ТЕХНОЛОГИЯ УПРАВЛЕНИЯ И МОНИТОРИНГА СИСТЕМАМИ БЕЗОПАСНОСТИ ОБЪЕКТОВ В МАСШТАБЕ ВЕДОМСТВ (КОРПОРАЦИЙ)

Основные направления деятельности Научно-производственного предприятия «ИСТА-СИСТЕМС» (ЗАО НПП «ИСТА-СИСТЕМС») – головной организации Группы компаний «ИСТА» – обследование, анализ уязвимости и категорирование особо ответственных объектов любых масштабов и форм собственности, проектирование, инсталляция, системная интеграция, комплектование, поставка оборудования и программных средств, сопровождение и сервисное обслуживание, а также разработка, производство и поставка специальных технических средств. Сегодня среди клиентов компании – минобороны РФ, Минтранс, Минэнерго, Росрезерв, ФСКН, Росатом, банки, в том числе и Банк России, Администрации муниципалитетов и другие весьма авторитетные организации, холдинги и просто солидные предприятия.

Работающим в «ИСТА-СИСТЕМС» специалистам не раз удавалось решить сложнейшие задачи по обеспечению безопасности секретных и особо важных объектов. Из недавних достижений – решение проблем информационного обмена между множеством автоматизированных систем, организационно и функционально включаемых в АПК «Безопасный город». Подробнее обо всём этом рассказали руководитель дирекции исследований и разработок ЗАО НПП «ИСТА-Системс» Геннадий Львович КУЗНЕЦОВ и заместитель генерального директора ООО «Итриум СПб» Дмитрий Владимирович КАЗАКОВ.

Геннадий Львович КУЗНЕЦОВ, руководитель дирекции исследований и разработок ЗАО НПП «ИСТА-Системс»

Дмитрий Владимирович КАЗАКОВ, заместитель генерального директора ООО «Итриум СПб»

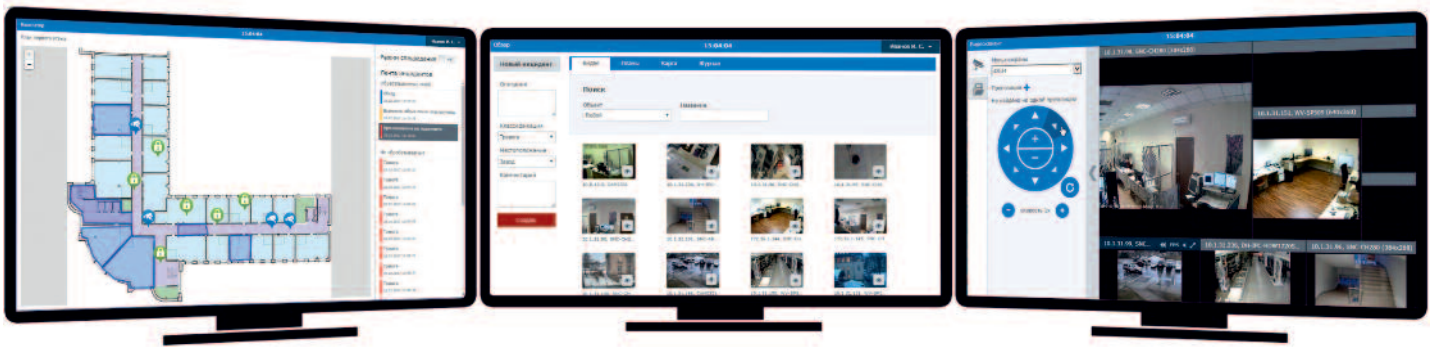
Актуальным вызовом настоящего времени в области обеспечения безопасности крупных вертикально-интегрированных компаний либо ведомств является создание инструментов для централизованного управления и мониторинга за состоянием объектовых систем безопасности. Первые пункты управления (либо мониторинговые или ситуационные центры) обеспечения безопасности, контролирующие распределённую сеть объектовых систем безопасности, появились не так давно, но уже однозначно доказали свою эффективность за счёт появления новых полезных возможностей. Во-первых, – это контроль работоспособности технических средств охраны, выполнения регламентов по их обслуживанию и ремонту оборудования. Во-вторых, – возможность анализировать действия дежурного персонала на объектах по обработке тревожных и аварийных событий. В-третьих, – это существенное сокращение времени на процедуры эскалации инцидента по серьёзным происшествиям, подготовка принятия решений, возможность анализа и прогнозирования развития ситуаций с учётом всей совокупности факторов (природных, техногенных, криминальных, террористических и пр.). Наконец, – это удобные площадки для проведения учений и подготовки персонала.

Однако для построения пунктов управления такого рода необходимо обеспечить доведение «сигналов» и потоков данных от объектовых систем безопасности, предоставить средства и возможность мониторинга широкого набора параметров. Но как это сделать, если системы безопасности различных объектов строились независимо друг от друга, оснащены системами от разных производителей, которые не «умеют» взаимодействовать между собой?

Исторически сложились три основных подхода к решению данной задачи. Первый – традиционный. Это интеграция через так называемые API (прикладные интерфейсы программирования) с созданием информационных шлюзов между множеством объектовых систем и системой, реализующей функциональные задачи автоматизации деятельности пунктов (центров управления). Второй подход – интеграция на основе специализированных продуктов – интеграционных шин, имеющих более или менее удобный инструментарий для разработки адаптеров взаимодействия с объектовыми информационными системами. Ну и третий вариант – монорешение. Когда все объектовые системы, инфраструктурные элементы и системы автоматизации детельности неразрывно связаны в рамках комплексного решения от одного производителя.

Все перечисленные варианты имеют серьёзные недостатки. Среди которых основные – это дороговизна интеграционных разработок и их короткий жизненный цикл, завышенная стоимость эксплуатации (владения) комплексных монорешений по причине возникающего монопольного положения разработчика, риски потери инвестиций в случае санкционных ограничений либо ухода производителя с рынка. Отдельным образом необходимо анализировать риски в части угроз кибербезопасности, возникающие при применении решений иностранных брендов.

Тем не менее, многие из перечисленных недостатков можно исключить за счёт нового подхода и технологических решений, предлагаемых ниже. Какой может быть альтернатива? Речь идёт о решениях, построенных на технологической базе стандартизации информационного взаимодействия в сфере безопасности на прикладном уровне, в основе которой лежит единый стек открытых протоколов (ЕСОП). Данный термин впервые был введён в 2014 году в документе «Временные единые требования к техническим параметрам АПК «Безопасный город», который задумывался как приложение к Концепции построения и развития АПК «Безопасный город». В этом документе были приведены детальные требования к реализации ЕСОП. В точном



соответствии с этими требованиями была создана реализация ЕСОП в рамках НИР МВД, шифр «Безопасный город» и передана в межведомственную комиссию АПК «Безопасный город» для свободного распространения.

Что же представляют собой поддержание технологии и решения на основе ЕСОП? Это сервис-ориентированная инфраструктура информационного взаимодействия между элементами распределённых объектовых систем безопасности (СБ), выступающими как системы-источники данных, и системами автоматизации деятельности пунктов либо центров управления безопасностью, которые потребляют данные от систем-источников. За счёт использования ЕСОП на прикладном уровне возникает единое информационное пространство – своеобразная информационная сеть для реализации функций управления и мониторинга систем безопасности объектов (ИСУМ СБО).

В состав ИСУМ СБО входят:

• ядро ИСУМ СБО – унифицированный инфраструктурный элемент информационной сети, реализующий информационное взаимодействие посредством ЕСОП, который также может быть внедрён независимо от других частей ИСУМ СБО;

• пользовательская прикладная система автоматизации деятельности центров (ППС АД) мониторинга и управления безопасностью, потребляющая информацию в виде сервисов ЕСОП;

• специализированные узлы сети для систем контроля и управления доступом, (КУД), охранной сигнализации (ОС), пожарной сигнализации (ПС) и противопожарной автоматики, систем с релейными выходами и т. д.;

• специализированный прикладной узел сети для интеллектуальных систем видеонаблюдения (ИСВН) и классических СВН;

• центр аутентификации.

Структура ИСУМ СБО приведена на рис. 1.

Специализированные узлы сети обеспечивают поддержку протокола со стороны систем-источников данных.

Для развёртывания и использования в качестве функционального ядра ИСУМ СБО компанией «Иста-Системс» разработан продукт серии «Истима. Сервисная платформа». В качестве специализированных узлов сети могут использоваться, в числе прочих, продукты компании «Итриум СПб» серий «ИГНИС», «БОРЕЙ», «ДЕВИЗОР», «ITRIUM», интегрированная система безопасности НЕЙРОСС, программные средства НЕЙРОСС Мониторинг и другие.

Внешний по отношению к ядру ИСУМ СБО Центр аутентификации позволяет более гибко внедрять элементы новой инфраструктуры безопасности, не нарушая функционирование старой.

В результате внедрения ИСУМ СОБ ожидается повышение эффективности инвестиций в проекты по обеспечению безопасности объектов за счёт создания более длительного жизненного цикла, снижения затрат на интеграционные разработки, ухода из-под монопольной зависимости от поставщиков, возможности выбора лучших производителей в каждом сегменте сети, возможности использования информации систем безопасности в смежных системах управления предприятиями.

ЗАО НПП «ИСТА-СИСТЕМС»
194100, г. Санкт-Петербург,
ул. Харченко, д. 5, лит. А
тел./факс: +7 (812) 960 0610
+7 (812) 960 0611
e-mail: info@ista.ru
www.ista.ru

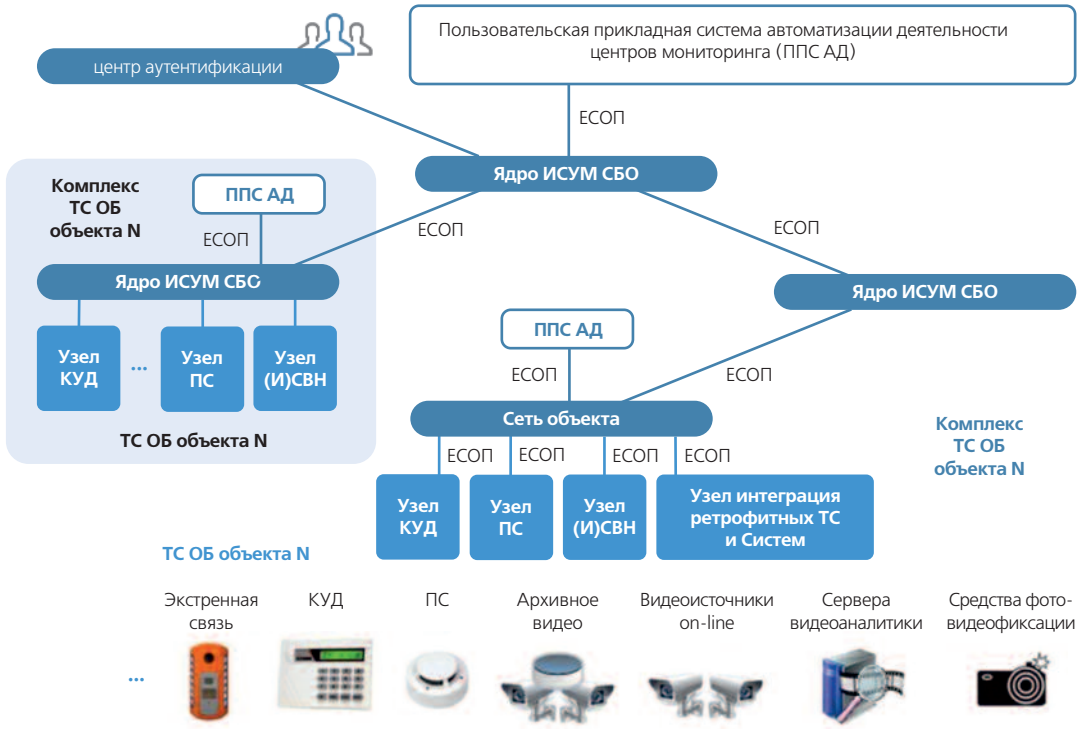


рис. 1. Структура ИСУМ СБО.