Описание работы интегрированной системы безопасности объектов-Плюс (ИСБО-Плюс)

Введение

Интегрированная система безопасности объектов – инструмент поддержки принятия управленческих решений во внештатных и чрезвычайных ситуациях – Плюс (далее Система) представляет собой комплексное инженерно-техническое решение, в которое с помощью одного из элементов системы – интеграционной шины включены все системы безопасности (инженерно-технические средствах охраны) предприятия:

- система контроля и управления доступом;
- система видеонаблюдения;
- система мониторинга персонала;
- система охранно-пожарной и охранно-тревожной сигнализации;
- система защиты периметра и другие инженерные системы.

Работа с Системой централизована и осуществляется через единый специализированный интерфейс – программный комплекс «**Контроль систем безопасности».** Он обеспечивает администрирование, мониторинг и управление комплексом на основе единой базы данных и сквозных алгоритмов взаимодействия подсистем.

Ключевой функцией Системы является поддержка принятия управленческих решений во внештатных ситуациях, минимизация ошибки персонала при ликвидации чрезвычайных ситуаций. Это достигается за счет оперативности в выявлении и идентификации угроз и рисков, выдачи информации заинтересованным лицам, выдачи распоряжений операторам и службам, контроля исполнения распоряжений.

Разработанная Система является распределенной, что позволяет реализовать совместное использование ресурсов, подключенных к сети в одно и то же время. Это свойство Системы позволяет производить ее масштабирование как горизонтально, так и вертикально. Распределенность Системы означает, что выход из строя какой-либо ее части (например, отключение какого-либо узла) не приводит к полной остановке работы, узлы могут продолжать работать автономно, а по восстановлении работоспособности всей Системы осуществить репликацию данных.

В описываемый функционал включено категорирование объектов по степени их защищенности, а также категорирование всех сигналов, по степени их чрезвычайности. Система позволяет осуществить:

- интеграцию и сопряжение систем сигнализации и обеспечения безопасности;
- потоковый сбор событий, влияющих на безопасность;
- сортировку событий по значимости и опасности для предприятия;
- отображение ситуационной обстановки и информации о событии;
- автоматизация поддержки реагирования на события;
- мониторинг состояния узлов Системы, серверов инженерно-технических средств охраны (далее ИТСО) объекта, подключенных устройств;
- многоуровневая информационная поддержка принятия решений при ЧС.

В случае возникновения ЧС информация поступает на все уровни управления объектом, в зависимости от категории защищенности объекта, путем уведомления в системе. При этом на экране монитора появляется:

- окно тревожного события;
- интерактивная карта объекта
- видео поток с видеокамеры;
- информация об объекте, на котором произошло аварийное событие;
- инструкция реагирования на аварийное событие;
- переход к делу объекта.

Также возможно настроить отправку сообщений в Telegram или на e-mail.

Система является модульной и готова к дальнейшей доработке под нужды конкретного заказчика.

Основные понятия и сокращения

АИС – автоматизированная информационная система;

ИТСО – инженерно-технические средства охраны;

ЦУБ – центр управления безопасностью (головной);

РЦУБ – региональный центр управления безопасностью;

Узел АИС – организационная единица Системы, которая выполняет функции надзора и координации событий, связанных с безопасностью объектов;

Сервер ИТСО – Trassir (современная автоматизированная система, назначением которой является организация видеонаблюдения, интеллектуальная обработка и хранение видеоинформации, а также предоставление средств доступа к видеоинформации);

Устройства ИТСО – устройства охраны предприятия, которые входят в систему Trassir;

События устройств – события, возникающие и фиксирующиеся системой Trassir, которые может обрабатывать (реагировать) Система;

Действие – то, что должна сделать Система, если случается событие, которое она отслеживает (всплывающее сообщение на сайте, тревожное окно на сайте, снимок с камеры, отправка сообщений в телеграмм или на е-мейл);

Категорирование событий – операция сопоставления типа события ИТСО, класса устройств и категории событий (переброс предмета, пожарная тревога, охранная сигнализация, несанкционированный доступ);

Объекты – то, за чем мы наблюдаем с помощью устройств ИТСО. Объект может содержать помещения, зоны, камеры, телепорты. К объекту привязывается паспорт объекта;

Основные функции работы Системы

При развертывании Системы осуществляется ее настройка, которая позволяет:

- создавать объекты;
- осуществлять привязку объектов к карте;
- создавать схемы объектов;
- заполнять информацию об объекте (на основании которой можно сформировать паспорт объекта);

- заполнять информацию об инженерно-технических средствах охраны (устройства ИТСО) на объекте;
- создавать привязки устройств к схеме объекта;
- иметь возможность просмотра статусов устройств, просмотра камер и управления исполнительными устройствами;
- получать события с устройств;
- категорировать полученные события по типам, категориям и классам устройств;
- определять категории пользователей, назначать им роли управлять их доступом к Системе;
- осуществлять мониторинг персонала;
- заполнять и вести различные справочники Системы;
- осуществлять мониторинг состояния как самой Системы (ее узлов), так и серверов ИТСО с подключенными к ним устройствами;
- выводить экран тревожного сообщения.

Данная настройка происходит с помощью файлов конфигурации и через интерфейс Системы, что позволяет значительно сократить время на установку Системы, ее обслуживание, а также обеспечить простоту в эксплуатации для различных пользователей Системы.

Так как Система имеет распределенную иерархическую структуру и узел верхнего уровня содержит данные всей системы, то можно создать необходимые объекты на нем и осуществить рассылку данных (репликацию). Так же создать объекты можно на любом узле и осуществить синхронизацию информации.
Замечание: справочник «Категорирование событий» должен быть создан на главном узле и разослан на нижестоящие.

На узле верхнего уровня есть возможность управления всеми инженерно-техническими средствами охраны, существующими в иерархии. Также доступ предоставляется ко всем данным всех объектов (редактирование, добавление).

На нижестоящих узлах доступ предоставляется к ИТСО и объектам, непосредственно относящимся к текущему узлу (редактирование, добавление).

В Системе реализована ролевая пользовательская модель. Каждому пользователю назначается роль. Для роли настраивается доступ к модулям (которые представляют собой определенный класс объектов, конкретный объект или событие).

Сбор и сортировка событий от устройств ИТСО осуществляется на нижнем уровне Системы в зависимости от списка устройств, которые подключены к нему. Отсортированное событие, помеченное как тревожное, заносится в базу данных. В зависимости от категории события осуществляется его обработка (выдача информации операторам) и передача на вышестоящий уровень. К переданному событию добавляется информация о решении, принятом на нижнем уровне.

Описание работы Системы с использованием ее веб-интерфейса

1. **Создание структуры Системы.** Настройка узла АИС (ЦУБ, РЦУБ). Часть информации содержится в конфигурационном файле и при развертывании прописывается в базу. Далее в модуле «Узлы АИС» происходит требуемая донастройка и связывание узлов в иерархическую модель. Подключенные и функционирующие в текущий момент времени узлы подсвечиваются зеленым индикатором, если узел по какой-то причине отключен (с ним нет связи, не работают службы и т.д.) он подсвечивается красным индикатором. Текущий узел («я сам») подсвечивается дополнительно зеленой звездочкой. Узел может обслуживать несколько объектов.

2. **Ролевая модель Системы.** Роли администратора и оператора (с уровнем доступа) прописаны в конфигурационном файле. Используя интерфейс Системы можно добавлять требуемые роли, определять пользователей, настраивать необходимый доступ к модулям.

3. **Регистрация сервера ИТСО (трассир, Орион, Сигур).** Осуществить добавление сервера ИТСО в модуле «Серверы ИТСО». После добавления сервер автоматом оказывается связанным с тем узлом, под которым его добавили. В режиме редактирования можно узел изменить.

4. **Регистрация устройств ИТСО в модуле «Устройства ИТСО».** Специальная служба после регистрации сервера ИТСО соединяется с сервером ИТСО и выгружает все устройства, подключенные к нему. Далее, через режим редактирования необходимо донастроить устройства (задать тип), а также **добавить действие**, которое должна предпринять Система при наступлении события, сопоставив категорию события, категорию объекта, код события и идентификатор устройства. Добавить действие можно также в модуле «Настройка действий».

5. Для корректной настройки действий **также необходимо осуществить категорирование событий**. В модуле «Категорирование событий» произвести соотнесение типа события ИТСО, категории и класса устройств. Данный справочник должен быть заполнен на ЦУБ, а для РЦУБ необходимо выполнить рассылку.

6. **Создание и привязка объектов к узлу АИС**. Объект – это то, за чем наблюдаем с помощью Системы. Добавление объекта происходит в модуле «Объекты». Функции, доступные в модуле:

– добавление объекта;

– привязка объекта к карте;

– привязка объекта к серверу ИТСО (происходит в момент натравки камеры);

– привязка паспорта объекта;

– прикрепить помещения объекта (из созданных в модуле «Планы помещений»), открепить помещение, редактировать план помещения;

– если объект состоит из нескольких помещений, то также можно задать телепорт (для перемещения между помещениями);

– задать зоны слежения и разместить устройства ИТСО (камеры, датчики и т.д.);

– настроить участников (для корректной рассылки информации по узлам).

7. В Системе **реализована блокировка документов** при редактировании. Под документом здесь понимается любой элемент Системы, информация о котором заносится (узел, сервер, объект, план, паспорт и т.д.).

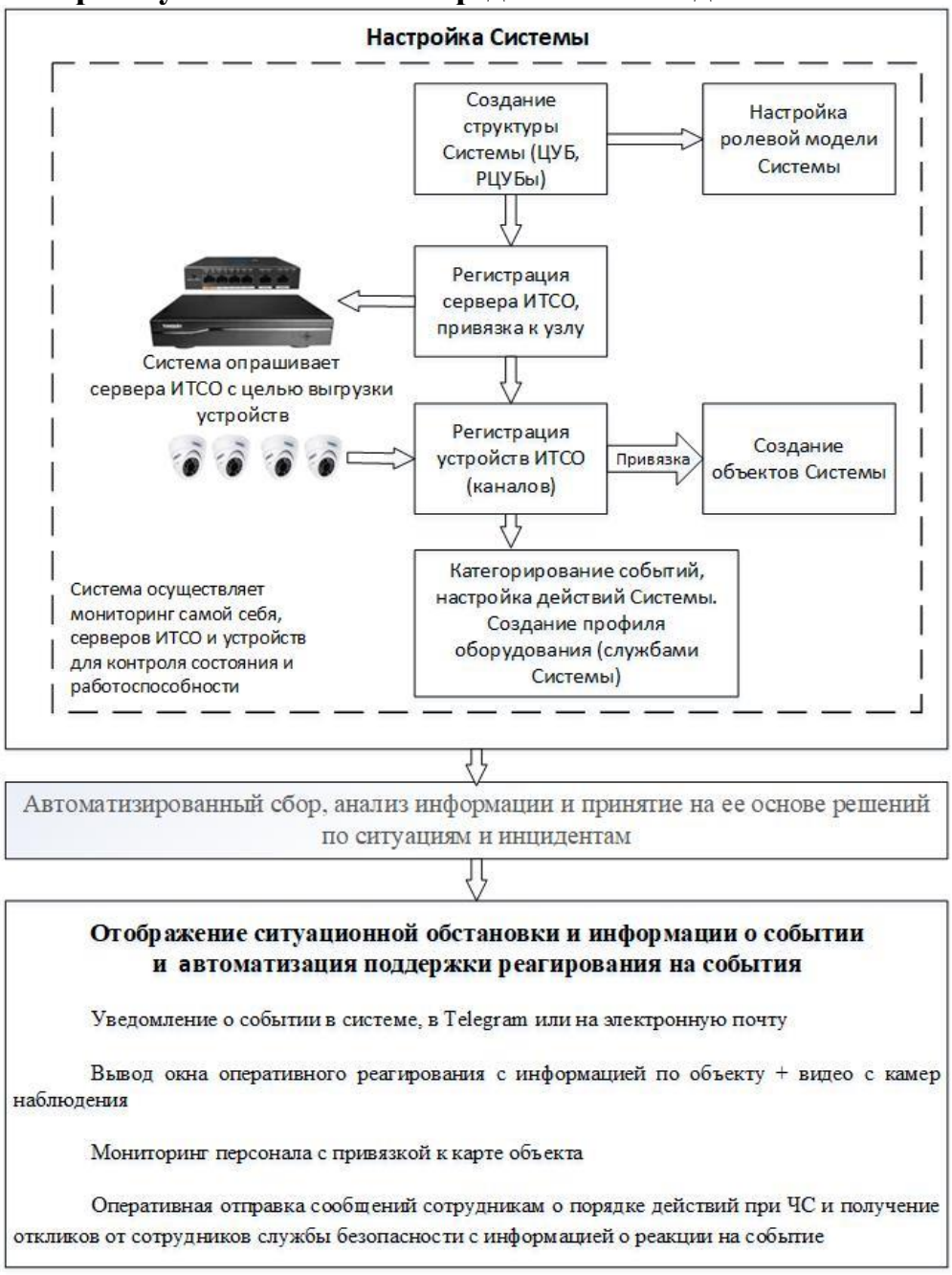
8. Если в Системе создается или редактируется документ (узел, сервер, объект), то **информация должна быть распространена** как сверху вниз, так и снизу вверх, по

структуре узлов. Замечание: справочник «Категорирование событий» распространяется сверху вниз.

9. **После** корректной настройки и **наступления события**, которое контролируется, **Система осуществит одно из заданных действий**: выведет всплывающее сообщение на сайте (с требуемой информацией); выведет тревожное окно; произведет снимок с камеры (который также можно вывести); отправит сообщения в Телеграмм (email). Для подсказки оператору правильных действий в Систему можно загружать инструкции, любые нормативные и регламентирующие документы, которые также будут выводится (отсылаться) при наступлении отслеживаемого события.

10. Система осуществляет **мониторинг собственного состояния**, следит за состоянием серверов ИТСО, подключенных к ним устройств.

Укрупненно работу Системы можно представить в виде схемы



Поддержание жизненного цикла ПО

Поддержание жизненного цикла Системы осуществляется за счет сопровождения и включает в себя проведение модернизаций Системы в соответствии с собственным планом доработок и по заявкам клиентов, консультации по вопросам установки и эксплуатации Системы.

В рамках технической поддержки Системы оказываются следующие услуги:

- помощь в установке Системы;
- помощь в настройке и администрировании;
- помощь в установке обновлений Системы;
- помощь в поиске и устранении проблем в случае некорректной установки обновлений Системы;
- пояснение функционала модулей Системы, помощь в эксплуатации Системы;
- предоставление документации;
- совершенствование Системы.

Техническая поддержка пользователей

Техническая поддержка пользователей осуществляется в формате консультирования пользователей и администраторов Системы по вопросам установки, администрирования и эксплуатации программного обеспечения Системы письменно по запросу, а именно:

- помощь по настройке/эксплуатации программного обеспечения Системы ИСБО-Плюс;
- оказание помощи в ходе плановых установок обновлений;
- техническая поддержка по восстановлению работоспособности после сбоев и отказов;
- устранение инцидентов и прочих выявленных недостатков в работе программного обеспечения;
- проверка функционирования программных средств Системы ИСБО-Плюс при смене версий;
- удаленный мониторинг рабочих параметров.

Консультационные услуги:

- консультирование по настройке/эксплуатации программного обеспечения ИСБО-Плюс;
- консультирование по установке/обновлении программного обеспечения ИСБО-Плюс;
- консультирование по вопросам документооборота в ИСБО-Плюс;
- консультирование по сообщениям журналов ИСБО-Плюс;
- консультации персонала Заказчика по особенностям работы с программным обеспечением ИСБО-Плюс.

Устранение неисправностей, выявленных в ходе эксплуатации ПО

В случае возникновения неисправностей в работе программного обеспечения Системы, либо необходимости в его доработке, пользователь направляет Разработчику запрос. Запрос должен содержать тему (краткая формулировка ошибки или предложения по доработке), суть (подробное описание проблемы или улучшения) и по мере возможности снимок экрана со сбоем (если имеется сбой).

Разработчик принимает и регистрирует все запросы, исходящие от пользователей, связанные с функционированием ПО. Каждому запросу присваивается уникальный номер.

Уникальный номер запроса является основной единицей учета запроса и при последующих коммуникациях по поводу проведения работ следует указывать данный уникальный номер.

После выполнения запроса Разработчик меняет его статус на «Выполнено», и при необходимости указывает комментарии к нему.

Разработчик оставляет за собой право обращаться за уточнением информации по запросу, в тех случаях, когда указанной информации недостаточно для выполнения заявки пользователя. Пользователь в этом случае обязуется предоставить информацию, включая журнал событий из компонентов, текстовые пакеты html и прочие необходимые атрибуты систем.

Неисправности, выявленные в ходе эксплуатации Системы, могут быть исправлены двумя способами:

- массовое автоматическое обновление компонентов Системы;
- единичная работа Разработчика по запросу пользователя.

Информация о совершенствовании программного обеспечения Системы

Цель процесса о совершенствования Системы заключается в непрерывном улучшении результативности и эффективности.

Совершенствование начинается с набора требований и реализации на разработку последовательности, которая содержит часть требований, далее добавляют дополнительные требования и так далее до тех пор, пока не будет закончено усовершенствование Системы. Для каждой части требований выполняют необходимые процессы, работы и задачи.

Программное обеспечение Системы регулярно развивается: в нем появляются новые дополнительные возможности, расширяется функционал, оптимизируется работа, обновляется интерфейс.

Пользователь может самостоятельно повлиять на совершенствование программы, для этого ему необходимо направить техническое предложение на электронную почту разработчика: info@center-inform.ru

Предложение будет рассмотрено и в случае признания его эффективности, будет добавлено в план разработки и соответствующие изменения появятся в новой версии.

Информация о персонале

Обслуживающий персонал, осуществляющий установку и настройку программного обеспечения Системы, должен обладать навыками работы с персональным компьютером и иными устройствами на уровне продвинутого пользователя операционных систем, а также иметь опыт работы.

Персонал на рабочих местах пользователей должен обладать навыками работы с персональным компьютером на уровне пользователя.

Техническая поддержка и модернизация программного обеспечения Системы осуществляется сотрудниками Разработчика, сбор и отработку запросов на техническую поддержку выполняют сотрудники техподдержки Разработчика.

Специалисты Разработчика (разработчики, аналитики, тестировщики, технические специалисты, консультанты) обладают необходимым набором знаний для работы со всеми компонентами, входящими в состав программного обеспечения Системы, при решении прикладных задач.