

# КСБ: ОТ ИНТЕГРАЦИИ «ЖЕЛЕЗА» К ИНТЕГРАЦИИ СЕРВИСОВ

*Рыбаков Михаил Иванович  
компания «Итриум»*

**Р**азвитие информационных технологий, их гибкость, подстройка под интересы потребителя, коммуникационные возможности и разнообразные сервисы – все это каждый видит вокруг себя, в том числе ежедневно используя персональные гаджеты. Поэтому неудивительны ожидания подобной гибкости и от современных комплексных систем безопасности (КСБ), желания обнаружить готовность систем адаптироваться «под меня», под мои бизнес-процессы, «просто» добавлять новые сервисы, приложения и т. д. и т. п.

Позитивный пример адекватного ответа на запросы потребителей – кардинальные изменения в области видеонаблюдения, в том числе как важнейшей подсистемы любой КСБ. И дело не только в том, что современное видеонаблюдение в кратчайшие сроки стало реальным дальновидением, что кардинально изменились качество, разрешающая способность, спектральные диапазоны и средства представления видеoinформации. Все чаще ожидания потребителей адресованы не к самим устройствам (видеокамерам, видеорегистраторам...), а к такой нематериальной сущности как «сервисы»: наблюдения, записи, интеллектуального анализа и т. д. и т. п. Не останавливаясь на технологических аспектах, скажем, что современное видеонаблюдение почти не требует интеграции, по крайней мере, она стала гораздо проще и технологичней.

Система видеонаблюдения – лишь одна, хотя и из наиболее важных систем физической безопасности, жизнеобеспечения и КСБ. Как обстоят дела с другими системами – охранной сигнализации, управления доступом, пожарной сигнализации, взаимодействия с системами автоматизации и жизнеобеспечения объектов? А дела обстоят по-прежнему, т. е. не очень. «Не очень» потому, что изначально все эти системы не предназначены для объединения или совместной работы друг с другом и иными системами. Приходится предпринимать какие-то нестандартные действия, чтобы все-таки эти системы объединить, получить от них то, что нужно и дополнительные бону-

сы от объединения. И это мы называем интеграцией.

Истории комплексных систем безопасности в России уже больше 20 лет. Все эти годы продолжают разговоры и дискуссии про интеграцию, а тема не стала менее острой. Если раньше заказчики по умолчанию считали, что с помощью программного обеспечения можно «интегрировать» все и всегда, то сегодня многие понимают, что не все и не очень.

## ИНТЕГРАЦИЯ «ЖЕЛЕЗА»

### Технологическая платформа

В основе подавляющего большинства систем охранной сигнализации, контроля и управления доступом, пожарной безопасности, применяемых в проектах, уровень техники 20-летней давности. Это могут быть так называемые «коробочные» или «готовые» КСБ или «типа открытые системы», дороже или дешевле, но это – старые технологии. В сравнении с информационными технологиями, эти системы как бы остановились в развитии. Вероятно, влияет «охранный» и ведомственный генезис технических средств безопасности и жизнеобеспечения, который распространился и на комплексные системы. В исторической ретроспективе вопрос о том, чем и как охранять и защищать, определял не потребитель, а ограничительные перечни, РД и ГОСТ, которые конституировали status quo. И в довершении типичный вопрос: «А где это стоит?», в котором выражается желание минимизировать потенциальные проблемы на фоне непонимания, что могут дать новые решения.

Экономические интересы бизнеса также влияют на динамику развития. Если в новых видеотехнологиях были заинтересованы крупнейшие мировые компании, то ведущие российские и не только российские производители средств сигнализации и СКУД, занявшие рынок в конце 90-х и в нулевые, были и ныне заинтересованы в максимально долгом продолжении массового производства однажды разработанных систем.

Основные ограничения:

- Слабые вычислительные ресурсы и позавчерашние коммуникационные

**КОМПЛЕКСНЫЕ  
СИСТЕМЫ**

## ■ КОМПЛЕКСНЫЕ СИСТЕМЫ

возможности. Вы не можете изменить или обновить программное обеспечение, добавить функции, новые алгоритмы работы, настроить взаимодействие с другими системами. Система работает только с теми устройствами, которые входят в ее состав. Вы не можете получить от нее любую информацию, только определенную производителем в соответствии с жесткими алгоритмами.

- **Закрытость.** Метод достижения монополии у крупных производителей – делать КСБ полностью на собственном «железе» и собственном программном обеспечении. Они предоставляют компьютерные интерфейсы с ограниченной функциональностью либо не дают их вовсе.
- **Несовместимость.** В основе – ментальность «доинтернетной» эпохи, отсутствие стандартов и опять-таки герметическая бизнес-мотивация.

А потребителю оставляют выбор: использовать «готовую КСБ» как есть или заниматься интеграцией.

### Интеграционное программное обеспечение

В апологию интеграции «открытых систем» часто приводят два тезиса.

- «Производители специализированных систем всегда делают их лучше, чем компании, предлагающие «все в одном флаконе».
- «Интеграция предоставляет потребителю новые возможности, и в результате «возникает синергия».

Однако, интеграционное программное обеспечение отражает все проблемы традиционных средств безопасности и аккумулирует в себе все недочеты интегрируемых средств, привнося и собственные. Интеграционные интерфейсы систем отличаются от их внутренних функциональных коммуникационных интерфейсов и разрабатываются по остаточному принципу. Стандартная практика – на фоне ошибок в API изменения «открытых интерфейсов» при обновлении функциональности. Протоколы и API разных производителей отличаются форматами, структурами данных, семантикой, могут конфликтовать друг с другом на ресурсах одной операционной системы. И т. д. и т. п. Как следствие, надежность комплексов снижается в соответствии с масштабами программной интеграции, а интеграционное ПО становится наиболее уязвимым звеном КСБ.

Поддержание необходимой надежности означает для разработчика интеграционного ПО многократное увеличение затрат на тестирование, затрат на обеспечение компетенции в области обслуживания множества производителей, постоянные издержки на поддержку и сопровождение чужого оборудования и сис-

тем. Проблемная экономика – вот оборотная сторона традиционной интеграции. В общем случае за интеграцию не платят, а по умолчанию она должна быть.

В итоге, на рынке лишь единицы продуктов являются действительно интеграционными платформами. Списки 100500 интегрированных средств и систем на сайтах многих российских компаний, в большей степени, – пропаганда и рекламные материалы. Программная интеграция – это не бизнес, а скорее искусство для отдельных компаний-энтузиастов. Бизнес нацелен на развитие, а программная интеграция занимается преодолением проблем, заложенных десятилетия назад. И не проблем интеграционного программного обеспечения, а системных проблем традиционной технологической платформы КСБ.

### ТОВАРЫ И СЕРВИСЫ

В индустрии информационных технологий, являющейся драйвером развития постиндустриального информационного общества, доминирует модель предоставления сервисов. Отрасль физической безопасности наглядно демонстрирует ментальность промышленной революции, в которой экономика – это производство и распространение товаров. Здесь под товарами понимаются технические и программные средства КСБ. Сервисы – это информация, а также программные инструменты контроля и управления, предоставляемые системой службам безопасности, руководству и собственникам объектов и организаций.

Для предоставления сервисов, так или иначе, требуются технические средства, но в постиндустриальном обществе акцент переносится на то, что эти средства дают пользователю. Один современный сетевой контроллер/гаджет может предоставить множество информационных услуг, в то время как товарная номенклатура традиционной КСБ может составлять десятки различных функциональных модулей при весьма скромном информационном предложении.

Материальная иллюстрация «товарной идеологии» современных КСБ – это сотни аппаратных модулей, многие километры нестандартных коммуникаций, т. е. морально устаревшие уникальные технические инфраструктуры, заложниками которых заказчики становятся на многие годы.

Все сказанное выше можно было бы рассматривать просто как предмет для дискуссии или критики, если бы сервисные решения уже не вторгались на когда-то герметичный рынок систем безопасности. Облачные видеосервисы не требуют от заказчика никаких дополнительных технических средств и никакой интеграции. Нужно только установить камеру и «подключиться к облаку», что-

бы получать весь спектр услуг, которые предоставляет традиционная видеоподсистема КСБ. Для некоторых видов систем безопасности, например, для пультовой охраны, явление провайдеров «видеонаблюдения как сервис» – уже прямая угроза бизнесу. А Интернет вещей – прямой путь «в облачные сервисы» охранной и пожарной сигнализации...

### СЕРВИСНАЯ ПЛАТФОРМА КСБ

Англоязычный термин «сервис=услуга» оказался мостиком между миром программистов и пользователей. В информационных технологиях (IT) сервис имеет две нотации. Это информационно-телекоммуникационная услуга, которую компания предоставляет своим клиентам, и процесс предоставления пользователям информационных ресурсов для обеспечения выполнения ими своих бизнес-функций.

Современная КСБ – это информационно-управляющая система. Ее ценность, в первую очередь, в том какие сервисы она дает пользователям, руководству объектов, собственникам бизнеса, а также иным потребителям, например, ответственным ведомствам.

### А где у вас сервисы?

Такой вопрос уже может озвучиваться сотрудником IT-службы, которому нужно встроить информацию КСБ в бизнес-процессы компании. И услышав: «...Ну, есть API...» – в лучшем случае, он посмотрит на вас с интересом натуралиста-энтомолога. Для него очевидно, что информационные системы должны предоставлять сервисы, которые понятно как применить.

А что PSIM? PSIM предоставляет пользовательские сервисы операторам и руководству службы безопасности. Безусловно, современные разработчики могут встроить в нее и «правильные сервисы», которые поймут IT-специалист и сторонняя информационная система. Но кто или что предоставит сервисы самой PSIM? Традиционные подсистемы КСБ не смогут. Здравствуй интеграция!?

И тот же IT-специалист без вопросов воспользуется сервисами, которые предоставляет система видеонаблюдения. Поэтому что ONVIF!

### Единый стандарт подключения для всех систем безопасности

Это декларация целей ONVIF. Тот, кто интересовался вопросами совместности/интероперабельности, неоднократно слышал подобное в последние десятилетия. Но сегодня эта фраза имеет вполне практическое значение, независимо от того, как далеко зашел и зайдет ONVIF в разработке профилей для контроля и управления доступом, для охранной и тревожной сигнализации. Обе организа-

ции, разрабатывающие «стандарты» интероперабельности, ONVIF и PSIA, однозначно определили технологию, в рамках которой разрабатываются спецификации, это веб-сервисы. Здесь для нас не важно, что существует два подхода к созданию веб-сервисов, а ONVIF и PSIA выбрали разные. Фактически, и бизнес (ONVIF), и «законодатели» (PSIA) констатировали, что современные средства и системы безопасности должны взаимодействовать/подключаться/обмениваться информацией, используя веб-технологии. Инструменты, используемые ONVIF и PSIA, – надстройка поверх HTTP, основного протокола Интернета. Уже одно это выводит возможности интеграции КСБ на современный уровень.

- Для IT-служб – это стандартный интерфейс интеграции в корпоративные системы.
- Для PSIM систем – многократное упрощение интеграции, возможность сосредоточиться на информационном менеджменте и пользовательских приложениях.
- Для устройств и систем – их способность взаимодействовать друг с другом, возможность обновлять программное обеспечение и добавлять сервисы.

В части ONVIF, по мере реализации новых спецификаций, интеграционная нагрузка будет снижаться, но стек протоколов и инструментов – «законодательная база совместимости» – уже определен. Потенциальные расхождения между инициативными разработками и будущими спецификациями фактически лежат только в области семантики. Хорошая новость в том, что как это должно работать и уже работает, наглядно показывают современные IP-видеосистемы. И не только видеосистемы.

В традиционных системах безопасности под платформой понималось какое-то программное обеспечение. Сервисная платформа КСБ – это набор стандартных спецификаций, правил, протоколов на базе веб-технологий, которым должны соответствовать интерфейсы технических и программных средств.

### СЕРВИСНАЯ ПЛАТФОРМА КСБ И ИНТЕРНЕТ ВЕЩЕЙ

Что такое спецификации ONVIF, PSIA в широком контексте? Это что-то специфическое, отраслевое, или тренд в развитии информационных технологий?

ONVIF занимается разработкой стандартизованных протоколов для вза-

имодействия различного оборудования и программных средств, входящих в состав систем безопасности. Также как и PSIA. В общем, это то, что сегодня называется Интернет вещей (IoT – Internet-of-Things), но есть особенности.

Несмотря на весь шум вокруг этого технологического тренда, единое определение IoT отсутствует. Общий смысл состоит в том, что это сеть устройств (компьютеров, датчиков, исполнительных устройств, контроллеров, приборов и т. д. и т. п.), связывающихся между собой, в том числе, и с использованием интернет-протокола IP.

Сегодня IoT – огромное количество решений, устройств и систем множества производителей. И главная проблема, с которой он закономерно столкнулся, – абсолютная несовместимость протоколов, устройств и программных средств.

Очевидным оказалось решение абстрагироваться от коммуникационных вопросов и использовать только готовые и проверенные веб-протоколы и инструменты поверх HTTP. Что собственно и сделали ONVIF и PSIA.

Неформально, сегодня это направление IoT называют Веб вещей (WoT – Web-of-Things).



Сделано в России



# ПАРИТЕТ

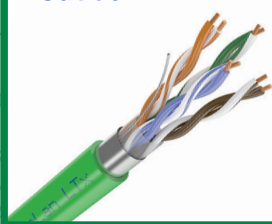
эталон кабеля

U/UTP F/UTP SF/UTP S/FTP

## ParLan™ - лучший LAN кабель

- ✓ высокое качество
- ✓ соответствие ФЗ и ГОСТ РФ
- ✓ сертификат ТРТС
- ✓ декларация Мин Связи
- ✓ кабель под Ваш проект

«Cat 5e»



«Cat 6»



«Cat 6A»



«Cat 7»



- ✓ исполнение нг(A)-HF
- ✓ низкотоксичные LTx
- ✓ огнестойкие FR 180 минут
- ✓ бронированные
- ✓ экстремальные условия эксплуатации