1. **Наименование** СПО «Синергет Ситуационный центр Сервер»
2. **Назначение**

СПО «Синергет Ситуационный центр Сервер» (далее сервер) предназначен для инцидентного управления системой безопасности, контроля технического состояния средств охраны, иерархического контроля и управления системами безопасности в глобальном масштабе.

Одной из задач сервера является управление инцидентами, происходящими на охраняемом объекте. Управление инцидентами является одной из важнейших задач организации системы безопасности объекта. В настоящее время уже недостаточно только предоставить информацию о возможном нарушении режима, необходимо проконтролировать, что информация верно проанализирована и предприняты необходимые действия. Для этого, сервер предоставляет оператору рекомендации по дальнейшим действиям, эти действия протоколируются и обеспечивается контроль всего процесса на верхнем уровне управления.

Создание инцидента может быть инициировано как любым событием системы: сработкой периметрального или пожарного датчика, получением извещения от модуля видеоаналитики, отказом оборудования, так и самим оператором, получившим информацию от системы видеонаблюдения или от другого сотрудника с территории объекта.

В процессе отработки инцидента события могут развиваться по самым различным сценариям. Предполагаемые типовые сценарии заранее программируются в систему при ее настройке, или добавляются в процессе эксплуатации, поэтому операторы работают только с интуитивно понятным интерфейсом управления. Создаваемые сценарии предполагают не только линейное развитие событий, но и условные переходы, ветвления, возврат для повторного сбора информации.

В качестве дополнительной информации в процессе реализации инцидента могут использоваться количественные данные от различных технических средств. Например, поступила информация о перегреве от датчика температуры в системе отопления. При небольшом перегреве оператору будут предлагаться определенные действия, если ситуация станет ухудшаться – температура расти, то экспертная система предложит другой, более радикальный, план управления инцидентом.

Сервер позволяет осуществлять многоуровневую обработку инцидентов. Данная возможность позволяет обрабатывать как инциденты разной важности, так и позволяет повысить надежность системы путем «резервирования» оператора. Отработка инцидента происходит и в случае отсутствия оператора на рабочем месте и в случае недостаточной компетенции оператора для отработки инцидента «особой» важности. При этом есть возможность анализа инцидентов на всех уровнях управления, в том числе в реальном времени.

На этапе настройки и конфигурирования системы каждое тревожное событие в системе классифицируется. Классификатор тревожных событий может содержать десятки и даже сотни вариантов определения принадлежности события к той или иной группе, например:

- «Нарушитель» - зона обнаружения пересечена человеком не санкционировано.
- «Сработка участка» - в зоне было обнаружено появление или перемещение постороннего предмета или животного любого типа, либо извещатель среагировал на шквальный ветер.
- «Контрольная сработка» - пересечение зоны обнаружения для проверки работоспособности извещателя.
- «Ложная тревога» - причину срабатывания установить не удалось. В видеокамеру объект-нарушитель зоны не попал и т.д.

В зависимости от вида события система в автоматическом режиме классифицирует данный инцидент и помещает его в определенную категорию: пожар, пересечение периметра, оставленный предмет и т.д. На основании присвоенной категории инцидента, система осуществляет анализ ситуации и предоставляет оператору всю необходимую информацию: видеоканалы, в зону видимости которых мог попасть инициатор инцидента, архивную видеозапись, схему местности, план подъезда, адреса и контактные телефоны ближайших отделений полиции, станций МЧС, больниц.

Так же оператору дежурной службы, который отрабатывает инцидент, система предлагает заранее подготовленную инструкцию, по выполнению действий оператором для отработки возникшего инцидента. На основании выбранного действия, система предлагает следующие шаги и скрывает предыдущие, до полного разрешения инцидента.

После закрытия инцидента формируется отчет по предпринятым действиям и видеоматериалами, связанными с инцидентом. Всегда имеется возможность открыть архивную информацию по закрытым инцидентам, просмотреть перечень всех действий, которые отрабатывали операторы ситуационного управления, список привязанных видеоканалов, просмотреть архивную запись. Сформированный отчет выводится на печать.

В качестве источников информации сервер использует данные, получаемые с различных технических средств охраны. Любые видеокамеры и видеосерверы, приемно-контрольные приборы охранной и охранно-пожарной сигнализации, охранные и периметральные извещатели различных принципов действия, датчики состояния инженерных сооружений, датчики состояния окружающей среды (сейсмические, паводка, схода лавин, и т.д.), координаты, передаваемые GPS/ГЛОНАСС трекерами, используемыми для оснащения подвижных объектов охраны или мобильных групп охраны и реагирования, РЛС – вот далеко не полный перечень тех технических средств охраны, которые поддерживает система. Для расширения функционала базового СПО можно подключить следующие лицензии:

- «Лицензия на подключение видеоканалов SYT-IP»
- «Лицензия на подключение системы СКУД SYT-ACMS»
- «Лицензия на подключение ОПС SYT-SEC»
- «Лицензия на систему конференцсвязи SYT-CONF»
- «Лицензия на подключение IP АТС SYT-ATS»
- «Лицензия на модуль оповещения SYT-WARN»
- «Лицензия на модуль геоинформационной системы SYT-GEO»
- «Лицензия на Синергет API SYT-API»
- «Лицензия на работу с системами распознавания лиц людей SYT-FACE»
- «Лицензия на подключение дополнительных серверов SYT-SERV»

Сетевые и топологические возможности «Синергет Ситуационный центр» позволяют использовать неограниченное число серверов ситуационного управления и неограниченное число клиентов (АРМ оператора), обеспечивать устойчивую работу в маршрутизируемых сетях с неоднородной пропускной способностью.

Сервер обладает двусторонней настраиваемой репликацией данных для получения произвольных топологий построения системы. В системе может быть несколько главных серверов, которые обмениваются информацией между собой и зависимыми серверами в соответствии с поставленными задачами и требованиями по безопасности.

В целях повышения надежности и сохранения работоспособного состояния системы при отказах серверного оборудования, сервер использует резервирование. Введение аппаратной избыточности в системе позволяет обеспечить работоспособность системы при отказе одного или нескольких серверов. Программное обеспечение дает оператору возможность управления с любого АРМ, входящего в систему, и обеспечивает, при необходимости, одновременную работу нескольких операторов с одной карточкой инцидента.

Базовое СПО для организации сервера ситуационного центра позволяет подключать до 50 внешних серверов или систем. Сервер обеспечивает режим совместной работы с другими серверами "Синергет Ситуационный центр" в случае необходимости расширения системы.

Лицензия распространяется на 1 сервер.

3. Область применения

Сервер применяется совместно с системой управления силами и средствами обеспечения безопасности «Синергет Ситуационный Центр», разработки Стилсофт.

4. Минимальные системные требования

Наименование параметра	Значение
Процессор, не ниже	Intel Atom
Оперативная память, не менее, ГБ	2

Локальная сеть Ethernet, со скоростью передачи данных, не менее, Мбит/сек	100
Операционная система*	Windows 7/Vista/8/10 CentOS 6/7 Ubuntu 16 Astra Linux Special Edition 1.4/1.5 Astra Linux Common Edition 1.10/1.11

***** – Выбор операционной системы оговаривается при заказе.