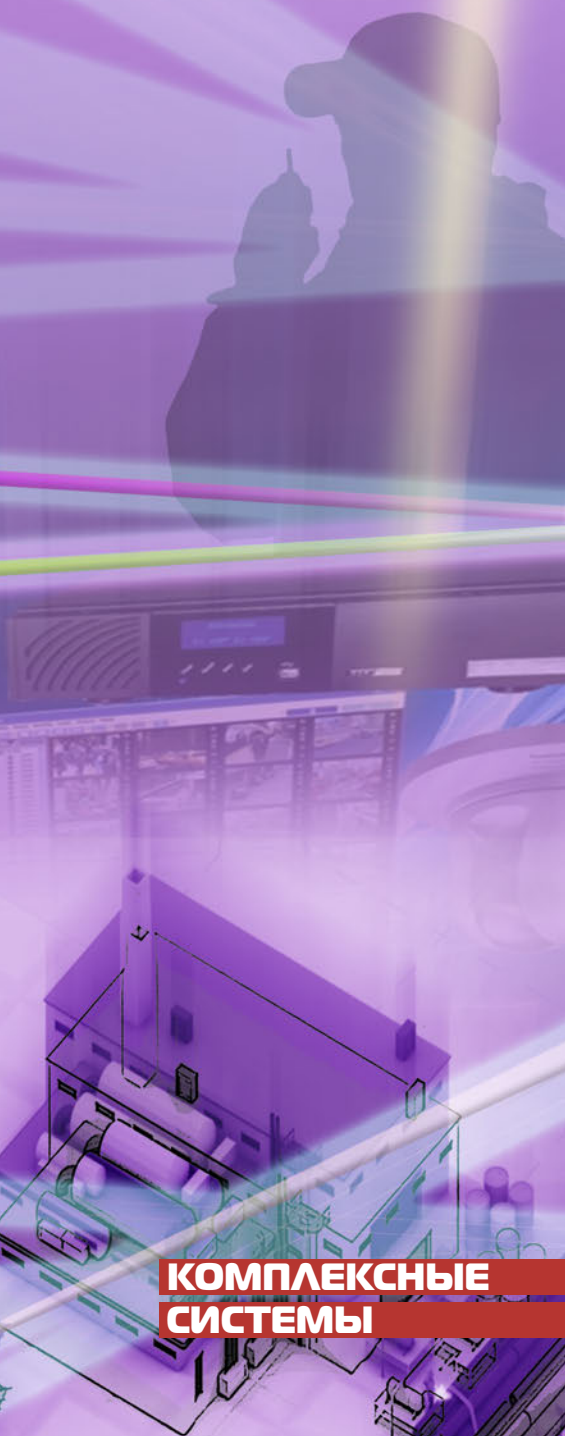
СИСТЕМЫ БЕЗОПАСНОСТИ КРУПНЫХ ОБЪЕКТОВ — ПОДХОД К СОСТАВЛЕНИЮ ТЗ

Татарченко Николай Валентинович
технический директор, Группа «Октаграм»

Приступая к работе по созданию системы безопасности крупного объекта, логично обратиться к существующему опыту и познакомиться с обзорами в специальных изданиях и Интернете. Русскоязычный сегмент паутины дает только очень общее описание и частные примеры. Специальная литература не всегда доступна. Часто материалы по данной теме носят пространный характер. В англоязычном секторе материалы более системны и структурированы, но тоже не дают прямого ответа на вопрос как лучше организовать безопасность крупного объекта.



КОМПЛЕКСНЫЕ СИСТЕМЫ

Начнем с основных понятий в системах безопасности [1]:

1. Основные аварийные сигналы генерируются путем обнаружения отклонений от нормы при измерениях процесса или оборудования. Правильные настройки системы устанавливаются так, чтобы аварийные сигналы запускались достаточно рано для эффективного ответа операторов, а с другой стороны — количество ложных тревог сводилось к минимуму.

2. Сгенерированные аварийные сигналы образуются путем объединения состояния нескольких основных аварийных сигналов, которые вместе описывают состояние системы или подсистемы точнее, чем один сигнал тревоги. Такие сигналы тревоги следует использовать только в том случае, если они приводят к значительному сокращению числа основных аварийных сигналов путем подавления или при предоставлении более прямого указания на причину проблемы.

3. Ключевыми аварийными сигналами являются важные аварийные сигналы, представленные после фильтрации таким образом, который позволяет на их основе построить максимально простую и полную картину происходящего на объекте.

4. Для некоторых видов тревог ввиду критичности их для безопасности объекта существуют механизмы валидации (т.е. проверки и подтверждения). Действия системы при таких тревогах обычно контролируются оператором (как «последнее средство» для обработки нерелевантных тревожных сигналов, включения тревог, которые не были сгенерированы системой, принятие решения о тревоге в случае поломки/порчи участка системы или отсутствия персонала) согласно процедуре.

5. Когнитивная обработка — это обработка информации в человеческом мозге на основе ранее приобретенных знаний. Эффективность обработки зависит от того, как воспринимается новая информация, а также в какой форме хранятся знания, используемые в обработке, и как к ней можно получить доступ (т.е. путем простого распознавания или размышлений). Когнитивный ответ — тип ответа, при котором оператор не выполняет никаких физических действий, от него требуется только внутренняя обработка информации.

6. Для восприятия информации требуется определенное количество времени. Оператор может одновременно хранить только 7 ± 2 единицы информации. Из-за этого важно, чтобы при всех вероятных сценариях тревоги общее количество одновременных сигналов, приходящихся на одного оператора, не превышало 7 и максимальная скорость обновления информации не перегружала оператора.

7. Интеграция разных систем безопасности позволяет объединить (агрегированный сигнал тревоги) информацию разного вида и уменьшить количество таких сигналов. Умственные способности, необходимые для обработки этой конкретной информации, не так загружены, и мозг сможет эффективно обрабатывать больше информации.

8. Мозг оператора гораздо легче воспринимает информацию, которая интуитивно понятна и легко распознается. Об этом более подробно поговорим в разделе об интерфейсах.

9. Для обеспечения более гибкой и удобной работы системы должны быть выбраны критерии представления информации и аварийных сигналов: время, система/подсистема, площадь, ответственность оператора, приоритет.

10. Не рекомендуется использовать более четырех приоритетов тревоги в системе. В любом типе дисплея для нормального отображения аварийных сигналов рекомендуется использовать не более трех приоритетов. Если на объекте существует несколько систем сигнализации, для всех систем должно использоваться согласованное определение приоритета тревоги.

11. Информация в системе должна выдаваться раздельно различным группам персонала (согласно решаемыми ими задачами): операторы диспетчерской, техники, персонал охраны, инженерный состав, пожарные и пр.

12. Уровень технического оснащения и подготовки злоумышленников довольно высок и позволяет нейтрализовать и преодолеть многие традиционные системы. В разрабатываемых и внедряемых системах должен учитываться человеческий фактор, приниматься во внимание халатность охранника или возможное вступление в сговор в корыстных целях.

Создание системы крупного объекта должно основываться на философии безопасности, включающей:

- Определение, назначение и обоснование приоритетов сигнализации.
- Определение принципов генерации и структурирования сигналов тревоги.
- Основные функции системы: предупреждение о событиях и тревогах и ведение журнала.
- Роль оператора и как она меняется в зависимости от рабочей ситуации, поддержка, необходимая оператору в разных состояниях системы.
- Учет ограничений оператора при разработке системы.

Важное место в создании, поддержании эффективной работы и модификации системы играет документация, включающая не только полное описание системы и ее функций, но содержащая полную информацию о жизненном цикле. На основе документации и анализа отчетов системы может быть разработана схема модификации системы безопасности.

При модификации системы безопасности (также можно использовать на этапе разработки проекта) важны показатели эффективности:

- Частота приходящих сигналов тревоги (с распределением приоритетов) согласно зарубежным источникам [1] рассматривается в диапазоне: тревога 1 раз в минуту (неприемлемо) — тревога 1 раз в 10 минут (оптимально).
- Количество аварийных сигналов в главном списке (с распределением приоритетов).
- Частотное распределение аварийных сигналов: для выявления любых «плохих участников», которые вносят значительный вклад в общую аварийную нагрузку.
- Время отклика оператора (время до принятия решения). Слишком длительное или слишком короткое время отклика указывают, что система используется не по назначению.

В настоящее время очевидно, что система для большого объекта требует перехода от отдельных «железных» решений в ИТ-область, т.е. использования программных комплексов, которые самостоятельно анализируют, систематизируют, архивируют необходимую информацию. Таким образом, создается система безопасности крупного объекта, обладающая повышенной программной и аппаратной устойчивостью, гибкостью и высокой степенью защиты.

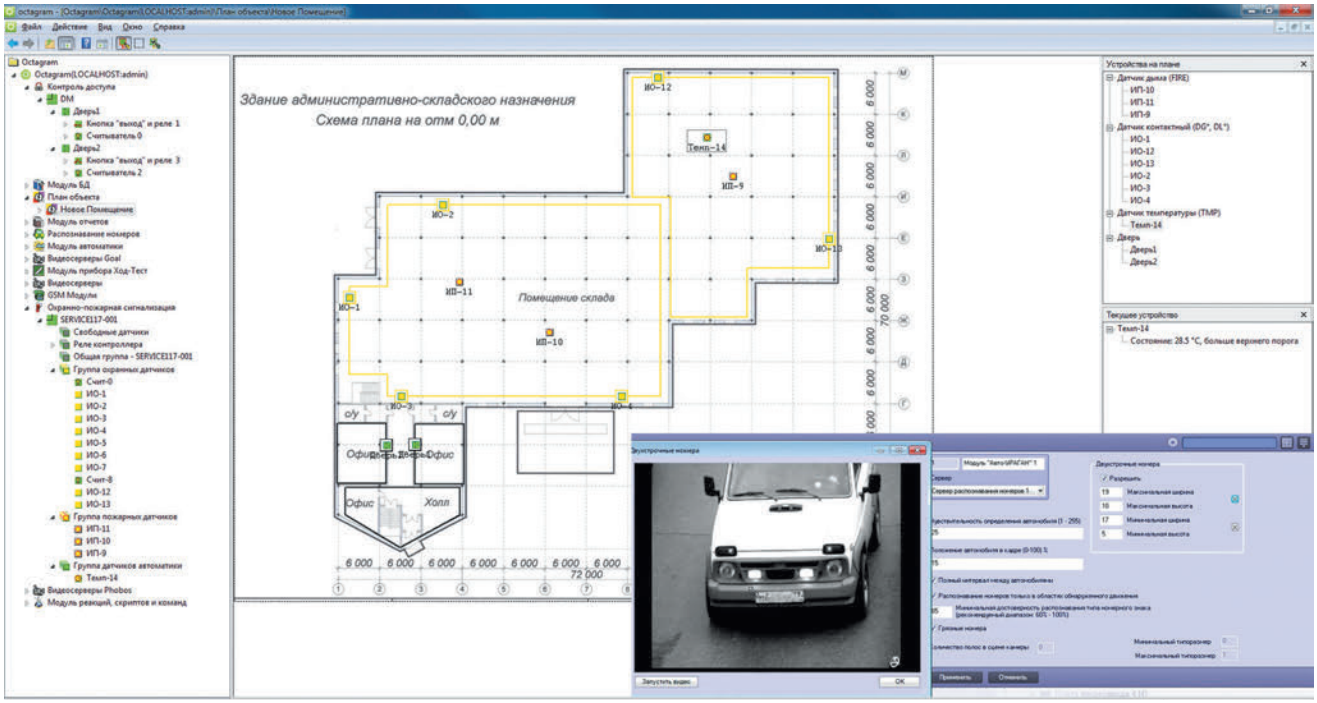
Свойства программного обеспечения, наиболее важные для систем большого объекта:

1. Широкий спектр поддерживаемого периферийного оборудования от различных вендоров. Объединение оборудования разного назначения от различных производителей в единую систему путем взаимодействия между подсистемами безопасности: системой контроля доступа, охранной и пожарной сигнализации, пожаротушения и оповещения о пожаре, системой видеонаблюдения и аналитики.

2. Наличие надежной и оперативной технической поддержки со стороны вендора и возможность доработки ПО под требования заказчика в разумные сроки.

3. Работа с продуктами Microsoft как стандартно используемой платформой в информационной отрасли.

4. Возможность интеграции с ПО, используемым заказчиком для управления деятельностью организации с целью повышения эффективности общих процессов управления. Открытость ПО для сторонних разработчиков позволяет IT-подразделениям заказчика самостоятельно взаимодействовать с системой безопасности, проводя



передачу данных из/в систему. Открытость обеспечивают: стыковка отдельных модулей, соответствующие форматы хранения настроек объектов, их экспорта и импорта, возможности работы с базами данных.

5. Встроенный аппарат реакций, позволяющий автоматизировать действия системы в случае необходимости.

6. Оптимальность для среднего и крупного предприятия любой сферы деятельности, что обеспечивается масштабируемостью — эффективной работой на объектах разного масштаба (используемые технологии и архитектурные решения могут обеспечивать его работу на малых, средних и крупных системах).

7. Высокая надежность и живучесть ПО. При выходе из строя отдельных рабочих станций и серверов нагрузка динамически перераспределяется между исправными компьютерами. Контроллеры могут работать автономно.

8. Возможность интеграции уже установленных на объекте систем безопасности в единый комплекс.

Существует точка зрения, что поскольку основная нагрузка ложится на программные комплексы, то требуются большие серверные мощности, и очень важно с самого начала рассчитать вычислительные ресурсы с серьезным запасом (порядка 30–40%). Наверное, имеет смысл принять во внимание такой опыт.

Это необходимо, так как за время реализации проекта, во-первых, линейка серверного оборудования может устареть; во-вторых, у заказчика могут появляться дополнительные желания по модернизации системы. Клиенту кажется, что внести изменения в уже реализованный проект довольно просто. Это может быть не сложно, если вы не зажаты в тиски вычислительных мощностей.

Нередко кибербезопасность системы не принимается во внимание при подготовке проекта, хотя играет очень важную роль в любой информационной системе. Более того, клиентам бывает трудно объяснить необходимость дорогостоящего оборудование и ПО, а стоимость построения системы информационной и физической безопасности сопоставимы. Нужно обязательно уделить внимание созданию серьезной системы информационной безопасности.

Не стоит недооценивать выбор контрольно-управляющего оборудования пожарной и охранной сигнализаций, системы контроля доступа и видеонаблюдения. Весьма эффективным может оказаться подход, принятый сейчас в информационной индустрии — использование стандартизованных мультивендорных систем [2]. При таком подходе создание, эксплуатация и модернизация системы безопасности большого объекта становятся несложной рутинной процедурой. Важную роль здесь играет однообразие используемых компонент системы, их взаимозаменяемость и возможность смены функций уже существующих узлов системы без замены оборудования. Например, один контроллер может выполнять множество функций в зависимости от того, какая микропрограмма в него записана. Имеются в виду готовые микропрограммы, которые все участники цепочки от вендора до пользователя используют как есть, а не создают для свободно программируемых контроллеров. Управляющее оборудование для безопасности должно, как персональный компьютер, быть применимым для любой задачи, существующей в отрасли, но при этом по возможности быть не компьютером, а специальным устройством, сочетающем простоту и универсальность.

До сих пор на больших объектах вы сталкивались с необходимостью использовать множество функций и, следовательно, большое количество разных моделей управляющего оборудования. Теперь с оборудованием ряда производителей (например Apollo, Octagram) возможно проектировать системы любой сложности, основанные на одном типе контроллера, что значительно упрощает задачи проектировщиков, монтажников и обслуживающего персонала. В сочетании с мультибрендовостью такие системы не только удобны для заказчика и исполнителя, но и экономически выгодны.

Выбор периферийного оборудования обычно связан с управляющим, но в случае использования мультвендорных систем может вестись исходя из лучших технико-экономических характеристик «периферии». Такой подход уже обсуждался на страницах этого журнала [2].

Определение правильной структуры связи компонент системы между собой или создание сети не менее важно, чем выбор основных узлов системы безопасности (компьютеры и контроллеры). Как было показано в статье [3]: «Для создания надежной СБ желательно, а в случае наличия соответствующих нормативных документов необходимо, использовать топологию сети, обеспечивающую непрерывную работу в случае злонамеренного или случайного повреждения связей с компонентами системы». Это в полной мере относится к системам безопасности крупных объектов.

Одну из важнейших ролей в обеспечении надежной и продуктивной работы системы играет интерфейс ПО для мониторинга большого объекта, поскольку основная задача системы состоит в выполнении функций центра монито-

ринга тревожных сигналов и управления различными системами безопасности на объекте. Информация о тревоге будет легко воспринята, если она хорошо видна среди других типов информации, и можно легко интерпретировать существенные элементы. Благодаря эргономичному графическому интерфейсу система помогает операторам быстро анализировать масштаб и важность происшествия и предпринимать немедленные и эффективные действия. Интерфейс обеспечивает предоставление операторам подробной информации о событиях, планы действий по всем возможным типам тревог. Интерфейс обеспечивает рабочие процессы взаимодействия между операторами с передачей сообщений и настраиваемыми сценариями.

Стандартом в интерфейсе де-факто стала поддержка планов объектов в основных стандартных графических форматах, стандартные значки детекторов и других объектов, включая определения цвета, события и управления.

Для облегчения когнитивной обработки информации наряду с графическим представлением важным является управление и мониторинг через интерактивные значки на планах объектов и использование представления объекта в виде логического дерева с всплывающими фотографиями, руководствами и инструкциями.

Важен обзор устройств всех подключенных подсистем, включая периферийные устройства (детекторы) и внутренние виртуальные устройства (оператор, сервер и т.д.). Эта информация представляется в форме древовидной структуры с подробной информацией об адресе, состоянии, типе, местоположении и примечаниях.

Снижать нагрузки на операторов и предотвращать злоупотребления позволяет использование настраиваемых прав доступа операторов для мониторинга и управления, предоставление операторам определенной информации, возможность разделения охраняемого объекта на автономные подразделения и предоставления операторам разрешений на управление только определенными подразделениями.

Невозможно представить систему без журнала для подробного документирования всех событий (включая полученные сообщения и предпринятые действия) и службы отчетов для быстрого создания отчетов на основании журнала событий. Однако при проектировании объекта следует согласовать с заказчиком основной набор отчетов.

Полезным будет отображение дополнительной графической информации в определенных ситуациях (например, маршрутов эвакуации в случае пожарной тревоги) в дополнение к стандартному интерфейсу.

Как уже отмечалось в основных определениях, в системе необходимо предусмотреть возможность оператора вручную включить сигнал тревоги на участке, например в том случае, если оператору сообщают по телефону об опасной ситуации.

Модуль запуска приложений позволяет системе запускать различные приложения на основе предварительно заданных условий. Типичным применением этой функции является автоматическое резервное копирование системы по заданному расписанию.

В случае использования платформы на базе веб-сервера для подключения клиентских рабочих станций требуется только веб-браузер, что значительно упрощает организацию удаленных рабочих мест.

Вот далеко не полный перечень важных свойств интерфейса системы безопасности большого объекта.

Таким образом, мы рассмотрели некоторые особенности системы безопасности большого объекта. С определения того, какие из них будут играть ключевую роль на вашем объекте, а какие останутся просто полезными на будущее или будут отвергнуты, следует начинать работу над проектом. Далее особое внимание нужно уделить обследованию объекта, обсуждению с заказчиком особенностей проекта. При разработке и построении эффективной системы защиты объекта важно провести анализ угроз, связанных с деятельностью, особенностями расположения, криминогенными факторами, которые и определяют выбор принципов и оборудования при построении системы защиты. Если предварительная работа сделана верно, то вы не упустите из виду даже такие (на первый взгляд) неочевидные подсистемы, как Ход-Тест, позволяющие точно документировать работу охраны и обслуживающего персонала или контролировать, жив ли сотрудник во время обхода территории.

Все сказанное в этой статье составляет малую часть информации, необходимой для правильной расстановки приоритетов при разработке и создании системы безопасности большого объекта. Надеюсь, что это пробудит в вас интерес к более детальному изучению этой темы. В результате выиграют все: и вы, и заказчик.

ЛИТЕРАТУРА

1. *Norwegian Petroleum Directorate. Principles for alarm system design. February 2001 YA-711.*
2. *Татарченко Н. В. Мультивендорные системы безопасности // Алгоритм безопасности. 2018. № 1.*
3. *Татарченко Н. В. Сети для систем безопасности. Теория. История. Практика // Алгоритм безопасности. 2018. № 2.*