков, дежурному Предприятия.

3. Основные технические решения

3.1. Структура системы

Система представляет собой комплекс аппаратно-программных средств, расположенный в здании Предприятия.

3.1.1. Состав системы

Оборудование системы состоит из следующих основных частей:

- Контроллеры сбора и обработки информации;
- Серверное оборудование;
- Рабочие места (АРМ);
- Сетевое оборудование компьютерной сети системы (ЛВС);
- Средства бесперебойного электропитания;
- Аппаратные шкафы, конструктивные элементы, дополнительное сервисное оборудование.

3.1.2. Расположение оборудования системы

Оборудование системы расположено на территории объекта в следующем порядке:

1) Серверное оборудование и контроллеры сбора и обработки информации расположены в аппаратных шкафах в помещении «СЕРВЕРНАЯ». В шкафах устанавливаются также источники бесперебойного питания (ИБП) и оборудование ЛВС. Кроме того, в аппаратном шкафу помещения «СЕРВЕРНАЯ» установлен и межсетевой экран Континент-К для защиты межобъектового канала связи. Также в помещении «СЕРВЕРНАЯ» расположен монитор LCD с клавиатурой и KVM-переключателем (на 16 компьютеров).

2) В помещении «СЕРВЕРНАЯ» расположен АРМ администратора ССОИ в составе: Переносной пульт управления (Notebook), мышь, сумка, сетевой фильтр, источник бесперебойного питания и цветной лазерный принтер.

3) В помещении поста охраны расположен АРМ поста охраны в составе: системный блок АРМ, монитор, клавиатура, мышь, звуковые динамики, сетевой фильтр и сканер для документов формата А5.

4) Также в помещении поста охраны установлен комплект оснащения шлюза для прохода посетителей в составе трех считывателей карт Proximity и комплекта интерфейсных модулей для подключения кнопок шлюза.

5) В вестибюле центрального входа установлена дополнительная IP-видеокамера.

3.2. Контроллеры сбора и обработки информации

В состав системы входят 7 контроллеров сбора и обработки информации:

- контроллер мониторинга пожарной сигнализации (модель Fractal-19"-002/KP);
- контроллер мониторинга аналоговой сигнализации (модель Fractal-19"-002/KR);
- контроллер мониторинга электропитания и параметров среды (модель Fractal-19"-002/КО);
- контроллер мониторинга СКУД (модель Fractal-19"-002/KS);
- контроллер громкого оповещения (модель Fractal-19"-002/KZ);
- контроллер состояния окружающей среды (модель EM1);
- блок регистрации проходов посетителей (модель Fractal-19"-002/MR)
- контроллер мониторинга охранной сигнализации (модель Fractal-C-010/КО).

Все контроллеры, за исключением контроллера мониторинга охранной сигнализации, имеют корпуса промышленного типа высотой 1U для установки в 19" шкаф с креплениями к лицевым профилям стоек.

Контроллеры сбора и обработки информации устанавливаются в существующие аппаратные стойки на горизонтальных направляющих, закрепленных на боковых профилях стоек.

Контроллеры сбора и обработки информации:

- представляют собой компьютерные устройства на базе IBM-совместимых серверных платформ;
- являются сетевыми устройствами со скоростью передачи данных 1 Гбит на 1 соединение;
- питаются от электросети переменного тока 220В.

Контроллеры сбора и обработки информации предназначены для круглосуточной работы. Для проведения профилактических и ремонтных работ блок демонтируется и вынимается из аппаратного шкафа.

На контроллерах сбора и обработки информации уставлено программное обеспечение:

- операционные системы;

- драйвера устройств хранения, сетевых адаптеров и других электронных компонентов ЭВМ;
- конфигурационные базы данных (на основе СУБД);
- модули программного обеспечения сбора информации и взаимодействия с системами ИТСО.

3.3. Серверное оборудование

Серверное оборудование располагается в существующих аппаратных стойках в помещении «СЕРВЕРНАЯ». Все блоки серверного оборудования имеют корпуса промышленного типа для установки в 19” шкаф с креплениями к лицевым профилям стоек.

Серверные блоки устанавливаются в стойки на горизонтальных направляющих, закрепленных на боковых профилях стоек.

Все блоки серверного оборудования:

- представляют собой компьютерные устройства на базе IBM-совместимых серверных платформ;
- являются сетевыми устройствами со скоростью передачи данных 1 Гбит на 1 соединение (в серверном блоке 2 сетевых порта);
- питаются от электросети переменного тока 220В.

Серверное оборудование эксплуатируется в круглосуточном режиме. Для проведения профилактических и ремонтных работ блок демонтируется и вынимается из аппаратного шкафа.

На блоках серверного оборудования уставлено программное обеспечение:

- операционные системы;
- драйвера устройств хранения, сетевых адаптеров и других электронных компонентов ЭВМ;
- СУБД MS SQL Server;
- базы данных системы;
- модули управляющего программного обеспечения.

Типы и назначения блоков серверного оборудования приведены в таблице:

№ п/п	Название блока	Назначение	Кол-во
1	Центральный блок управления	Обеспечивает обработку поступающей информации, поддержку работы сценариев обработки данных, функционирование	1

	Fractal-19"-005/MU	компонентов системы ССОИ	
2	Блок управления Fractal-19"-002/MU	Обеспечивает функционирование компонентов системы ССОИ	3
3	Блок архивации (архив 2 Тбайта) Fractal-19"-005/МА	Обеспечивает запись и хранение информации. Выполняется автоматическая очистка устаревшей информации.	1
4	Блок архива видеоданных (архив 4 Тбайт) Fractal-19"-005/МА	Обеспечивает запись, хранение и автоматическую очистку устаревшей видеoinформации.	5

При хранения больших объемов данных (видеоинформация, базы данных) на блоках предусмотрены дополнительные жесткие диски. Для хранения баз данных используется дополнительный дисковый массив архитектуры RAID-1 (1+1 “зеркало”) или RAID-5.

3.4. Рабочие места

Рабочие места (пульты) системы представляют собой настольные компьютерные комплексы в составе: системный блок (или терминал), ЖК-монитор, клавиатура (для АРМ компьютерного типа), мышь. АРМ администратора реализован на базе переносного пульта управления типа ноутбук.

Системные блоки пультов сертифицированы.

Мониторы устанавливаются на столах или горизонтальных плоскостях, системные блоки (тип – мини деск-топ) могут быть установлены на любой горизонтальной поверхности, вертикально или закреплены на вертикальной поверхности.

Рабочие места (АРМы) системы:

- представляют собой компьютерные устройства на базе IBM-совместимых платформ для рабочих станций;
- являются сетевыми устройствами со скоростью передачи данных 1 Гбит на 1 соединение (в системном блоке может быть 1 или 2 сетевых порта);
- питаются от электросети переменного тока 220В.

Рабочие места предназначены для круглосуточной работы, но могут быть использованы в течение времени работы операторов. Для проведения профилактических и ремонтных работ пульт полностью выключается.

На рабочих местах уставлено программное обеспечение:

- операционные системы;
- драйвера устройств хранения, сетевых адаптеров и других электронных компонентов ЭВМ;
- модули программного обеспечения управления, видеонаблюдения, настройки и мониторинга системы.

3.5. Организация локальной вычислительной сети и каналов связи

Локальная сеть системы соответствует сетевым технологиям Ethernet 10/100/1000 Мбит/с. (семейство стандартов IEEE 802) и обеспечивает:

- поддержку транспортных протоколов TCP/IP;
- пропускную способность каналов соединения серверов и рабочих станций не менее 100 Мбит/с;
- возможность территориального переноса структурных элементов системы в пределах расположения сети, а также подключение в систему новых аппаратных средств в количестве не менее 10 % без изменения организации сети.

ЛВС системы предназначена для обеспечения информационного обмена между оборудованием системы. Используется активное сетевое оборудование со скоростными показателями передачи информации по каналам связи 10/100/1000 Мегабит/с.

Основу ЛВС составляют сетевой коммутатор D-Link DGS-3100-24 на 24 порта 10/100/1000 Мбит/с, сетевой маршрутизатор D-Link DGS-3627 на 24 порта 10/100/1000 Мбит/с (последний – из поставки 2008 года), расположенные в помещении «СЕРВЕРНАЯ», и один сетевой коммутатор DGS-1005D/GE на 5 портов 10/100/1000 Мбит/с, установленный в помещении поста охраны.

Управление сетью осуществляется с помощью Центра управления сетью ЦУС «Континент».

Многие объекты Предприятия оборудованы волоконно-оптическими каналами.

Для организации «последней мили» с каналом, предоставляемым провайдером для связи с объектами, расположенными в других городах, используется ADSL-модем компании **ZyXEL**, а для защиты этого канала – межсетевой экран АПК «Континент».

3.6. Общеорганизационные решения

3.6.1. Эксплуатация, ремонт и обслуживание

Оборудование и аппаратура, устанавливаемые вне помещений, устойчивы к внешним воздействиям в условиях умеренного климата по ГОСТ 15150-69 - (У1).

Оборудование и аппаратура, устанавливаемые в помещениях, устойчивы к внешним воздействиям по ГОСТ 15150-69 (У3.1—для помещений без искусственно регулируемых климатических условий, У4.2—для помещений с искусственно регулируемыми климатическими условиями).

Блоки и модули устанавливаемого оборудования являются взаимозаменяемыми с аналогичными блоками.

Обслуживание устанавливаемого оборудования производится обученным персоналом.

3.6.2. Электропитание

ССОИ работает круглосуточно при нормальном питающем напряжении сети.

Электропитание системы ССОИ осуществляется в соответствии с требованиями ВМП-001-01 (потребители 1 категории и особой группы 1 категории надежности) от однофазной промышленной сети переменного тока с номинальным значением 220 В 50 Гц, с допуском по величине $-15...+10\%$, по частоте $+1$ Гц. Электропитание обеспечивается Заказчиком.

Электропитание обрабатывающего оборудования и АРМ осуществляется от локальных источников бесперебойного питания системы. Емкость источников резервных бесперебойного питания является достаточной для корректного завершения работы и сохранения необходимых данных.

3.6.3. Безопасность эксплуатации технических средств

Для обеспечения безопасности персонала и клиентов Предприятия проектом предусмотрено выполнение следующих требований:

- устанавливаемое оборудование и кабельная сеть являются безопасными для лиц, соблюдающих правила их эксплуатации;
- технические средства ССОИ, устанавливаемые на территории объекта являются безвредными для здоровья лиц, имеющих доступ на территорию объекта;

- устанавливаемое оборудование отвечает требованиям электробезопасности по ГОСТ 12.2.006-87;
- устанавливаемое оборудование отвечает требованиям пожарной безопасности по ГОСТ 12.2.007-97;
- допустимые уровни электромагнитных полей на рабочих местах отвечают требованиям ГОСТ 12.1.006-84;
- применяемое оборудование, его расположение и условия эксплуатации отвечают требованиям «Санитарных правил и норм».

3.6.4. Стандартизация, унификация и возможности расширения

Система состоит из типовых блоков, узлов и плат, применяемых при разработках систем безопасности на объектах Предприятия. Система обеспечивает взаимозаменяемость отдельных элементов, проектируемых и существующих систем.

Конфигурация системы и применяемое оборудование обеспечивают возможность наращивания системы за счет расширения аппаратной и программной частей без нарушения работоспособности смонтированного оборудования.

Проектом предусмотрена возможность модернизации ССОИ за счет развития программного обеспечения.

3.6.5. Надежность

Время восстановления работоспособности ССОИ после отказа не превышает 24 часов независимо от характера неисправности при условии наличия необходимых запасных частей.

Надежность оборудования ССОИ, его технические параметры в процессе эксплуатации обеспечиваются заводом изготовителем.

3.6.6. Гарантийные обязательства

Гарантийный срок на систему и ее компоненты составляет не менее 1 года.

3.6.7. Эргономика и техническая эстетика

Оборудование размещено в стандартных металлических шкафах и корпусах, обеспечивающих удобный доступ к коммутационным разъемам и органам управления, регулировки и настройки, с учетом статистических характеристик основных

антропометрических признаков человека (ГОСТ 12.2.049-80). Все блоки системы имеют необходимые поясняющие надписи.

Дизайн всех интерфейсных панелей программного обеспечения выдержан в едином, удобном для восприятия стиле.

3.6.8. Защита информации от несанкционированного доступа

Информация, полученная от систем ИТСО, хранится на жестких носителях данных аппаратных блоков под защитой паролей.

Доступ к информации и программам мониторинга и управления закрыт парольной защитой, совместимой с аналогичными средствами системы «XVmatic».

3.6.9. Виды обеспечения

Для всех рабочих мест системы разработана справочная информация пользователя в соответствии с уровнем его доступа (аналогично функции «Help» стандартных приложений Windows®).

Все сообщения программного обеспечения системы (за исключением системных сообщений) представлены на русском языке.

Программное обеспечение создаваемой системы обеспечивает:

- защиту от несанкционированного доступа;
- защиту баз данных и систем управления базами данных от некорректных действий операторов постов контроля;
- русификацию всех системных сообщений и пользовательского интерфейса (за исключением сообщений об ошибках операционных систем и драйверов);
- информационную и программную совместимости с действующим программным обеспечением;
- создание резервных копий баз данных и прикладного программного обеспечения;
- подтверждение права использования программного обеспечения лицензией от фирмы поставщика.

В составе системы не используются операционные системы, запрещенные к применению на Предприятии.

Комплект поставляемого программного обеспечения обеспечивает полную переустановку системы силами сотрудниками Заказчика без участия специалистов

Исполнителя. Комплект программного обеспечения содержит тестовые и диагностические программы.

Допускается использование, в составе программного обеспечения системы, программных продуктов, поставляемых производителями технических средств, применяемых в системе, или сопрягаемых с ней инженерно-технических системах.

Дистрибутивные версии по всем программным продуктам поставляются на машинных носителях и имеют лицензии или сертификаты на его использование.

3.6.10. Расчет выбора источников бесперебойного питания.

При прекращении основного энергоснабжения предусмотрено функционирование системы от источника бесперебойного питания (ИБП) в течение 0,5 часа. Выбор ИБП сделан исходя из расчётной мощности оборудования, а также зависимости времени работы на аккумуляторах от уровня нагрузки, рассчитанной заводом-изготовителем.

4. Мероприятия по подготовке объекта автоматизации к вводу системы в действие

4.1. Установка и настройка программного обеспечения

Исполнитель устанавливает предусмотренное проектом программное обеспечение на установленное оборудование системы.

Исполнитель в рамках пуско-наладочных работ производит заполнение баз данных и настроек программного обеспечения для начального рабочего запуска системы.

Исполнитель обеспечивает передачу Заказчику списка регистрационных имен и паролей для доступа к программному обеспечению и базам данных системы.

4.2. Мероприятия по подготовке персонала для работы с системой

Персонал системы должен пройти обучение работе с оборудованием и программным обеспечением перед вводом системы в эксплуатацию.

Для поддержки работы системы необходимо обучить персонал Заказчика по следующим направлениям:

- администратор, выполняющий настройки полномочий доступа операторов к функциям программного обеспечения системы;
- пользователь АРМ поста охраны.