ССОИ — куда впадают потоки данных

В соответствии с постановлением правительства РФ № 969, системы сбора и обработки информации (ССОИ) входят в перечень оборудования, подлежащего обязательной сертификации. К настоящему моменту ФГУП «ЗащитаИнфоТранс» выдано 17 сертификатов на данную категорию систем. Мы попросили вендоров, заявивших о наличии сертификата, предоставить детальную информацию о своих решениях.

Текст: Дмитрий Воронин

Участие в обзоре приняли:

RUBEZH
КОНСОРЦИУМ ИНТЕГРА-С
insentry.
TRS Транссеть
axxonsoft MEMBER OF ITVGROUP
ISS
bcc
Stil SOFT
ЧИП ТЮН
Научно-техническая компания ИНФОРМ-АЛЬЯНС КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ
ИСТА
AMT GROUP
TwinPro project products

СИСТЕМЫ ФЕДЕРАЛЬНОГО И МЕСТНОГО ЗНАЧЕНИЯ

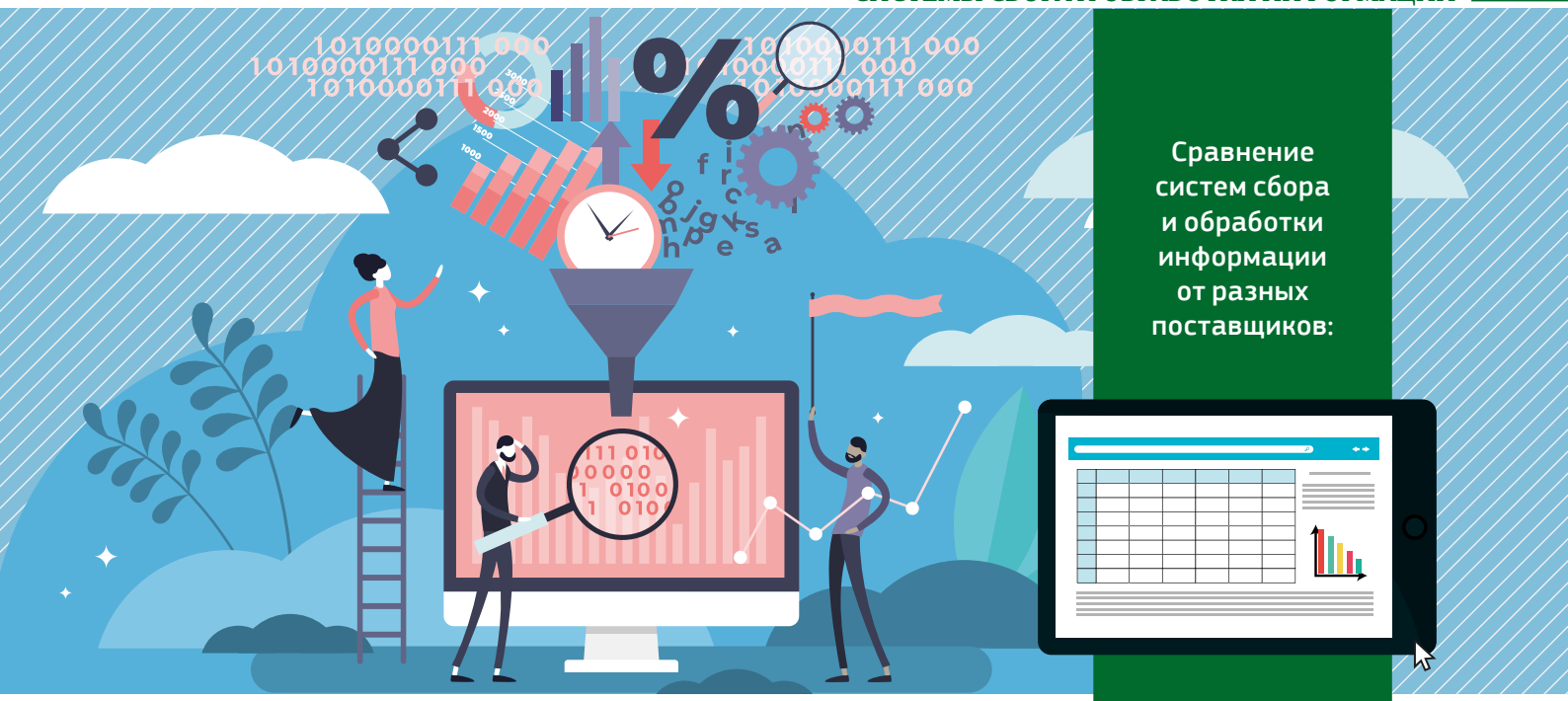
В 2011 году Комплексная программа безопасности населения на транспорте, утвержденная распоряжением правительства РФ, оговорила создание в масштабах страны системы сбора результатов технического мониторинга и контроля (ССТМК). Задача системы — аккумулировать информацию о состоянии всех объектов транспортной инфраструктуры (ОТИ) России для обеспечения эффективных управленческих решений на стороне уполномоченных органов.

Первичный сбор информации с объектов в данной доктрине доверен объектовым системам сбора и обработки информации — ССОИ. Требования к ним прописаны в известном постановлении № 969. Одно из главных при этом условий — сопряжение ССОИ с устройствами слежения, досмотра, контроля доступа и так далее, установленными на ОТИ. Главная задача ССОИ — предоставить оператору данные от технических средств обеспечения транспортной безопасности (ТСОТБ) в единой, универсальной форме. На основе такой информации оператор будет выстраивать свои действия и реагировать в случае возникновения инцидентов.

Поэтому конечная эффективность ССОИ на объектах транспортной инфраструктуры зависит от того, на-

Where data flows / By Dmitriy Voronin

In accordance with Decree of the Government of the Russian Federation No. 969, systems of information collection and processing are included in the list of equipment subject to mandatory certification. To date, FSUE «ZaschitaInfoTrans» has issued 17 certificates for this category of systems. We asked the vendors who announced the availability of the certificate to provide detailed information on their decisions.



Сравнение систем сбора и обработки информации от разных поставщиков:

сколько оптимально и полно реализована интеграция с периферийным оборудованием на объекте.

ИНТЕГРАЦИЯ

Перечень систем, которые должны быть интегрированы в ССОИ, — оговорен постановлением правительства № 969 (системы видеонаблюдения, СКУД, охранная сигнализация, интеллектуальное видеонаблюдение, досмотровая техника, системы аудиозаписи, средства оповещения, средства связи, приема и передачи информации). Участники обзора подтверждают, что их ССОИ интегрированы со всеми необходимыми системами.

Однако специалисты по сертификации рекомендуют запрашивать в каждом случае детальный перечень вендоров, чье оборудование было протестировано на совместимость с ССОИ. Многое зависит от протокола, по которому осуществляется интеграция. Важно наличие открытого протокола, который может самостоятельно взять сторонний разработчик — без помощи и согласования вендором ССОИ — и осуществить интеграцию своего оборудования с системой безопасности на объекте заказчика через API или SDK.

Многие поставщики отвечали на запрос по их ССОИ: да, есть свой протокол. Но насколько реализован доступ сторонних разработчиков к программным кодам – полной ясности нет. Как отмечают эксперты журнала, многие вендоры настаивают на заключении договора с ними как условии предоставления своего протокола для интеграции стороннего оборудования. Среди участников опроса, такую схему подключения — по HTTP-API с договором о неразглашении — обозначила, например, компания «Иста-Системс» (в то же время доступно подключение оборудования к системе через ONVIF).

ЭЛЕМЕНТЫ ИНТЕГРАЦИИ С ССОИ

К сожалению, не все разработчики ССОИ уделяют внимание в своих обзорах разделу пожарной безопасности — а это один из ключевых факторов безопасности объектов, в том числе транспортной инфраструктуры. Хоть автоматическая пожарная сигнализация (АПС) и не отражена в 969.

С другой стороны, некоторые вендоры уделили более широкое внимание вопросу интеграции — и организовали ее даже с непрофильными в рамках постановления 969 системами. В частности, об интеграции с системами автоматизации зданий (протокол BACnet) заявили разработчики решений «Интеллект» (AxxonSoft) и R-Platforma (ГК «Рубеж»). А о сопряженности с охранным освещением — разработчики системы «Бастион-2» от ГК «ТвинПро».

Во всех случаях на стороне заказчика будет не лишним каждый раз запрашивать у потенциального поставщика ССОИ детальный перечень устройств и брендов, с которыми интегрирована конкретная система сбора и обработки информации. Важно, чтобы вендор ССОИ предоставлял возможность выбора нескольких производителей интегрируемых подсистем, в первую очередь основных: СКУД, видеонаблюдения и охранной сигнализации.

ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

При условии правильной интеграции ССОИ превращает любой «зоопарк устройств» в комплексную систему, причем с функциями прогнозного мониторинга и сценарной аналитики. О поддержке принятия решений заявляют разработчики из ГК «Рубеж» — R-Platforma, Консорциума «Интегра-С» — платформа «Интегра Планета», и другие.

За что отвечает каждый из протоколов

TCP/IP — сетевая модель передачи данных, представленных в цифровом виде.
SNMP (Simple Network Management Protocol) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. Применяется в ССОИ для мониторинга систем объекта.
SOAP (Simple Object Access Protocol) — протокол обмена структурированными сообщениями в распределенной вычислительной среде.
UDP (User Datagram Protocol) — один из центральных сетевых протоколов для интернета.
RTMP (Real Time Messaging Protocol) — проприетарный протокол потоковой передачи данных для передачи потокового видео и аудио через интернет.
BACnet (Building Automation and Control network) — сетевой протокол, применяемый в системах автоматизации зданий и сетях управления. Применяется в ССОИ для интеграции с инженерными системами.
ONVIF (Open Network Video Interface Forum) — группа протоколов для интеграции ССОИ с системами видеонаблюдения и СКУД.
RTSP (Real Time Streaming Protocol) — протокол для удаленного управления потоком данных с сервера, предоставляет возможность выполнения команд «старт», «стоп» и т. д
OPC (Open Platform Communications) — семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами.
Modbus — открытый коммуникационный протокол. Широко применяется в промышленности для организации связи между электронными устройствами.
OSDP (Open Supervised Device Protocol) — открытый двунаправленный контролируемый протокол устройств, реализованный на базе RS485

Вендоры также заявляют функции, которые выполняются полностью автоматически без участия оператора. Система «EVA.TRANSPORT SECURITY» от АО «Транссеть» и немногочисленные другие способны приоретизировать поступающие сообщения и автоматизировать порядок реагирования в соответствии с утвержденными на ОТИ нормативно-правовыми документами. В системе SecurOS от ISS и некоторых других автоматизированый сбор данных с устройств видеоаудиомониторинга, мета-данных предназначен для передачи «карточки происшествия» в центр мониторинга, а также в сторонние системы служб экстренного реагирования. Если подтверждения не последует в течение заданного времени, выполнятся действия по умолчанию.

В отдельных системах — ПАК «АРМ ОД ОТИ» (НТК «Информ-Альянс») — предусмотрена автоматизация деятельности оперативного дежурного подразделения по выполнению утвержденных регламентов действий на основе мониторинга событий и расчетных сценариев действий нарушителей, а также осуществление контроля за действиями подразделений транспортной безопасности (ПТБ). Подсистема некоторых ССОИ, например «Синергет» («СТИЛСОФТ»), позволяет произвести произвольную настройку информирования и реакции операторов на возникающие в системе события, в том числе вызов групп реагирования, фиксацию действий оператора, отслеживание движения групп реагирования на картах, распределение нагрузки по реагированию между операторами.

Возможно также наличие шаблонов сценариев работы досмотровой зоны различных объектов.

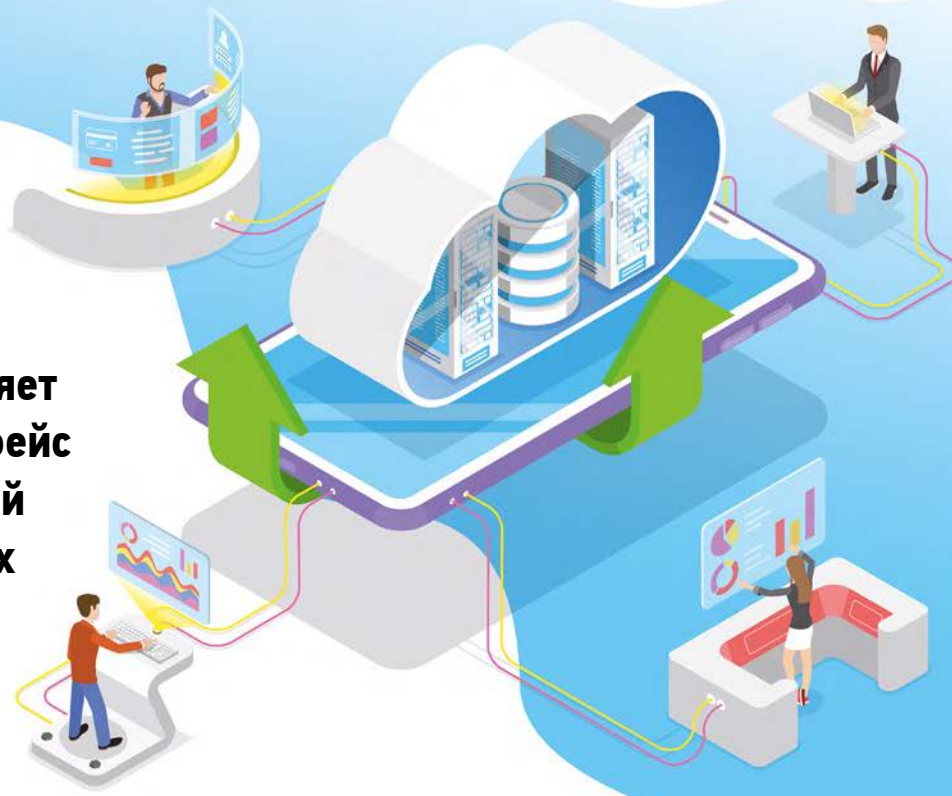
БЫСТРОДЕЙСТВИЕ

Еще один немаловажный фактор при выборе системы — ее быстродействие. Согласно постановлению 969, установлено номинальное быстродействие системы по предоставлению информации — не более 15 секунд в расчете на 1 сутки запрашиваемого диапазона времени. На практике отклик системы даже с такой незначительной задержкой может приводить к тому, что оператору работать будет некомфортно. Ведь информация будет постоянно «подлагивать».

При этом эффективность ССОИ в том числе определяет количество событий, которые система может обработать за единицу времени (для крупного международного аэропорта оно может достигать 2 млн в день). Количество одновременно обрабатываемых запросов на получение информации, согласно требованиям 969, не может быть менее 30. Однако и тут не понятно, что имеется в виду, какое количество пользователей и какое количество информации через себя они могут транслировать.

В совокупности факторов такой параметр, как признают сами поставщики ССОИ, позволяет поставлять не самые быстродейственные решения.

Приятно увидеть в данных участников обзора, что наиболее технологичные компании предпочитают измерять эти параметры по-своему. К примеру, разработчики ГК «ТвинПро» заявили о выработке собственных критериев быстродействия. А в AxxonSoft журналу RUБЕЖ пояснили: «Мы измеряем быстродействие для каждого типа процессоров путем тестирования на нужной конфигурации». Такой подход можно расценивать как позитивный признак — если компания может рассказать о том, как именно она измеряет быстродействие системы и даже разработала свою методику оценки, значит, она понимает продукт и задачи его эксплуатации.



Технология cloud-base в некоторых ССОИ позволяет использовать web-интерфейс для визуализации событий на мобильных платформах

ОБЛАЧНЫЕ СЕРВИСЫ

Программное обеспечение ССОИ является клиент-серверным. В одних случаях разработчики делают выбор в пользу «толстых» клиентов, которые отличаются довольно сложным процессом установки, настройки и обновления. Другие же выбирают более современные методы разработки с применением web-технологий, которые подразумевают использование в качестве клиента («тонкого») обычный web-браузер (так называемые cloud-based-решения). Они упрощают техническое обслуживание, обновление системы. А также сокращают время на подключение новых пользователей. Для постоянных обновлений безопасности, зашитых в программных кодах, все чаще разработчики используют готовые библиотеки, готовые наборы фреймворков. Облачное хранение системы обеспечивает полноту и оперативность таких обновлений. Если заказчик планирует использовать продукт в течение 5-7 лет, то надо понимать, что мир меняется все быстрее, и переход к облачным сервисам в принципе говорит о том, насколько поставщик решения шагает в ногу с индустрией.

Технология cloud-base в некоторых ССОИ позволяет использовать web-интерфейс для визуализации событий на мобильных платформах. Например, R-Platforma, разработанная на основе web-технологий, обеспечивает работу полнофункционального клиента (администратора, оператора) при наличии только web-браузера. В таких ССОИ заказчик может организовать доступ пользователей к системе через внутреннее (в инфраструктуре заказчика) облако.

В ряде ССОИ (например, у «Интеллект» от AxxonSoft) есть возможность создания web-сервера, к которому через браузеры могут подключаться web-клиенты (web-клиент поддерживает функции: воспроизведение живого и архивного видео; настройка раскладки камер на экране; постановка и снятие камер с охраны; управление детекторами; управление PTZ-устройствами).

Кстати, ожидаемые возражения со стороны служб безопасности относительно защищенности данных в облачных хранилищах тут находят очевидное решение — в виде применения частных облачных хранилищ. Кроме того, участники обзора ответили относительно средств обеспечения информационной безопасности.

УСЛОВИЯ И ЦЕНА КОНТРАКТА

Краеугольная тема для многих поставщиков — что должно входить в договор поставки, только оборудование или еще и его монтаж, пусконаладка и даже техническое обслуживание. В сегменте систем ССОИ большинство вендоров предлагают схему «поставка системы отдельно, ее обслуживание отдельно».

Проектированием, монтажом и пусконаладкой занимаются либо заказчики систем (проектные, инсталляционные и сервисные компании), либо сами конечные заказчики (собственники объектов ОТИ). Обслуживанием системы клиента в таких случаях будут заниматься инсталляторы или интеграторы.

Частый аргумент вендоров в пользу дробления контрактов — согласно требованиям постановления правительства 969, продаются только сертифицированные программно-аппаратные комплексы (ПАКи). По другим направлениям может продаваться отдельно ПО. У некоторых поставщиков ССОИ (пример — ССОИ «Бастион-2»

Требования к ССОИ по постановлению правительства 969

XI. Требования к функциональным свойствам технических систем сбора и обработки информации

58. К техническим системам сбора и обработки информации предъявляются следующие требования:

а) выполнение запросов на сбор, обработку и получение информации в соответствии с полномочиями, задаваемыми в процессе администрирования прав пользователей, инициировавших запросы;

б) срок хранения собранной информации — не менее 30 суток;

в) скорость получения информации — не более 15 секунд в расчете на 1 сутки запрашиваемого диапазона времени;

г) скорость получения информации — не более 60 секунд в расчете на 30 суток запрашиваемого диапазона времени;

д) количество одновременно обрабатываемых запросов на получение информации — не менее 30.

59. Технические системы сбора и обработки информации должны обеспечить:

а) взаимодействие с системой сбора результатов технического мониторинга и контроля при получении и передаче информации в указанную систему по локальной сети Ethernet с использованием стека протоколов семейства TCP/IP;

б) обмен информацией с системой сбора результатов технического мониторинга и контроля с использованием унифицированных протокола передачи данных и формата метаданных, разработанного на основе XML.

от ГК «ТвинПро») техподдержка первого уровня входит в стоимость договора поставки.

Вопрос цены без обсуждения контракта вендоры трактуют своеобразно. Так, на запрос журнала о стоимости ССОИ большинство предпочитало давать уклончивый ответ, сравнивая свои решения со стоимостью аналогов.

В целом, согласно данным участников обзора, в зависимости от количества оборудования и величины размеров объекта стоимость бюджетной ССОИ составит 350 000–750 000 рублей. Инсайдеры журнала также обратили внимание на ряд реализованных проектов, где предположительная цена ССОИ может достигать 12 млн рублей.

РАБОТА С ВОЗРАЖЕНИЯМИ

Главный драйвер спроса на ССОИ понятен — это выполнение требований постановления правительства 969, взаимодействие и обмен информацией с ТСОТБ по протоколу, утвержденному департаментом программ развития Минтранса России 18 мая 2017 года («Протокол взаимодействия технических средств (ТС) обеспечения транспортной безопасности (ОТБ) с системой сбора результатов технического мониторинга и контроля объектов транспортной инфраструктуры»).

Но в целом, судя по данным проведенного редакцией журнала обзора, практика продаж ССОИ на объекты довольно специфична.

Из однозначно понимаемых заказчиками выгод внедрения ССОИ вендоры называют сокращение затрат на персонал, повышение эффективности системы принятия решений, удобство ведения отчетности, снижение расходов и затрат на эксплуатацию и стоимость владения оборудованием и программным обеспечением систем безопасности, полный контроль над распределенными объектами. Заказчиков интересуют также контроль ситуации в реальном времени и реагирование на тревоги, расследование происшествий, повышение достоверности информации за счет многофакторности оценки событий, минимизация затрат на оснащение объекта, снижение негативного влияния человеческого фактора, рисков, связанных с нелояльностью персонала, сговором и, наконец, экономия фонда оплаты труда (за счет учета рабочего времени).

Характерно, что при довольно размытой системе спроса и ценообразования поставщики ССОИ практически не встречают принципиальных возражений со стороны заказчиков. «Были замечания по функционалу (скорее не замечания, а пожелания на расширение функционала), которые были оперативно устранены» — так, в общем, комментируют вендоры в обзоре (*см. полную версию по qr-коду*) свой опыт переговоров о поставке ССОИ на объекты ОТИ. Даже цена оказывается не принципиальным фактором, все решает функционал системы, который в общем наборе ТСОТБ на объекте редко превышает 5% всего бюджета проекта.

Чтобы заказчик не переплачивал, вендоры, например «Транссеть», предоставляют услугу бесплатного экспресс-анализа предприятия. Такой шаг позволяет продолжить разговор даже на тех объектах, где поставщиков ССОИ встретили фразой «Вы опоздали. В этом году все оснастили».

Наконец, «золотым аргументом» служит предложение по бесплатному тестированию и опытной эксплуатации ССОИ на объекте — в данном обзоре его предлагают, например, компании «СТИЛСОФТ» и «Чиптюн». Период такого тестирования может составлять от 1 до 3 и более месяцев. А ГК «ТвинПро» по запросу заказчика готова предоставить полнофункциональную демоверсию системы, единственным ограничением которой является необходимость перезапуска клиентов каждые два часа.