




ТОЧКА ОПОРЫ

Система виброконтроля

-  мониторинг
-  защита
-  диагностика

с. 16



Технология
synectica®



36 ЛЕТ НА РЫНКЕ ПРУЖИННЫХ ИЗДЕЛИЙ
с.2

РЫНОК ФОТОВИДЕОФИКСАЦИИ В РОССИИ: ОТ ЛОКАЛЬНЫХ РАЗРАБОТОК К ИНТЕЛЛЕКТУАЛЬНЫМ ТРАНСПОРТНЫМ СИСТЕМАМ
с.6

РАДИОСТАНЦИИ РАДИАЛА
с.24

16+



ПРОЕКТНО-ИНЖИНИРИНГОВАЯ ФАБРИКА КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ (КСБ) ПОЛНОГО ЦИКЛА

Основным направлением АО «НПП «ИСТА-Системс», основанного в 1988 году, является разработка и установка систем безопасности, а также разработки в области высоких технологий. Со дня своего основания компания не использовала государственные ресурсы и государственные каналы сбыта. Фактор самостоятельности в значительной степени способствовал успехам предприятия. Сегодня компания позиционирует себя как проектно-инжиниринговая фабрика полного цикла. О комплексных системах безопасности, разрабатываемых на предприятии, рассказывают представители руководства компании: директор по развитию АО «НПП «ИСТА-Системс» Геннадий Львович КУЗНЕЦОВ и заместитель генерального директора по науке АО «НПП «ИСТА-Системс» Вячеслав Викторович СОКОЛОВ.

Потребности современного заказчика комплексных систем безопасности (КСБ) значительно меняются. Ещё вчера обычной практикой был проектный подход. Его суть проста: КСБ – одна из слабых систем. Так же, как и другие инженерные системы, она проектируется, комплектуется, производится монтаж и общая сдача вместе с объектом. Качество оценивается на соответствие СП, ГОСТ, РД и иным ведомственным и отраслевым документам на момент сдачи.

Сегодня крупные заказчики рассматривают КСБ как самостоятельный высокотехнологичный продукт длинного жизненного цикла. В состав требований включаются: устойчивость производителя, серийность производства, соответствие его современным стандартам качества и информационной безопасности. КСБ должны иметь гарантии сервиса, модернизации, технической поддержки, а также быть включён в информационную модель предприятия.

Современный заказчик видит КСБ не как набор датчиков, полевых шин, контроллеров, а как устойчивую к физическим и информационным атакам кибер-физическую систему со стандартизированными протоколами, наборами данных, развиваемой функциональностью, искусственным интеллектом с возможностью локального обучения.

Изменяется и бизнес-модель. От отдельных статей «капитальные вложения», «эксплуатационные расходы» – к «сервисной модели», при которой производитель КСБ становится постоянным партнёром на весь жизненный цикл системы.

КСБ – это больше не забор с камерами, а инструмент управления рисками, важнейшая составляющая устойчивости бизнеса современного предприятия.

В ответ на новые запросы рынка наша компания – АО «НПП «ИСТА-Системс» – предлагает себя заказчикам как проектно-инжиниринговую фабрику полного цикла, поддерживающую самые современные требования и подходы к производству и эксплуатации КСБ.

Как же работает наша фабрика? Она состоит из функциональных участков (цехов). Первыми вступают в производственные отношения с заказчиком наши аналитики, которые готовы выполнять следующий комплекс работ:

- предварительное категорирование;
- анализ уязвимости от АНВ;
- разработку паспортов (планов) обеспечения безопасности, в том числе для строящихся объектов.

Для предприятий, имеющих площадки разной ведомственной принадлежности, актуальны вопросы рационального районирования (например, между площадкой ТЭК и отгрузочным морским терминалом).

АО «НПП «ИСТА-Системс» поддерживает предоставление всех перечисленных консалтинговых услуг для предприятий ТЭК, транспорта, промышленности, объектов использования атомной энергии, медицины, спорта, гостиниц и др.

Аналитические работы довольно часто заканчиваются разработкой ТЗ на проектирование КСБ. В эту часть консалтинга входит правильный подбор действующих нормативных документов, полный и точный учёт требований к КСБ в зависимости от результатов категорирования, особенностей моделей угроз, актуальных требований бизнес-процессов и взаимодействия с внешними системами. К специалистам-аналитикам на этом этапе подключаются Главные инженеры проектов (ГИПы).

Данными компетенциями обладают и другие компании-интеграторы. Однако в этой статье мы хотели бы акцентировать внимание на технологических аспектах создания КСБ. В этом смысле цифровая платформа «НЕЙРОСС» (ИТРИУМ) является нашей главной технологической линией.

«НЕЙРОСС» – это программный продукт и набор базовых элементов инфраструктуры для развертывания КСБ: серверов, рабочих мест, контроллеров, видеоинформационных консолей, средств контроля работоспособности, PSIM, отчётности и пр. Платформа «НЕЙРОСС» кросс-плат-

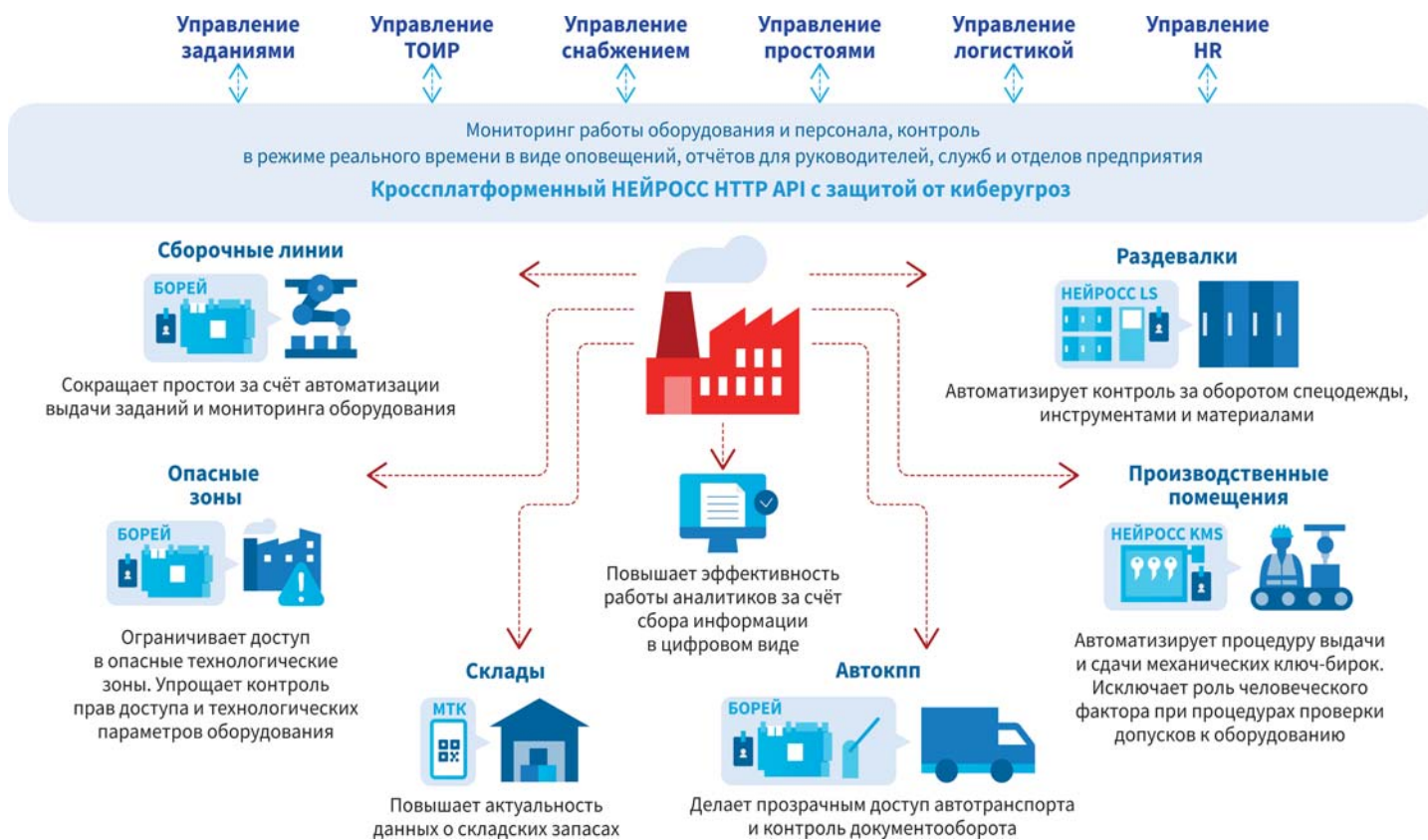


Рис.1 Пример взаимодействия КСБ предприятия со смежными системами и службами.

форменна. Может работать как на отечественных сертифицированных ОС: Astra Linux, ALT Linux, так и на Windows или, скажем, Linux Debian. Универсальные контроллеры СОС/СКУД, программные средства для видеонаблюдения и видеоменеджмента, бюро пропусков, управляющие консоли, АРМы мониторинга безопасности и ситуационного реагирования работают под управлением одного и того же программного продукта, обеспечивая бесшовную среду управления КСБ.

Для взаимодействия с внешними системами используются специальные средства:

- ПАК Интеграция – для взаимодействия с широким набором приборов и контроллеров внешних производителей по проприетарным и промышленным протоколам (Орион, Рубеж, Болид, Parsec, OPC-клиенты/серверы и мн. др.);
- стандартизированные программные интерфейсы (НЕЙРОСС HTTP API, профайлы ONVIF, Modbus);

Для развития базовой функциональности применяются средства встраивания плагинов и пользовательских сценариев на LUA-скриптах.

Широкий набор инструментов, их гибкость позволяют нашей «фабрике» реализовать многие частности в пожеланиях заказчиков КСБ, обеспечить сопровождение и развитие функциональности систем безопасности в течение всего их жизненного цикла.

Для разработки прикладных программных и аппаратных решений, проектного оборудования, различных встраиваний и интеграций, обучения пользователей и технической поддержки служит ключевой цех нашей «фабрики ИСТА», наша **Дирекция исследований и разработок (ДИР)**. Здесь также разрабатываются и обучаются нейронные сети для различных видеодетекторов, новых интерфейсов для взаимодействия с КСБ, отрабатываются проектные и конструкторские технические решения, вырабатываются оптимальные параметры и конфигурации сетей КСБ и многое другое.

Проектно-конструкторский центр

– это самое большое подразделение нашей компании: современные средства автоматизации общего и проектного документооборота, разработка 3D моделей и инженерных данных, наличие всех необходимых компетенций для разработки и оформления проектной и конструкторской документации в области комплексных систем безопасности, включая разделы по защите от БПЛА.

Сборочный цех нашей фабрики ИСТА

– это центр, где производится изготовление и сборка проектного оборудования, узлов высокой заводской готовности, изделий собственного производства и комплектация всей поставки заказчиком с решением задач по логистике. Производятся маркировка, наладка, заводские и комплексные заводские испытания (FAT/IFAT). Так реализуется одно из важнейших современных требований заказчиков к поставке оборудования для КСБ.

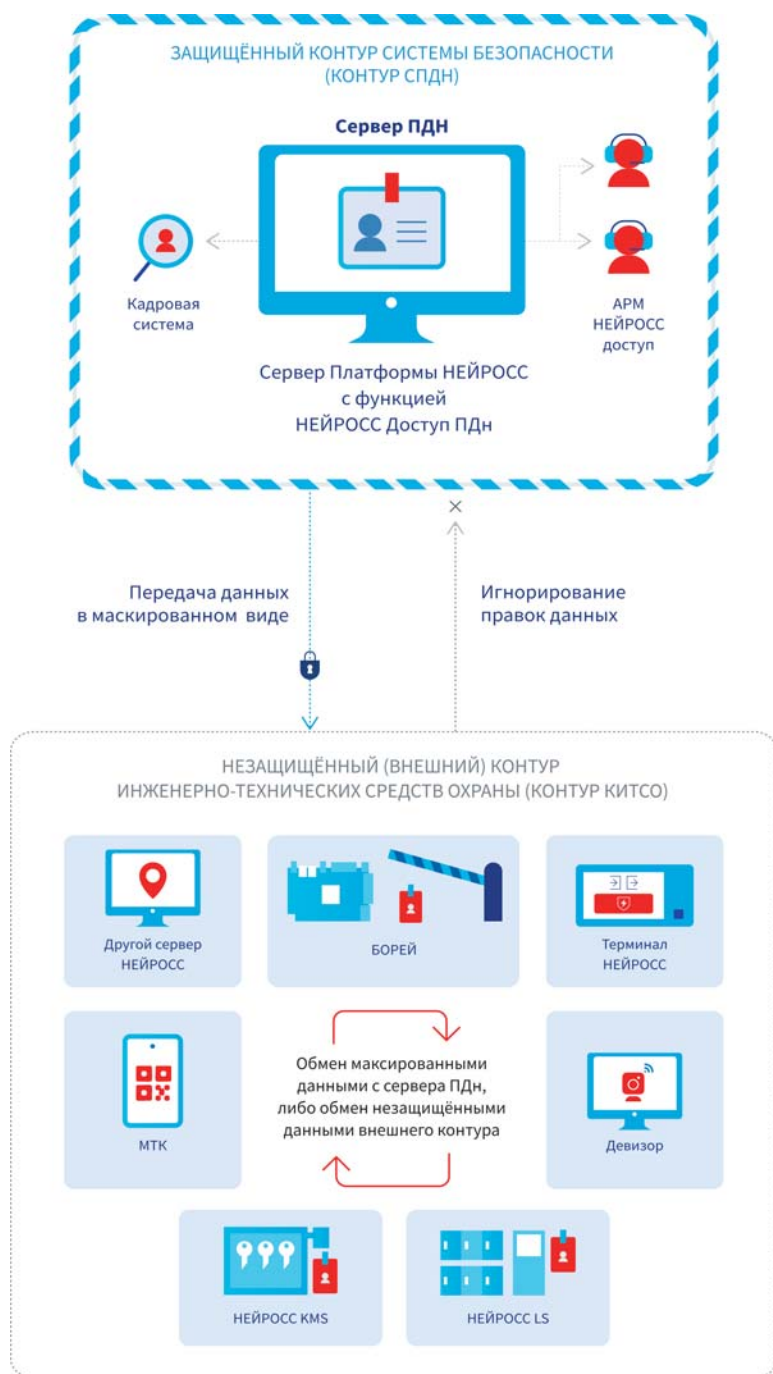


Рис. 2 Выделение минимально возможного сегмента обработки ПД в КСБ.

Участок Информационной безопасности.

Требования к ИБ в последнее время значительно ужесточились. Регулятор активно взялся за наведение порядка в части защиты персональных данных (ПД), в т.ч. циркулирующих в Бюро пропусков КСБ. Заказчики осмыслили, насколько опасны могут быть последствия потери контроля над СОС/СКУД видеосистемой для антитеррористической устойчивости предприятия и его

экономической безопасности. Произошедшие теракты высветили новые актуальные аспекты ИБ:

а) Базовые аппаратные платформы компьютерного и коммуникационного оборудования в массе своей импортные. Быть уверенным в том, что в них не таится угроза информационной безопасности, к сожалению, не приходится. В этих условиях АНВ полностью исключить практически невозможно, но можно добиться киберустойчивости автомати-

зированной системы КСБ, т.е. такого состояния, при котором даже если АНВ произошло, то функциональность быстро восстановлена, а отрицательные последствия атаки минимальны.

б) Киберустойчивость АС КСБ не должна зависеть от киберустойчивости других АС предприятия.

Участок ИБ нашей фабрики ИСТА освоил выпуск КСБ с минимально возможным периметром циркуляции ПД (пример – Рис. 2), а также с поддержкой всех требований законодательства к защите ПД и обеспечением сбалансированного уровня киберустойчивости КСБ с помощью проектных и конструкторских решений.

Добавим к описанию нашей фабрики наличие сертификатов ГОСТ Р ИСО 9001-2015, ГОСТ Р ИСО/МЭК 27001-2021, наличие лицензии ФСБ на работу с гостайной.

Директор по развитию
АО «НПП «ИСТА-Системс»
Геннадий Львович КУЗНЕЦОВ

Заместитель генерального
директора по науке
АО «НПП «ИСТА-Системс»
Вячеслав Викторович СОКОЛОВ



194100, г. Санкт-Петербург,
ул. Харченко, д. 5, литер А
тел. +7 (812) 960 0610
факс +7 (812) 960 0611
e-mail: info@ista.ru
www.ista.ru

