# УПРАВЛЕНИЕ ТЕХНИЧЕСКИМ СОСТОЯНИЕМ КСБ — ПРОБЛЕМЫ И РЕШЕНИЯ

***Садеков Данат Сямиуллович***
*директор по развитию бизнеса,*
***Таран Сергей Валерьевич***
*руководитель проектов ООО «ВИТ-Центр»*

***Современные комплексные системы безопасности предприятий (КСБ) становятся большими и сложными. Управление техническим состоянием КСБ — непростая задача. Для обеспечения стабильной и надежной работы КСБ требуется учитывать множество новых аспектов от управления инженерной и IT-инфраструктурой до инвентаризации активов и управления конфигурациями.***

Информация данной статьи в большей части предназначена для технических руководителей крупных предприятий и организаций, которые отвечают за эксплуатацию и развитие территориально распределенных комплексных систем безопасности. Особенно она актуальна для объектов следующих типов:

- Предприятия нефтегазовой отрасли.
- Промышленные предприятия.
- Предприятия транспорта и связи.
- Предприятия торговли и логистические комплексы.
- Офисные центры и гостиницы.

Для надежной работы КСБ требуется качественная эксплуатация большого количества систем, в том числе, систем антитеррористической защиты, пожарно-охранной сигнализации, охранного телевидения и видеонаблюдения, пожаротушения, аварийного освещения и оповещения, охраны периметра, контроля и управления доступом, электроснабжения, IT-инфраструктуры, диспетчеризации, связи.

Современные системы безопасности на крупных объектах включают в свой состав десятки и сотни технических средств с сетевым взаимодействием и управлением, и сами являются довольно сложными IT-системами.

Довольно распространенной практикой на объектах являются создание и модернизация систем безопасности в разное время и разными организациями. Эксплуатационное обслуживание перечисленных систем в крупных компаниях часто передается подрядным организациям. В этом случае у управляющей компании возникает проблема объективного, независимого от подрядчика, контроля фактического состояния систем. Выборочный, эпизодический контроль или контроль по инцидентам не позволяет объективно оценить качество постоянной работы подрядчика по обслуживанию. Недобросовестные исполнители, зная об отсутствии технического контроля, зачастую злоупотребляют доверием заказчика.

Опытный специалист возразит и скажет, что современные системы содержат в своем составе средства для удаленного контроля работоспособности и управления основными режимами работы. Действительно, наиболее профессиональные системы имеют штатные средства для организации централизованного управления и мониторинга территориально распределенных иерархичных систем. Однако в большинстве случаев системы управления являются средством администрирования и управления определенным классом систем или систем от конкретного производителя. Дежурная смена службы безопасности, как правило, реагирует только на аварийные сообщения от систем управления. Администрированием же этих систем занимаются либо подрядчики, либо инженеры разных служб. Поэтому общая информация о статистике и динамике изменений параметров систем, как правило, централизованно не собирается и не анализируется.

Другой проблемой при эксплуатации систем безопасности часто бывает сложность по поддержанию в актуальном состоянии базы исполнительной документации и информации о фактическом составе оборудования на объектах.

При завершении строительства объектов предприятий, при сдаче в эксплуатацию систем безопасности и других слаботочных систем исполнитель каждой системы передает исполнительную документацию на смонтированные системы. Но, зачастую, в ней далеко не в полной мере отражены последние изменения состава и конфигурации технических средств, внесенные на этапах пуско-наладочных работ и опытной эксплуатации.

Эксплуатирующей компании бывает трудно проверить в полном объеме фактический состав систем и выявить расхождения с исполнительной документацией, так как эта проверка в большинстве случаев проводится вручную. Средств автоматизированной проверки систем, как правило, нет.

В процессе эксплуатации, особенно в период гарантийного обслуживания, довольно часто подрядными организациями осуществляется замена вышедших из строя устройств на аналогичные, на время ремонта. Однако контроль факта замены устройств как на время ремонта, так и возврат отремонтированного устройства, также осуществляется вручную. Изменения состава технических средств в эксплуатационную документацию вносятся очень редко.

Подобная ситуация приводит к недостоверности данных о составе технических средств, сложности проведения инвентаризации, некачественному управлению ТО, недостоверности учета периодов эксплуатации и неоптимальному планированию ремонтов и замен технических средств.

Похожая ситуация складывается и с информацией о конфигурационных настройках. Информация о конфигурации конкретных систем и программно-технических средств на объектах хранится в виде разрозненных комплектов бумажной или электронной документации. У различных подрядчиков и сервисных организаций приняты свои правила учета изменений конфигураций систем на объектах. Как правило, это электронные файлы различных форматов, которые хранятся на файловых ресурсах подразделений, ответственных за эксплуатацию и их подрядчиков. Резервное копирование файлов конфигураций в лучшем случае осуществляется вместе с резервным копированием файловых ресурсов компании. И в документацию оперативные изменения конфигураций обычно не вносятся.

Все перечисленные проблемы эксплуатации программно-технических средств на самом деле не новы, и буквально еще недавно были очень актуальны и для большинства IT-систем предприятий. В связи со значительно большей динамикой развития IT-систем, быстрым проникновением их во множество бизнес-процессов компаний и значительно меньшими длительностями их жизненных циклов, IT-отрасль довольно быстро прошла путь от реактивного управления IT-ресурсами до процессного управления IT-услугами.

В настоящее время для управления IT-услугами и IT-ресурсами предприятий принято использовать сервисные модели управления ITSM, основанные на практиках ITIL. Использование процессных моделей ITIL для управления информационными технологиями получило широкое применение как в мировой практике, так и в российских компаниях.

**ITSM (IT Service Management, управление IT-услугами)** — подход к управлению и организации IT-услуг, направленный на удовлетворение потребностей бизнеса.

**ITIL (IT Infrastructure Library)** — библиотека инфраструктуры информационных технологий, описывающая лучшие из применяемых на практике способов организации работы подразделений или компаний, занимающихся предоставлением услуг в области информационных технологий.

На основе ITIL разработан международный стандарт ISO 20000 «Information technology — Service management». В России в 2010 году принят стандарт ГОСТ Р ИСО/МЭК 20000 «Информационная технология. Менеджмент услуг», который разработан методом аутентичного перевода ISO 20000.

В настоящее время актуальным является издание ITIL v.3, состоящее из 5 книг:

- «ITIL Service Strategy» («Стратегия сервиса»);
- «ITIL Service Design» («Проектирование сервиса»);
- «ITIL Service Transition» («Передача сервиса»);
- «ITIL Service Operations» («Эксплуатация сервиса»);
- «ITIL Continual Service Improvement» («Постоянное улучшение сервиса»).

Библиотека ITIL содержит описание процессов, в том числе такие, как управление каталогом услуг, управление финансами, управление знаниями, управление качеством и более 20 других процессов управления. Конечно же, в реальной практике, в зависимости от размеров предприятия и критичности IT-сервисов для основной деятельности, на предприятиях внедряются и формализуются не все процессы ITIL. Наиболее часто даже небольшие предприятия внедряют процессы управления каталогом услуг (service catalogue management), управления активами и конфигурациями (service asset and configuration management), управления поддержкой (service desk) и управления изменениями (service management).

Для автоматизации процессов управления IT используются специализированные программные комплексы. Профессиональные системы ITSM включают в свой состав как минимум следующие основные модули:

- IT Asset Management (ITAM) — управление IT-активами, автоматизации процессов закупки, планирования, учета и отслеживания состояния IT-активов;
- IT Service Desk — автоматизация процессов управления сервисной поддержкой;
- Network Monitoring (Management) — контроль качества работы сетевого оборудования и сетевых сервисов.

Комплексные ITSM-системы от крупных производителей, таких как BMC, HPE, IBM, рассчитаны на использование в крупных IT-структурах и способны удовлетворить потребности самых разных функциональных бизнес-пользователей. Однако вместе с большими возможностями, эти системы обладают и высокой стоимостью, требуют специальной технической и организационной подготовки для эффективного их использования.

Также на рынке существуют и open source решения, способные решать задачи автоматизации процессов управления IT. Эти решения, как правило, направлены на решение отдельных задач и очень непросто поддаются адаптации под требования конкретного предприятия или для взаимодействия со смежными системами.

Итак, вернемся к проблемам управления системами безопасности.

Может ли опыт IT-отрасли быть применен в сфере обеспечения безопасности объектов? Да, конечно! Как мы уже вспоминали в начале статьи, современные КСБ де-факто стали вполне серьезными IT-системами и используют самые современные IT-технологии. Вполне логично можно предположить, что уже апробированные методики управления в IT-отрасли должны быть так же эффективны и при управлении системами безопасности на всех этапах их жизненного цикла: проектирования и внедрения; эксплуатации, периодической модернизации и вывода из эксплуатации.

Для реализации системного подхода к управлению техническим состоянием КСБ объектов разумно обратить внимание на накопленный опыт в IT-отрасли и использовать его с учетом специфики деятельности по обеспечению безопасности. Как правило, внедрение процессного управления в IT начинается с описания и формализации основных процессов управления активами и конфигурациями, а также управления изменениями и управления поддержкой. После описания этих процессов становится возможным их автоматизировать.

Однако использование систем управления ITSM применительно к системам безопасности простым копированием опыта сталкивается с особенностями их структур. К ним относятся: отсутствие описанных и регламентированных процессов по управлению активами; разнородность технических средств систем безопасности; недостаток квалифици-


***Рис. 1.*** Структура зонтичной системы мониторинга

рованного в области IT эксплуатирующего персонала; сложность и высокая стоимость ITSM-решений. И тем не менее, применять методики ITIL для управления активами комплексной системы безопасности (КСБ) можно. Просто нужно с чего-то начать.

Наиболее оптимальным первым шагом на пути использования практик ITIL применительно к системам безопасности является внедрение процесса управления активами систем безопасности и организация объективного контроля их технического состояния. Ведь невозможно управлять тем, что не контролируется.

В качестве технической основы для практической реализации этих процессов может послужить внедрение зонтичной системы мониторинга технического состояния программно-технических средств безопасности, что позволит осуществить их инвентаризацию и начать объективный контроль фактического состояния, протоколирование изменений и инцидентов.

При этом, несмотря на большое количество представленных на рынке систем зонтичного мониторинга, выбрать систему, подходящую для систем безопасности, не так просто, как может показаться на первый взгляд. Это связано с тем, что классические системы мониторинга IT-оборудования, как правило, ориентированы на работу с IT-оборудованием и ПО, использующими стандартные протоколы сетевого взаимодействия Ethernet и TCP/IP. В то же время в системах безопасности до сих пор широко используются интерфейсы и протоколы более низкого уровня взаимодействия RS-232/RS-485, Modbus, часто используются проприетарные протоколы.

На наш взгляд, для КСБ в качестве системы зонтичного мониторинга наиболее удачно подходят системы на базе интеграционных платформ класса «Интернет вещей» (Internet of Things). Такое обобщенное название класса систем обычно смущает специалистов и наводит на мысли об умных холодильниках, самостоятельно заказывающих продукты в Интернет-магазине. Действительно, понятие «Интернет-вещей» повсеместно используется производителями и участниками рынка в маркетинговых целях и затмевает собой техническую сущность этих систем. Укрупненно системы для «Интернета вещей» можно разделить на два типа:

**1.** Системы, ориентированные на управление умными устройствами, подключенными к сети Интернет (управление бытовыми приборами, видеокамерами, охранными системами, датчиками контроля окружающей среды, освещением и т.п.). Как правило, пользователями являются физические лица, а серверная часть является облачным сервисом в сети Интернет. К этим же системам можно отнести и системы «Умный дом» с сервером в виде сервиса в сети Интернет.

**2.** Системы, предназначенные для управления устройствами различного назначения с использованием сетей передачи данных, в том числе Интернет, в качестве транспортной среды. Отличительной особенностью этих систем является наличие программного или программно-аппаратного сервера, который размещается внутри локальной сети, но может быть размещен и во внешней сети, в том числе с подключением через сеть Интернет. Эти системы в большинстве случаев являются развитием систем управления технологическим оборудованием (SCADA) или систем управления сетевым оборудованием (Network Node Management).

В настоящей статье, в контексте рассматриваемого вопроса, мы говорим только о системах второго типа, т.е. системах управления оборудованием с использованием сетевых технологий, и далее называем зонтичными системами мониторинга и/или управления техническим состоянием программно-технических средств.

В настоящий момент на рынке представлены и активно развиваются несколько подобных платформ, в том числе отечественного производства. Такие системы позволяют организовать мониторинг и контроль совершенно различного оборудования, как классических средств IT-инфраструктуры (компьютерное, серверное, сетевое оборудование и т.п.), так и промышленных контроллеров различного назначения, в том числе, контроллеров

систем безопасности. За счет модульности структуры подобных систем мониторинга становится возможным реализовать на одной платформе как контроль технического состояния, управление изменениями конфигураций, так и автоматизацию процессов управления активами КСБ. Следует отметить, что даже без использования проприетарных протоколов производителей оборудования, а только с использованием стандартных протоколов сетевого взаимодействия, таких как SNMP, ICMP, WMI и т.п., такие системы позволяют организовать мониторинг функционирования КСБ в целом и отдельных технических средств по значительному числу параметров. Это позволяет внедрять систему мониторинга независимо от производителей ПТС КСБ.

Внедрение системы зонтичного мониторинга позволит системно реализовать на техническом уровне и с минимизацией влияния человеческого фактора базовые задачи управления активами КСБ, в том числе:

- периодическую инвентаризацию и контроль состава систем и программно-технических средств,
- объективный контроль фактического состояния и качества функционирования ПТС систем безопасности и обеспечивающих систем,
- протоколирование, уведомление и отчетность об изменениях в конфигурациях систем безопасности, важных событиях и инцидентах, а также о действиях эксплуатирующего и дежурного персонала.

Непосредственно эксплуатацию системы зонтичного мониторинга должна осуществлять служба эксплуатации технических систем безопасности. При этом этим специалистам не следует опасаться дополнительной нагрузки, т.к. они получают новый и удобный инструмент для повышения эффективности своей деятельности.

Для развертывания системы зонтичного мониторинга в большинстве случаев не требуется больших вычислительных ресурсов, ведь система не является заменой основных систем управления техническими средствами безопасности. Для выполнения контрольных функций не обязательно осуществлять мониторинг каждого устройства в реальном времени, вполне достаточно периодичности опроса в 1–5 минут только ключевых параметров работоспособности. Для развертывания системы достаточно небольшого сервера или рабочей станции. Доступ функциональных пользователей к системе может осуществляться по сети либо с помощью клиентского приложения, либо посредством браузера к веб-серверу.

Периодические отчеты о фактическом состоянии и о важных событиях могут отправляться в виде сообщений электронной почты ответственным специалистам по графику или немедленно. Таким образом, ответственные за эксплуатацию систем безопасности в начале рабочего дня могут получать автоматический объективный отчет о состоянии дел и оперативно принимать управленческие решения превентивно, не дожидаясь поступления жалоб от потребителей.

При внедрении системы мониторинга необходимо будет осуществить обнаружение и подключение устройств. Если устройства, которые мы подключаем к системе мониторинга, поддерживают стандартные протоколы SNMP, ICMP, WMI, то трудоемкость этих операций невысока и в значительной степени автоматизирована. При этом специалисты службы эксплуатации систем безопасности получают дополнительные преимущества, которые упрощают повседневную деятельность и снижают непроизводительные потери рабочего времени за счет:

- автоматического получения оперативной и достоверной информации о фактах сбоев в работе технических средств, что позволяет выполнять восстановительный ремонт, основываясь на достоверной и детализированной технической информации вместо неточных устных сообщений от пользователей,
- осуществления упреждающего ремонта и профилактики технических средств, находящихся в предаварийном состоянии, по оптимальному графику вместо срочных аварийных выездов в неурочное время,
- накопления объективной статистики функционирования технических средств и инцидентов для планирования обновления оборудования, оптимального планирования графиков обслуживания и т.п.

На крупных предприятиях с большим количеством эксплуатируемых подсистем безопасности внедрение системы зонтичного мониторинга позволит воспользоваться ее функционалом для исполнения своих должностных функций пользователям и ответственным лицам различных подразделений, используя единый источник достоверной информации. Это также позволит настроить распределенную систему оперативного информирования о техническом состоянии ПТС специалистов разных подразделений, при этом сохраняя централизованный контроль за состоянием КСБ в целом.

*Внедрение зонтичной системы мониторинга технического состояния КСБ является первым шагом на пути перевода системы управления системами безопасности на следующий уровень от ресурсной модели к процессной и позволит снизить риски неконтролируемого снижения показателей надежности функционирования систем безопасности.*

БИК ИНФОРМ
ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ
BOSCH
Разработано для жизни

ВЗРЫВОЗАЩИЩЕННЫЕ
IP КАМЕРЫ

Совместное решение
от компании «БИК-Информ»
и Bosch Системы Безопасности

Ex 1ExdIIBT6Gb класс взрывозащиты
ХЛ1** от -61°С



- Максимальная надежность работы в агрессивных средах 24/7.
- Высокая степень детализации изображения.
- Дистанционное управление объективом с помощью ПО Bosch Video Management System.
- Шифрованный канал связи.

**При создании камер использованы:**

- взрывобезопасный гермобокс ВСМ-400Ex с системой холодного старта от -61°С и питанием PoE++ мощностью 75 Вт (производство «БИК-Информ»);
- системы дистанционного управления объективом, антизапотевания и антиобледенения (патент «БИК-Информ»)
- IP камера Bosch с видеоаналитикой IVA (Bosch Системы безопасности)

БИК-ИНФОРМ
20 лет с вами
ISO 9001:2011

СИСТЕМЫ БЕЗОПАСНОСТИ, НАБЛЮДЕНИЯ
И АВТОМАТИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ

С-Петербург, ул. Бумажная, д. 9, корп. 1;
тел.: (812) 447-95-55

Москва, ул. Б. Почтовая, д.55/59, стр.1 офис 744;
тел.: (495) 645-23-92

WWW.BIC-INFORM.RU