PSIM — игра по правилам и без

Бизнес-революцию готовят разработчики программных платформ управления информацией о состоянии физической защиты объектов. Аббревиатура PSIM уже стала новым технологическим трендом рынка. Журнал RUБЕЖ первым из отраслевых изданий провел анализ этого продуктового сегмента, выявив ключевые приоритеты его поставщиков, интеграторов, заказчиков.

Текст: Дмитрий Воронин, Станислав Тарасов, Фарид Волков

Рецензенты:

Михаил Рыбаков, генеральный директор, ООО «Итриум СПБ»

Михаил Онищенко, генеральный директор, ALPHAOPEN

Андрей Скворцов, директор по развитию, ООО ПСЦ «Электроника»

Вадим Сосенко, директор департамента технической экспертизы и поддержки продаж, Группа «Астерос»

Сергей Раевский, руководитель направления, RVi Integrator

PSIM — НОВОЕ ИМЯ ДЛЯ ПРЕЖНИХ ЗАДАЧ

PSIM (Physical Security Information Management) — технология, которая в реальном времени обеспечивает анализ событий (тревог) безопасности, исходящих от сетевых устройств, с возможностью реагирования на них в рамках заданных регламентов.

Как коммерческое решение технология дебютировала в сегменте информационной безопасности. С 2005 года получила маркетинговое название SIEM (Security Information and Event Management), которое состоит из двух терминов: SIM (Security Information Management — управление информацией (от системы) безопасности) и SEM (Security Event Management — управление событиями безопасности). По мере интеграции рынков — safety|security и ИТ — технология была спроецирована на системы физической безопасности во всем их многообразии и получила название Physical Security Information Management (PSIM).

О родственных связях между технологиями красноречиво свидетельствует их одинаковый функционал, который состоит из шести ключевых опций: сбор, анализ, визуализация данных, поддержка бизнес-процессов, формирование отчетов и ведение контрольного журнала.

PSIM — ЕДИН В ДВУХ ВЕРСИЯХ

Как трактуют PSIM за рубежом

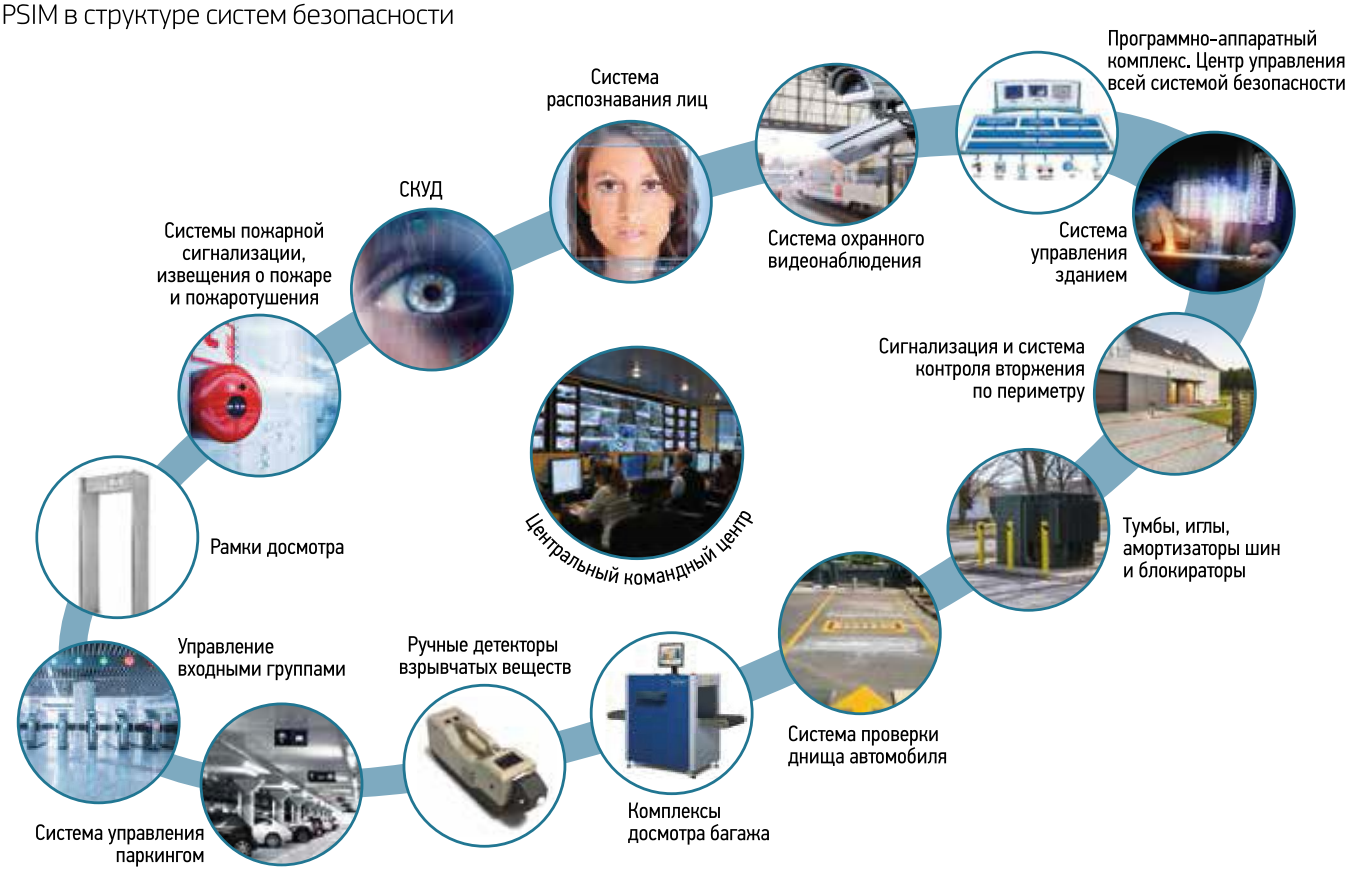
Международный партнер журнала RUБЕЖ — глобальный проект по безопасности a&s Magazine — опросил в своих обзорах компании, которые играют заметную роль на зарубежных рынках, описывает довольно масштабный охват компетенций в связи с позиционированием PSIM.

PSIM в мировой практике — это программная платформа, которая собирает и обрабатывает информацию из разрозненных устройств обеспечения безопасности и информационных систем, после чего складывает ее в одну общую картину (событие). Истинное решение PSIM дает пользователям возможность интегрировать уже существующие системы, чтобы в будущем без ограничений использовать лучшие в своем классе технологии. Важно,

PSIM: Fair Play and Dirty Pool. Supremal Software Platforms for Complex Security Systems. Russian Market Analytical Review / By Dmirty Voronin, Stanislav Tarasov, Farid Volkov

Security software platforms developers are ready to start a business-revolution. PSIM abbreviation has already become a new technological trend on the security market. A&s RUBEZH Russia Magazine carried out an analysis of this product segment and defined the key priorities of suppliers, system integrators and customers.

PSIM в структуре систем безопасности



что основное преимущество системы PSIM — в трактовке международных вендоров — заключается в возможности ее интеграции с существующими и планируемыми системами без привязки к конкретному поставщику.

В отличие от традиционных интегрированных систем безопасности PSIM предлагает еще одно важное отличие — интеллектуальное решение. Сбор и обработка информации из различных источников предполагает, что оповещения формируются только при возникновении тех событий, которые важны. «Истинная система PSIM имеет способность идентифицировать возникающие события и эффективно управлять ими для снижения возможного риска», — считает Джейми Уилсон, менеджер по маркетингу в регионе EMEA в компании NICE Systems.

Другим важным отличием PSIM является способность обеспечить активное управление событиями для повышения операционной эффективности. Благодаря использованию адаптивных рабочих процессов оператор знает, что происходит, где это происходит и что должно быть сделано.

«PSIM может обеспечить гораздо больше, чем просто физическую безопасность, — уверен Майкл Месарос, менеджер по продукции в Proximex, одного из брендов Tyco Security Products. — У нас есть проекты, где просят интегрировать все виды систем, которые использует клиент, — лифты, системы управления зданием, багажные транспортеры и даже системы экологического контроля на телескопических трапах в аэропорту».

Помимо прочего, PSIM позволяет осуществлять централизованное управление, не будучи привязанным к определенному месту. «Благодаря способности PSIM отображать одну и ту же информацию на разных языках мы можем объединить штаб-квартиру компании в Европе с объектом в Африке, — пояснил Хагай Кац, вице-президент по развитию бизнеса в Magal Systems. — Эта связь позволяет штаб-квартире компании быстро решить вопросы и убедиться, что первоначальная реакция была правильной. Компания может расширить выгоду, которую получают от PSIM системы безопасности, в этом смысле PSIM также способствует управлению рисками компании».

Кооперация данных, собранных от систем безопасности в сочетании с другими системами, позволяет

Функциональные задачи, которые решает PSIM

- Контроль и оперативное выявление рисков и угроз
- Мониторинг и контроль состояния технических средств, электроснабжения, инженерных систем, программного и технического обеспечения и телекоммуникационных сетей
- Учет эксплуатационных ресурсов оборудования
- Планирование использования оборудования, прогнозирование выхода оборудования из строя, оптимизация работ по сервисному обслуживанию
- Эффективное использование человеческих ресурсов и координация их взаимодействия

Поколение Next

Как развивают опыт эксплуатации PSIM-систем в других странах

По материалам компании Qognify (разработчик PSIM-систем, офисы компании расположены в США, Сингапуре, Израиле, Индии)

PSIM — преодоление перегруженности данными информационной безопасности. Четкое представление о текущей ситуации.

Физическая безопасность (PSIM) рассматривается в качестве слоя, который находится поверх всех прочих систем безопасности и датчиков. Его задача — организовывать, анализировать и управлять всей информацией, которую они производят. Вместо того чтобы управлять десятками, а может быть, и сотнями систем, PSIM объединяет все в единое централизованное представление.

Управление информацией о физической безопасности и ситуационное управление. Заказчик должен знать, что делать.

Каждая система и датчик на объекте отправляют обновления статуса, уведомления и предупреждения. Как вы все это понимаете? И что еще более важно, как работают ваши операторы безопасности? PSIM дает общую картину, а также все важные детали для ваших операций безопасности.

Осведомленность о ситуации

Программное обеспечение для управления информацией о физической безопасности дает представление обо всех данных, поступающих в диспетчерскую. PSIM не просто повышает осознание того, что происходит, но делает это раньше оператора. Система подскажет, какие службы отправить, куда, в каком количестве, даже проверит, есть ли у сил реагирования подходящее оборудование.

Накопление опыта реагирования

PSIM также обеспечивает согласованность с тем, как система, управляемая людьми, обрабатывает инциденты. Используя записи, отчеты и анализ, необходимые для улучшения, PSIM дает операторам рекомендации относительно того, как обрабатывать события, и автоматизирует некоторые из задействованных задач.

Обработка BigData

Мониторинг, измерение и анализ массовых объемов данных в Центре оперативной разведки дает представление и позволяет подготовиться к событиям заранее, тем самым сводя к минимуму влияние рисков на деятельность организации. Настраиваемые и агрегированные панели мониторинга обеспечивают визуализацию наиболее важных бизнес-сервисов и ключевых показателей эффективности. Система обнаруживает отклонения в ведущих индикаторах, которые часто являются прекурсорами потенциальных инцидентов.

PSIMplus

Исходные данные, доступные из программного обеспечения PSIM — видеопотоки, карты ГИС, аналитика, системные и сенсорные данные и многое другое, — могут быть чрезвычайно полезны для подразделений всего предприятия.

Следующий уровень систем после PSIM — так называемые системы управления ситуациями PSIMplus. В то время как управление информацией физической безопасности (PSIM) информирует о том, что происходит, управление ситуациями расширяет ценность этих знаний за пределами области безопасности. Благодаря этому собственник объектов может интегрировать системы безопасности для управления рядом других функций помимо безопасности. Например, для улучшения рабочих областей с более быстрым обслуживанием и оптимизацией затрат — за счет ликвидации «белых пятен» и операционных пробелов, вызванных информационной перегрузкой.

Проактивная система управления инцидентами

В Центре оперативного интеллекта есть усовершенствованный механизм правил, который улучшает механизм корреляции факторов текущей ситуации.

Центр оперативного интеллекта включает в себя:

- непрерывный мониторинг и измерение ведущих ключевых показателей эффективности и обслуживания;
- текущий статус снимков объектов и подразделений организации и прогноз инцидентов в режиме реального времени;
- анализ причинно-следственных связей, включая анализ тенденций и шаблонов (регламентов). Центр предложит владельцу идеи улучшений, направленных на снижение инцидентов в будущем;
- настраиваемые потоки данных в зависимости от уровня доступа. Это позволяет сотрудникам организации — от руководителей до персонала на местах — наилучшим образом выполнять свои обязанности.

Расчет рентабельности инвестиций

Сбои бизнеса являются дорогостоящими. Настолько, что в некоторых случаях их стоимость рассчитывается на минуту. Благодаря способности учиться на прошлом опыте с помощью анализа тенденций и шаблонов Центр оперативного интеллекта может предоставить информацию, которая позволяет рассчитать убытки от конкретных инцидентов и экономический эффект от их недопущения.

превратить решение PSIM в платформу для комплексного управления объектом. Это означает, что PSIM может использоваться не только для обеспечения безопасности. Зарубежные игроки PSIM-рынка уже делают клиентам предложения, в которых next generation решений позволяет осуществлять более целостный подход к управлению организацией, сочетая обеспечение безопасности и управление.

Следующим за PSIM этапом зарубежные поставщики уже предлагают формат платформ CSIM (Converged Security Information Management). В частности, компания Videosys, предлагает программное обеспечение, в котором CSIM использует правила фильтрации на основе времени, местоположения, продолжительности, частоты и типа. CSIM оптимально работает для широко распределенных активов, поскольку использует мобильное приложение — инструмент повышения осведомленности о ситуации со стороны акционеров, линейных руководителей, сотрудников ИТ-подразделений.

Наконец, футурологи отрасли предсказывают развитие парадигмы информационной системы управления объектом (FMS — Facility Management System), с «наборным» функционалом (как аппаратным, так и программным) от разных поставщиков по текущим потребностям объекта. Причем, прийти к требуемой функциональности такая информационная система может по разным «траекториям» как за счет «добора» функционала, к той же VMS, так и к уже существующей FMS или любой другой «системе управления» (например, АСУ ТП). «Эра FMS» предположительно наступит на пике проникновения интернета вещей в data-процессы, благодаря удешевлению самих датчиков (и росту их количества на объектах) и за счет дальнейшего развития и повышения стойкости информационных систем к отказам.

PSIM в России. Новый сегмент или «перестановка слагаемых»?

В России судьба PSIM пока складывается неоднозначно. Решения класса PSIM в 2017 году были представлены на крупнейших российских специализированных выставках, но фурора не произвели. Что вполне объяснимо. В отличие от зарубежных коллег российские поставщики PSIM-решений начинают путь самоопределения на фоне еще не остывшего тренда: комплексных систем безопасности (КСБ) и интегрированных систем безопасности (ИСБ). Их в России на рынке систем безопасности активно продвигали все без исключения крупные вендоры оборудования на протяжении последних лет.

Решения класса PSIM в 2017 году были представлены на крупнейших российских специализированных выставках, но фурора не произвели

До недавнего времени широкая аппаратная интеграция сохраняла ИСБ и КСБ в статусе венца технологического развития. Лишь в последние два-три года усиление софтверного компонента (программная поддержка более мощных процессоров, постепенная замена аналоговых каналов связи цифровыми) привело к появлению все более широких возможностей сопряжения разных систем на базе единых программных платформ. Так стала актуальной тема «программного ядра», надстройки над ИСБ и КСБ, а вместе с ней и над инженерными системами — то есть тема PSIM.

В результате к моменту написания этого материала единого мнения у российских разработчиков PSIM о месте этого продукта в системе решений по безопасности не сложилось.

При всем разнообразии трактовок игроки рынка признают: PSIM, как и любая ИСБ, — это именно элемент системы безопасности, который объединяет ее программным ядром, своеобразный функциональный хаб.

Обобщив высказывания специалистов, можно составить следующий перечень отличий, которыми те наделяют PSIM-решения и КСБ (табл. 1).

Таблица 1. Отличия PSIM-решений и КСБ

	PSIM	КСБ
1	Программный комплекс «верхнего уровня», кроссплатформенность, возможность использования операционной системы с открытым кодом как обязательное условие.	ПО не всегда имеет клиент-серверную архитектуру, бывают ограничения по используемой операционной системе
2	Возможно использование системы управления базами данных (СУБД) сторонних производителей: SQL, Oracle, Firebird	Часто используется только одна база данных, без альтернативных вариантов
3	Неограниченная распределенная модульная мультисерверная система с возможностью организации кластерных связок, сегментация базы данных	Как правило, существует ограничение по количеству серверов, клиентов. Отсутствует или имеет ограничения централизованное управление несколькими локальными системами безопасности (разные объекты, в т. ч. территориально)
4	Работа основных функциональных блоков ПО PSIM как служб, не как приложений (за исключением клиентской части), с возможностью размещения на разных хостах	Часто серверная составляющая ПО размещена строго на одной машине, в том числе как приложение
5	Возможность интеграции со SCADA, ERP, HR-системами	Интеграция возможна не всегда, отработанные решения такой интеграции редки, исключением можно считать разве что интеграцию с 1С

	PSIM	КСБ
6	Наличие реализованных (со стороны поставщика PSIM) «пакетов интеграции» с производителями аппаратной части и софта подсистем (СКУД, СТН, СОТС, САПС и т.д.)	Есть нюансы. Если КСБ построена на базе одной из подсистем (СКУД или видеонаблюдения), то пакеты интеграции есть только на смежные подсистемы (к примеру, если базовая система — СКУД, то доступны пакеты интеграции на другие подсистемы, кроме СКУД) Если КСБ предлагается как комплекс подсистем от одного вендора (например, изначально есть СКУД, видеонаблюдение и охранная система), то пакеты интеграции будут представлены пожарными системами, видеодомофонами и, возможно, SCADA. Команда, экспортируемая в подсистему, обязательно должна вписываться в логику ее работы, но не должна встречать субъективных противоречий разработчика подсистемы, например некоторые производители СКУД не позволяют менять «уровень доступа» владельца карты командами «извне» (в рамках предоставляемого ими SDK)
7	Наличие собственных аппаратных решений, разработанных поставщиком самой PSIM-системы, допустимо, но не является обязательным	«Железо» и софт строго — от одного вендора. Из преимуществ — решение «под ключ» от одного производителя, 100%-ная совместимость, при возникновении сложностей всего одна точка входа
8	Использование оператором PSIM клиентских приложений производителя подсистем недопустимо. Мониторинг и управление ведется в рамках единого информационного поля и единого интерфейса. Функционал подсистем должен быть доступен в PSIM в полном объеме, причем элементы управления подсистемой, интуитивность и информативность должны быть не хуже, чем в ПО производителя подсистемы	Если КСБ сделана, например, на базе видеонаблюдения, то в нее можно интегрировать СКУД. Однако настройку системы СКУД придется выполнить в ПО этой подсистемы и только потом можно перенести точки доступа на планы КСБ и видеть там события. Или наоборот — КСБ сделана на базе СКУД, соответственно, на планах камеры есть, но вот шаблонов (мультиплексированное отображение нескольких камер) с видеокамерами нет, можно только посмотреть картинку живого видео с конкретной камеры или поднять архив с нее по какому-либо событию СКУД. И если с первым примером (КСБ на видеоподсистеме) еще можно смириться, то второй неприемлем
9	Использование только жестких шаблонов недопустимо. Система использует гибкое конфигурирование «событийных связок», так называемую систему управления инцидентами, где входящее событие со стороны подсистем может вызвать практически любую настраиваемую индивидуально реакцию системы управления инцидентами	Крайне субъективный подход по определению алгоритма действий оператора в той или иной ситуации (особенно последовательность действий) либо отсутствует, либо ограничен. Реакция на события в автоматическом режиме возможна, но сам набор этих реакций ограничен. Большие сложности вызывают комбинированные реакции, где часть действий выполняется автоматически, а часть — оператором в ручном режиме. При этом все «ручные» действия оператора должны быть запротоколированы отдельно для составления отчета в дальнейшем
10	Гибкая конфигурация приоритетов и уровней доступа операторов к системе. Возможно изменение графического интерфейса для каждого оператора	Часто использованы укрупненные уровни доступа к системе. Оператор может только выдавать карты СКУД или не выдавать. Тонкая настройка недоступна, для каждой функции нужен свой отдельный ответственный. Например, право создавать зоны доступа для выдаваемых карт будет недоступно выдающему, по разграничению прав потребуется, например, начальник службы безопасности. Другой пример — оператор может просматривать только запись с камер или только живое видео, смешанные типы просмотров с определенных камер ему будут недоступны
11	К недостаткам текущих PSIM-систем можно отнести следующие: • не рассчитаны на применение на небольших предприятиях с малым количеством устройств, тем более на тех, где отсутствует оперативная диспетчерская; • универсальность, многообразие поддерживаемого оборудования, круг решаемых задач таковы, что делают продукты этого класса сложными и трудоемкими в реализации	К недостаткам текущих «интеграционных платформ», применяемых с КСБ, можно отнести следующие: • интеграция с другими системами сводится лишь к информационному обмену на уровне событие-реакция; • отсутствует общая логика управления процессом; • отсутствует поддержка ГИС

НЕТ ГОСТов — НЕТ РЫНКА

С лингвистической точки зрения «X-SIM» формат продуктов — всего лишь системы, которые призваны помочь со структурированием, упорядочением, фильтрацией, обобщением и вычленением (полезной) информации из потока данных от разнообразных датчиков и программно-аппаратных сис-тем «умных» объектов. То есть все это только системы «управления информацией».

Положить конец спорам и «перетягиваниям одеяла» при определении места PSIM в рынке систем безопасности сможет регулирование. Даже в мировой практике для PSIM до сих пор не существует отраслевых стандартов. В России они разработаны только для ИСБ и КСБ. В связи с этим у отраслевых ассоциаций есть прекрасная возможность освоить никем не занятое пространство, создав на нем новый технический комитет и линейку ГОСТов и регламентов.

Это тем более актуально, что по мере стандартизации и регулирования PSIM-решения будут прямым спутником укрупнения бизнесов в отрасли физической

PSIM — взгляд разработчиков

ITV | AxxonSoft

PSIM — это система управления физическими средствами охраны, которая позволяет строить сложнейшие событийно-реактивные связи между разными системами безопасности, а также между системами безопасности и пользовательскими интерфейсами. Исходя из этого определения **Андрей Христофоров**, директор по продажам ITV|AxxonSoft, относит непосредственно к PSIM продукт «Интеллект» (многофункциональную открытую программную платформу, предназначенную для создания комплексных систем безопасности любого масштаба).

«В технологическом плане любая VMS, интегрированная хоть с чем-нибудь, хоть с каким-нибудь техническим средством безопасности, является КСБ. Возьмем крайность. VMS, которая интегрирована с IP-камерой, — уже теоретически КСБ. Подчеркиваю, теоретически. Но любая система, которая интегрирует в себя большое количество технических средств, еще не PSIM. Комплексная система безопасности, на мой взгляд, это клиент-серверная система, которая позволяет создать некий комплекс средств безопасности, а PSIM думает о пользователе, — считает Христофоров. — Комплексные системы безопасности (КСБ) и интегрированные системы безопасности (ИСБ) — это возможность нескольких систем работать совместно. PSIM же решает другие задачи, прежде всего принятия решений. Поэтому PSIM — это гораздо больше, чем КСБ».

По словам Андрея Христофорова, во-первых, PSIM — это система, вобравшая большое количество интеграций с различными системами безопасности, а во-вторых, дающая пользователю событийно-реактивный ряд. Это система, позволяющая выстроить взаимосвязь между событиями различных систем безопасности. Возможность построить невероятные, неочевидные связи, необходимые в конкретном данном проекте.

ALPHAOPEN

Генеральный директор ALPHAOPEN **Михаил Онищенко** уверен, что в России нет большой необходимости широко использовать термин «PSIM». Заменой ему служит термин «Комплексная система безопасности». В большинстве случаев ПО в него уже входит. Оба термина подразумевают интеграцию обширного круга систем, «увенчанную» программным продуктом верхнего уровня.

«Термин «PSIM» появился за рубежом не так давно, — говорит Онищенко. — На том рынке есть разделение на «логическую безопасность» и «физическую безопасность». Термин «безопасность» там разделился, когда уязвимость электронных систем стала проблемой, и вокруг этого начал формироваться бизнес. Под «логической безопасностью» понимают атаки через системы связи, провода, по Wi-Fi и т. д. Они преследуют цель похищения данных. И с «логической безопасностью» связывали защиту от внедрения в Сеть. Для средств, обеспечивающих безопасность на физическом уровне, соответственно принят термин «физическая безопасность». То есть защита от грабежей, нападений, иных несанкционированных проникновений. Это что касается слов physical security в аббревиатуре».

В жизни, считает директор ALPHAOPEN, происходит так: «Если заказчик попросит КСБ с аналитикой данных, мы друг друга поймем. Никого такой запрос не удивит и никто не скажет, что термин „КСБ“ употреблен неправильно».

Вторая часть термина «PSIM», «information management», подразумевает, что производится сбор информации, ее аналитика, предоставляется определенный доступ к системе для проведения расследования, построения отчетов, аудита действий операторов и т. д. Это подчеркивает, что в PSIM уделяется серьезное внимание именно программной части, сбору и обработке данных.

«Система может быть интегрированная, но ПО в ней может не быть. Термин „ИСБ“ тут подойдет, PSIM — нет. В PSIM ПО — важная часть системы», — считает Михаил Онищенко.

Еще одной особенностью решений класса PSIM, по мнению гендиректора ALPHAOPEN, может являться немонобрендовость решения. «Разработчики ПО для создания решений класса PSIM, как правило, не ангажированы производителями какой-либо одной системы: СКУД, видео, охранной или пожарной сигнализации и т. д. Неангажированность позволяет заниматься интеграцией всех брендов рынка», — сформулировал Онищенко одно из достоинств «истинной» PSIM.

ГК «Сигма»

Комментируя разницу между PSIM и КСБ, главный конструктор ГК «Сигма» **Сергей Левин** уточнил: «PSIM — это прежде всего софт, то есть программная интегрирующая платформа для объединения на верхнем уровне всех физических ресурсов системы безопасности. А ИСБ/КСБ — это программно-аппаратный комплекс, куда входят как ПО, так и оборудование систем безопасности: аппаратура сбора и обработки информации, средства обнаружения, исполнительные устройства и т. д. Если говорить про определение КТСО (комплекс технических средств охраны), то он еще дополняется как минимум средствами ограждения: заборы, калитки и т. д. По крайней мере у наших военных так».

Для каких объектов можно использовать PSIM

Проблемы клиентов

Потребности клиентов, которые решает PSIM

безопасности. Производители оборудования заинтересованы в создании своей ИСБ по схеме «железо + софт», которая дает особое конкурентное преимущество. Оно дорогое, технологичное, под него нужно иметь определенную структуру, чтобы этим продуктом пользоваться. У PSIM и без того высокий порог вхождения в рынок, из-за стоимости обладания ИСБ не все участники рынка пройдут в этот сегмент. Стандарты сыграют роль фильтра «высшей очистки» среди крупных производителей PSIM — и наведут порядок на рынке этих решений.

«Белые пятна» PSIM в России — какие факторы тормозят развитие сегмента

1. Потенциальные заказчики слабо осведомлены, какой функционал системы несут в себе PSIM-продукты и что они в итоге могут дать для бизнес-процессов.
2. Отсутствуют типовые (общепринятые) формулировки относительно структуры построения системы, нет упорядоченного перечня предлагаемых для интеграции модулей.
3. Отсутствует обобщенное (в идеале — в виде реестра) описание существующих платформ и их функциональных возможностей.
4. Уникальность (разобщенность, отсутствие топологии) каждого проекта ставит заказчиков в финансовую зависимость от конкретного разработчика системы при ее эксплуатации и обслуживании.
5. В предлагаемых PSIM-продуктах отсутствует разделение на решения для бизнеса и решения для государственного сектора.
6. Отсутствует наработанный пул кейсов с обобщенной экспертизой интеграций PSIM и линеек КСБ, с разбивкой на практики внутри России и за рубежом.
7. Проблема «длинных инвестиций» — протяженные (от года!) сроки реализации, при неочевидности результата на старте, но с условием масштабных вложений в разработку, инсталляцию и обслуживание системы.
8. Не регламентированы алгоритмы взаимодействия всех внутренних систем PSIM.

СПРОС И ПРЕДЛОЖЕНИЕ — В ПОИСКАХ ДРУГ ДРУГА

Заказчикам предстоит сыграть не последнюю роль в развитии рынка PSIM. В коммерческом сегменте они должны увидеть четкий экономический эффект от внед-рения дорогостоящих систем. Тем более что для открытых рынков эксперты предсказывают строго определенные ниши, в которых PSIM-решения будет востребованы. Первая ниша — технологическая, где есть объекты определенного типа, которые уже развились настолько, что функционал PSIM требуется сам по себе, без него предприятие не сможет работать эффективно. Второй класс объектов связан с развитием конкурентной способности и развитием бизнес-структуры. Это не технические ограничения, а требования конкуренции к получению прибыли, исходящие от руководства и собственников компании. Там этот продукт уже востребован как коммерческий, т. е. необходимость не потому, что иначе объект не будет работать, а необходимость

Прогнозы инвестиционных аналитиков

Наиболее заметные оценки и прогнозы по рынку PSIM с 2012 года публикуют аналитические агентства IHS Inc. и Frost&Sullivan. Оба агентства сошлись в том, что PSIM-системы будут наиболее востребованы в сегментах критической инфраструктуры (в первую очередь), быстрого реагирования, коммерческих и военных приложений. При этом чем больше позитивного опыта использования таких систем будет у конечных пользователей, тем быстрее будет расти рынок.

Правда, аналитики IHS Inc. указали на серьезный сдерживающий фактор для роста продаж PSIM: развитие конкурирующих продуктов, успешно внедряемых на объектах среднего уровня, на рынке, который исторически был вне досягаемости для высокого класса программных платформ PSIM в связи с их ценником.

коммерческая, где цель заказчика или заработать денег, или сэкономить за счет внедрения PSIM. Объектов второй группы будет существенно меньше.

Другой сегмент потенциальных заказчиков PSIM — государственный, он имеет иную специфику принятия решений. Именно здесь решающим фактором будет конкретное формализованное (в виде стандартов и регламентов) обоснование для рассмотрения затрат на покупку PSIM как возможной статьи расходов.

Производителям при этом предстоит очень серьезно поработать над аргументацией.

Традиционно (и это признают сами компании) рынок систем безопасности «нависает» над заказчиками, исходя не из оценки их потребностей, а насаждая то, что смог разработать и произвести вендор. Поэтому продажи PSIM — особенно на коммерческом рынке — будут во многом зависеть от способности поставщиков развернуть собственное сознание от abc-анализа конкурентов в сторону клиентоориентированного подхода.

PSIM-РЕВОЛЮЦИЯ НАЗНАЧЕНА НА ЗАВТРА. СВЕТАЕТ...

Споры вокруг терминов и определений PSIM, по большому счету, не имеют влияния на развитие самого направления. Специалисты по бизнес-процессам утверждают, что PSIM — революция не только в безопасности, но и в управлении объектами и территориями. Инсталляторы комплексных систем полагают, что новая аббревиатура — очередное англоязычное заимствование, поскольку решения этого класса в России давно разработаны и применяются. Правы и те и другие — PSIM найдет свое место на рынке независимо от определений. Аналитики (например, из Frost&Sullivan) прогнозируют в краткосрочной пятилетней перспективе взрывной рост рынка PSIM.

Опрошенные в ходе подготовки материала эксперты единодушны: развитие PSIM в России пойдет по своему пути. И не приведет — на первом этапе точно — к появлению отдельных мультивендорных решений, так как крупных независимых разработчиков систем такого уровня на рынке до сих пор нет. Созданием собственных платформ займутся производители оборудования. Таким образом, они могут использовать выпуск брендированных PSIM, чтобы защитить свои коммерческие интересы за счет привязки интеграции оборудования и платформы к определенным протоколам (схожие примеры уже известны — в сегменте радиоканальных систем пожарного мониторинга).

Пожалуй, главная интрига на 2018 год — кто из компаний, вкладывая средства в разработку собственной PSIM (а таких несколько, с принципиально разными подходами), угадает тренд и окажется технологическим лидером к моменту появления общих отраслевых стандартов на PSIM и к моменту, когда заказчики и интеграторы пройдут фазу ранних новаторов и сформулируют свои ожидания от нового поколения систем управления физической защитой.

Чего хотят заказчики PSIM

Дружелюбный интерфейс, доступный для простого охранника

Михаил Румянцев
начальник отделения технических средств, управление защиты ресурсов, ОАО «Славнефть-Ярославнефтеоргсинтез»

У нас крупный распределенный объект — Ярославский НПЗ. Общий периметр — 14 км. Завод имеет 8 КПП, железнодорожные въезды и т. д.

В качестве программного обеспечения мы используем Security Wizard от ПСЦ «Электроника», система была инсталлирована около 12 лет назад и модернизировалась по мере необходимости. Сначала система использовалась для отображения состояния технических средств охраны: тревоги, готовности и т. д. Также туда включалась система контроля и управления доступом как людей, так и автомобилей.

Новое решение «Электроники» — ESM-система (входит в класс PSIM) — это Security Wizard, плюс там появляются такие функции, которых в нашей системе нет: например контроль несения службы персоналом. То есть персонал в системе является интерактивным элементом, допустимо принятие решений на разных уровнях.

На большинстве объектов сейчас любой инцидент передается начальнику караула независимо от важности инцидента. В ESM инциденты могут регулироваться на разных уровнях. То есть могут принимать решения охранники, а начальника караула только информируют об этом. Наиболее важные инциденты могут сразу передаваться начальнику караула или его помощнику, т. е. более квалифицированному, нежели охранник, лицу.

Заказчику это дает полную информацию о безопасности на объекте. Мы можем сказать, что через такой-то участок забора в данный момент никто не пытается перелезть. В случае более простой системы я должен был позвонить на тот участок, тому охраннику и спросить: «У тебя там все хорошо?»

Кроме того, в новых системах появилась возможность вводить уровни опасности. Один и тот же датчик в зависимости от уровня опасности может изменять свою чувствительность. Могут подключаться дополнительные датчики, которые в обычное время снимаются с охраны. Плюс появилась интеграция с IP-телефонией. В общем, много интересных возможностей для администратора. Важно правильно сконфигурировать систему под конкретный объект.

Однако системы такого класса вряд ли помогут сократить расходы на персонал. В работе с современными системами появляются штаты системных администраторов, которые занимаются поддержкой. Такие системы — новый уровень информированности, но и персонал для их обслуживания необходим, причем высококвалифицированный.

Современные системы позволяют также собирать информацию по бизнес-процессам компании. Из общей информации можно вычленить, сколько автомобилей, например, возят песок. Если с умом конфигурировать систему, то информации она предоставляет много, она становится более объективной, сокращается количество лиц, которые могут изменять ее. Контроль управления доступом дает свои плюсы. Даже сейчас самыми большими пользователями нашей информации являются налоговые службы.

Охранник не обязан являться пользователем вообще какого-либо интерфейса. Поэтому надо делать такой интерфейс, с которым он мог бы работать, не бояться, понимать его. В случае с ESM ПСЦ «Электроника» вставили в продукт ту оболочку, которая позволяет охраннику сразу пользоваться и системой безопасности, и системой контроля и управления доступа. Когда один продукт, одна оболочка, охранник быстрее привыкает к этому.

Можно и в VSM, например, подключить все системы. Но я скажу, почему мы таким путем не пошли. У нас отдельно видео, и отдельно СКУД. В случае выхода из строя VSM, вся система рухнет, а так замки все будут закрыты, я смогу охранять объект, датчики целы. Если у меня сломается СКУД, я смогу контролировать объект с помощью видеонаблюдения. Они функционируют взаимосвязанно, но не теряют автономности в работе.

В ESM нет своего софта для работы с данными видеонаблюдения, здесь интегрирован «Интеллект» AxxonSoft. ESM принимает информацию от «Интеллекта» и переводит ее в свой интерфейс, но при желании — достаточно щелкнуть кнопкой, и откроется интерфейс «Интеллекта», можно будет работать в нем.

Системы могут помочь объектам сэкономить и на страховании. Сейчас все заводы застрахованы, и когда первоначально построили систему безопасности на одном из предприятий, английская компания-страховщик снизила страховую сумму так, что это позволило окупить почти всю систему безопасности, т.е. страховая сумма была уменьшена в разы.

Вопрос перевода информации системы в «событие» и определения сценария реагирования на данный момент не рассматривается

Тимур Камалетдинов
директор МБУ «Департамент телекоммуникационных технологий города Казани»

С 2017 года Департамент телекоммуникационных технологий города Казани выступает единым заказчиком по системам обеспечения безопасности на объектах социальной инфраструктуры города Казани (более 760 объектов). В состав систем безопасности на объектах социальной инфраструктуры включаются системы пожарной автоматики, передачи извещений без участия человека на пульт централизованного наблюдения пожарной охраны, контроля и управления доступом, тревожной (охранной) сигнализации, видеонаблюдения.

Первичной задачей является мониторинг систем обеспечения безопасности, которые помимо получения сигналов с объектов при грамотном подходе и глубоком погружении позволяет проводить анализ состояния систем на объектах, выявлять слабые места, строить прогнозы и планы развития. Именно в таком порядке разрабатывалась городская информационная система в сфере ЖКХ — от заявок к аналитике и прогнозированию. Вторая задача — непосредственное управление. Третьей задачей является создание универсальной платформы для дальнейшего предоставления доступа к информации в различные заинтересованные ведомства в рамках АПК «Безопасный город».

Департамент рассматривал несколько предложений имеющихся на рынке решений, но на данный момент, к сожалению, мы не видим возможности их применения под указанные задачи. Сложности связаны с тем, что перед разработчиками ставится задача интеграции оборудования различных производителей, моделей, разных годов выпуска. При этом мы не можем себе позволить унифицировать оборудование на объектах на уровне производителя, поскольку это затратно и неэффективно с точки зрения дальнейшего роста. По нашему мнению, требуется единая шина, или же сервисная платформа, предоставляющая возможность перевода информации к формату единого стека открытых протоколов.

Вопрос перевода информации системы в «событие» и определения сценария реагирования на данный момент не рассматривается. На первом этапе необходимо получить возможность мониторинга и управления, и уже после эксплуатации, накопив определенную книгу знаний, можно будет говорить о возможных сценариях реагирования и, соответственно, о возможности отказа от участия человека.

В некоторых городах и субъектах есть что-то отдаленно похожее на PSIM, но это сугубо локальные разработки, адаптировать которые под наши задачи и цели проблематично.

Типовые сценарии реагирования заказчику не нужны

АО «ОКБ Новатор»
(концерн ВКО «Алмаз-Антей»)

По данным источников в АО, в концерне изучают предложения на рынке PSIM в целях проведения модернизации контроля доступа. Три блока задач: пешеходная зона (закрыть несанкционированный доступ людей), автомобильная зона (закрыть доступ несанкционированных автомобилей), воздушная зона.

Заказчик намерен модернизировать систему безопасности и связать ее воедино, чтобы время реагирования было минимальным. Кроме того, интересен контроль информационной безопасности.

Источники в АО «ОКБ Новатор» убеждены: большинство заказчиков сейчас отнеслись бы к оборудованию со сценариями реагирования позитивно. Однако нужно учитывать, что готовые сценарии заказчику не нужны. Ему нужны сценарии под конкретный объект. Перед заказчиком стоят задачи ограничения доступа нежелательных людей, предотвращения актов незаконного вмешательства, при этом ограничить не только проникновение на периметр, но и в конкретные помещения на объекте. Задача сократить штат не стоит, задача в том, чтобы людей разгрузить.

Ключевой критерий PSIM — это открытость, мультивендорность

РоссельхозБанк

По мнению источников в банке, система безопасности верхнего уровня не должна быть привязана к одному конкретному типу (производителю) систем нижнего уровня и должна иметь свой определенный алгоритм (логику) работы, при этом она, в соответствии с заданной иерархией, способна работать с массивом всех данных, поступающих из систем нижнего уровня различных типов всех производителей. В единой системе для каждого уровня должен быть свой ограниченный объем данных и определены строгие правила обмена данными между различными уровнями.

Специалистам служб безопасности на различных объектах/уровнях целесообразно иметь сценарии реагирования на все внешние и внутренние угрозы, разработанные для каждого конкретного объекта в отдельности, и общие корпоративные сценарии реагирования на возникающие глобальные чрезвычайные ситуации.

Новая платформа построения системы безопасности предприятия на базе решений PSIM может помочь в решении целого спектра задач: управления реагированием на возможные возникающие угрозы, аналитики уже произошедших ЧП и инцидентов.

Поэтому ключевой критерий PSIM — это открытость, мультивендорность. Мы можем выйти на объект и предложить необходимое оборудование от популярных брендов, и вся система будет нашей. Заказчик получит необходимый функционал независимо от оборудования.

PSIM глазами интеграторов

PSIM «цементирует» разрозненные аппаратные решения

Василий Перевощиков
инженер технического отдела СП «УНИБЕЛУС» (Беларусь)

PSIM может интегрировать в себя несколько подсистем СКУД различных производителей и уровней. Подобная мультивендорность зачастую отсутствует в интегрированных системах безопасности. Для нас это проблема, потому что мы, например, не работаем с каким-то вендором или конкретный вендор не дает нам право защиты проектов.

PSIM выглядит перспективнее. Мы обычно сводим системы на базе одного из блоков, например VMS, и PSIM работает с любым нашим решением. Как ПО верхнего уровня, оно не принадлежит ни одной такой системе и не имеет ограничений по интеграции. В PSIM можно взять сильные стороны одного бренда и удачные стороны продукта другого, совместить их в одной системе. Нам доводилось интегрировать СКУД с видеонаблюдением, считыватели с тачскрином и т. д.

Бывают ситуации, когда нужно «скрестить бульдога с носорогом». Для Беларуси в департаменте охраны сертифицирована одна охранная система российского производства — Bolid. Частных охранных предприятий у нас нет, поэтому сдать объект под охрану можно только на этом оборудовании. А заказчика не устраивает функционал этой системы в каких-то местах, он хочет, например, PERCo. Иметь на объекте две совершенно не связанные системы — это ненадежно и неудобно. PSIM может их свести.

PSIM может быть также полезна в случае движения собственности на рынке. Если одна компания поглощает другую. Естественно, у собственника появится желание выгружать всю информацию в одну систему. А оборудование может стоять на объектах старых, оно может быт очень разным, поэтому дешевле будет купить PSIM, нежели менять оборудование на одном или нескольких объектах.

Сценарии реагирования не являются уникальным свойством PSIM-систем. Но за счет этого софта можно наделить сценариями те системы, которые исходно их не имеют. А также предложить сценарии реагирования сразу для нескольких конфигураций системы.

PSIM — это скоординированность действий и быстрота реакции

Иван Царев
руководитель направления слаботочных систем компании КРОК

Я бы назвал PSIM софтом верхнего уровня, неким агрегатором, который объединяет разные системы — инженерные, видеонаблюдения, контроля доступа — и позволяет управлять зданием или целым комплексом из единой точки без привлечения лишних человеческих ресурсов.

На личном опыте могу отметить, что такие системы к тому же отлично экономят затраты на эксплуатацию — в КРОК интегрированы все инженерные, пожарные и видеосистемы. Но, конечно, особенно актуальна эта технология для «умных городов», аэропортов, стадионов — любых объектов, где от скоординированности действий и быстроты реакции зависит безопасность тысяч человек. Например, при теракте можно одновременно отследить, как на инцидент отреагировали новые системы, как сработали диспетчеры, в какой последовательности началась отработка ситуации и т. п.

В России PSIM в классическом виде встречается нечасто — у нас любят относить к этой категории любое сочетание видеонаблюдения со СКУД или системой охранно-пожарной сигнализации.

От постоянного мониторинга к проактивности

Вадим Сосенко
директор департамента технической экспертизы и поддержки продаж, Группа «Астерос»

На заре развития PSIM-систем вся логика их работы сводилась к агрегации поступающих от различных систем данных и визуализации тех или иных состояний конечных устройств. Сейчас PSIM-системы превратились в мощные инструменты обеспечения безопасности объектов, с расширенным набором аналитических модулей, позволяющих принимать, обрабатывать и визуализировать инциденты. Множество компаний на рынке способны смонтировать низкоуровневое оборудование, некоторые из них могут закрыть средний уровень, интегрировав оборудование под управлением программной платформы. Но только единицы готовы внедрить мощное высокоуровневое решение, с помощью которого заказчик сможет управлять инцидентами, планировать сервисные мероприятия и быть в курсе уровня защищенности вверенного ему объекта.

Нельзя сказать, что применение PSIM-системы каким-то образом упрощает интегратору вхождение в проект. Как правило, при помощи PSIM-системы интегратор решает проблемы заказчика, которые другими способами решить либо сложно, либо вовсе невозможно. PSIM-система может быть полезна заказчикам, которым приходится обеспечивать определенный уровень безопасности на большой площади либо на критически важных объектах, где даже команда операторов системы не справится с потоком аварийных событий от систем безопасности в случае возникновения инцидента. PSIM-система моментально проанализирует происходящее на объекте, смоделирует развитие инцидента, самостоятельно подберет оптимальный сценарий решения и пошагово подскажет оператору, как справиться с возникшей проблемой. В критических условиях оператору останется лишь механически следовать указаниям умной системы. И заказчики такие возможности PSIM-систем высоко ценят.

Актуальные программные платформы для создания интегрированных систем безопасности

В условиях несформированного рынка широкий круг компаний в России предлагает заказчикам программные платформы в формате PSIM-решений. В данный обзор умышленно включены системы разной степени соответствия термину Physical Security Information Management — с охватом отечественных и зарубежных примеров. Знакомство с функционалом и ограничениями продуктов разных вендоров должно способствовать более конструктивному диалогу заказчиков и производителей в тех случаях, когда речь будет идти о разработке и развертывании PSIM на различных объектах.

Оценка сильных и слабых сторон дана на основе отзывов компаний-интеграторов.

PSIM-система Electronika Security Manager (ESM)

electronika.ru/products-solutions/products/esm/

ESM — программная платформа для создания систем управления безопасностью предприятий с повышенными требованиями к уровню защищенности. Представляет собой платформу для интеграции систем безопасности различных производителей. Существует собственная СКУД для решения сложных задач, в первую очередь — организации СКУД транспортных КПП. В рамках одной системы СКУД возможна поддержка нескольких производителей.

Позиционируется как полноценная PSIM-система, соответствует требованиям законодательства для объектов транспортной инфраструктуры, ТЭК и спортивных объектов. В разработке мобильное приложение для координации и управления полевым персоналом из центра мониторинга.

Сильные стороны

- ✔ Интеграция оборудования и систем различных производителей в части всех систем (видеонаблюдение, СКУД, охранно-пожарная сигнализация, защита периметра). Установка как системы верхнего уровня для эксплуатируемых на объекте систем с целью их интеграции и автоматизации реагирования на угрозы и управления силами охраны.
- ✔ Создание центров мониторинга и ситуационных центров, обеспечивающих контроль за реагированием при возникновении нештатных ситуаций, контроль состояния защищенности объектов и наличия отклонений в реализации штатных мер обеспечения безопасности.
- ✔ Реализация единого бюро пропусков, в т. ч. для нескольких локальных СКУД различных производителей. Электронная система заказа пропусков.
- ✔ Большой перечень интегрированного оборудования, сильная интегрированная видеоподсистема «Интеллект».
- ✔ Сценарное управление реагированием на инциденты.
- ✔ Первопроходцы на рынке PSIM-продуктов.
- ✔ Кроссплатформенность.

Слабые стороны

- ✘ Направленность исключительно на проектные решения.
- ✘ Система не предназначена для объектов, на которых требуются простые и низкобюджетные решения.

Интеграционная система безопасности «Интегра-Планета 4D»

integra-s.com/products/systemonitoring/

«Интегра-Планета-4D» представляет собой геоинформационную систему (ГИС) с частичным функционалом PSIM-системы.

Все объекты, датчики, устройства и даже видеоизображение привязаны к географическим координатам и времени.

Первоочередное внимание при разработке уделяется всестороннему соответствию требованиям законодательства в части реализации интегрированных систем безопасности.

Платформа применима для работы как с небольшими объектами (одиночные здания или подвижной состав), так и с большими территориями (города и регионы).

Сильные стороны

- ✔ Использование электронно-цифровых подписей для проверки прав на получение информации при подключении к территориально удаленным объектам.
- ✔ Поддержка ГИС и 3D-моделей объектов с привязкой изображений к координатам местности, наложение видеоизображения на 3D-модель объекта. Интеграция с системами спутникового мониторинга.
- ✔ Активация обработки инцидентов по результатам верификации тревожных событий.
- ✔ Кроссплатформенность, поддержка ОС Windows и Linux.

Слабые стороны

- ✘ Не обеспечена интеграция со СКУД других производителей.

- ✘ Малый перечень интегрированных систем сторонних производителей, в части систем видеонаблюдения поддерживается только своя и «Интеллект».
- ✘ Система ориентирована в первую очередь на сбор информации о внештатных ситуациях, не на организацию реагирования на них. В каталоге есть отдельное, имеющее другой интерфейс пользователя, программное обеспечение для управления силами и средствами реагирования в рамках АПК «Безопасный город». Однако информация о его возможностях и интеграции с «Интегра-Планета-4D» отсутствует.
- ✘ Инциденты и задачи создаются и назначаются вручную.

PSIM-система FAST (TERRA 4D)

fastprotect.net

FAST (TERRA 4D) представляет собой геоинформационную систему (ГИС), в которой все объекты, датчики, устройства и даже видеоизображение привязаны к географическим координатам и времени. Система обладает всеми функциями PSIM-систем.

Сильные стороны

- ✔ Интеграция оборудования и систем различных производителей в части всех систем (видеонаблюдение, СКУД, охранно-пожарная сигнализация, защита периметра и др.).
- ✔ Поддержка ГИС и 3D-моделей объектов с привязкой изображений к координатам местности, наложение видеоизображения на 3D-модель объекта.
- ✔ Интеграция с системами спутникового мониторинга.
- ✔ Базовые функции в части вывода операторам пошаговых инструкций по верификации тревожных событий и координации реагирования на инциденты.
- ✔ Интеграция с системами телефонной связи.
- ✔ Координация и управление полевым персоналом из центра мониторинга с использованием мобильных устройств.
- ✔ Создание центров мониторинга и ситуационных центров.

Слабые стороны

- ✘ Ориентированность системы FAST (TERRA 4D) в первую очередь на системы общественной безопасности (112, 911).
- ✘ Инструкции по реагированию являются линейными, без возможности адаптации под развитие ситуации.
- ✘ Высокая стоимость внедрения системы.
- ✘ Не имеет представителей и опыта работы в России.

Интегрированная система безопасности «Интеллект»

itv.ru/products/intellect/

«Интеллект» — многофункциональная открытая программная платформа, предназначенная для создания комплексных систем безопасности любого масштаба.

Система безопасности на базе программного комплекса «Интеллект» способна объединить видеонаблюдение, охранно-пожарную сигнализацию (ОПС), систему охраны периметра, систему контроля и управления доступом (СКУД), аудиоконтроль в согласованно работающую инфраструктуру.

Сильные стороны

- ✔ Наличие простейших функций по обработке тревожных событий, возможность отметить их как ложные, подозрительные и тревожные, есть эскалация обработки событий.
- ✔ Большой перечень интегрированного оборудования.
- ✔ Сильная видеоподсистема.
- ✔ Известность на рынке.
- ✔ Доступная, по сравнению с рынком PSIM-решений, цена

Слабые стороны

- ✘ Нет возможности интеграции с VMS сторонних производителей.
- ✘ Нет функций по организации реагирования на инциденты и управления силами охраны.
- ✘ Нет поддержки ГИС.
- ✘ Система не кроссплатформенная (только ОС Windows).

Интегрированная система безопасности VideoNet

videonet.ru/videonet-9-download.html/

«VideoNet» — программная платформа системы видеонаблюдения, предназначенная для интеграции видеоаудиосистем, СКУД и ОПС. Поддерживает спецификации OPC DA 2.0 для мониторинга технологических процессов и взаимодействия с внешними системами. Не является PSIM-системой — управление инцидентами не подтверждено функционалом в описании системы, продукт допускает мониторинг и автоматические реакции в пределах классического функционала ИСБ.

Сильные стороны

- ✔ Использование нейронных сетей для видеоанализа.
- ✔ Встроенная видеоподсистема.

Слабые стороны

- ✘ Малое количество интегрированных систем: «Орион» (ОПС и СКУД), малопопулярная Quest (СКУД), INTREPID II (защита периметра).
- ✘ Нет возможности интеграции системы видеонаблюдения сторонних производителей.
- ✘ Нет функций по организации реагирования на инциденты и управления силами охраны.
- ✘ Нет поддержки ГИС.
- ✘ Система не кроссплатформенная (нет поддержки ОС Linux), нет инцидентов и настройки процессов и регламентов их обработки.

Интеграционная система безопасности и управления инженерной инфраструктурой Alphalogic

alphaopen.com/products/platform/

Программная платформа Alphalogic является основой для создания интегрированных систем безопасности и систем управления инженерной инфраструктурой зданий. В рамках создания ИСБ обеспечивается интеграция систем видеонаблюдения, СКУД, ОПС и системы защиты периметра различных производителей.

В рамках создания систем управления инженерной инфраструктурой зданий обеспечивается поддержка множества общеотраслевых стандартов, инженерных систем популярных производителей.

Доступен биллинг потребляемых ресурсов.

Система рассчитана на объекты различного масштаба. Позиционируется как PSIM-платформа, однако отсутствие в открытом доступе подробной информации по возможностям программной платформы Alphalogic не позволяет подтвердить или опровергнуть эту информацию.

Сильные стороны
- ✔ Большой перечень интегрированного оборудования и протоколов.
- ✔ Неограниченные возможности конфигурирования системы (интерфейсов и бизнес-логики) под задачи заказчика.
- ✔ Поддержка ОС Windows и Linux.
- ✔ Обработка инцидентов.

Слабые стороны
- ✘ Нет поддержки ГИС и 3D-изображений.
- ✘ Сложность и трудоемкость конфигурирования и настройки.
- ✘ Сложность лицензионной политики, точная стоимость ПО определяется после реализации проекта по файлу конфигурации.

Интеграционная система безопасности КСБ ITRIUM

itrium.ru/products/itrium/

ITRIUM — программная платформа для создания интегрированных систем безопасности объектового уровня, предназначенная для интеграции систем видеонаблюдения, СКУД, ОПС и системы защиты периметра различных производителей. При проектировании ИСБ отдается предпочтение системам видеонаблюдения (СВН), СКУД и ОПС собственного производства.

Поддерживает нестандартные протоколы для интеграции систем безопасности и технических средств различных производителей.

Автоматизирует процессы управления безопасностью объекта — комплексный мониторинг безопасности, управление пропускным режимом, видеонаблюдение.

ITRIUM интегрирована с системой комплексного мониторинга «ULTIMA», которая предназначена для создания центров мониторинга. Отсутствие в открытом доступе подробной информации по возможностям программной платформы «ULTIMA» не позволяет сделать выводы о поддержке ею основных принципов PSIM-систем.

Сильные стороны
- ✔ Интеграция оборудования и систем различных производителей.
- ✔ Установка системы как верхнего уровня для эксплуатируемых на объекте систем с целью их интеграции.
- ✔ Реализация единого бюро пропусков, в т.ч. для нескольких локальных СКУД различных производителей. Электронная система заказа пропусков.
- ✔ Возможность создания центров мониторинга с использованием программной платформы «ULTIMA».
- ✔ Большой перечень интегрированного оборудования и протоколов, известность на рынке.

Слабые стороны
- ✘ Нет функций по организации реагирования на инциденты и управления силами охраны. Нет поддержки ГИС и 3D-изображений.
- ✘ Система не кроссплатформенная.

Интеграционная система безопасности «Индигирка»

sigma-is.ru/products/software/id-spo.html/

СПО «Индигирка» — специальное программное обеспечение для создания интегрированной системы безопасности на базе оборудования производства компании «Сигма-ИС». Предназначено для организации автоматизированных рабочих мест (АРМ) дежурного режима операторов ТСО (технических средств охраны), СКУД (системы контроля и управления доступом), СОТ (системы охранного телевидения), КПП (контрольно-пропускные пункты) в интегрированных системах безопасности (ИСБ).

Работает совместно с оборудованием ИСБ Р-08 и «Индигирка» производства ГК «Сигма» и обеспечивает прием информационных и тревожных событий, интерактивное отображение состояния объекта охраны на графических планах, управление техническими средствами охраны операторами службы безопасности.

Сильные стороны
- ✔ СПО «Индигирка» и интегрируемое оборудование выпускается одним производителем, что гарантирует полную поддержку всех возможностей оборудования.
- ✔ Поддержка защищенных операционных систем МСВС и Astra Linux.
- ✔ Соответствует требованиям 188-ФЗ о едином реестре российского программного обеспечения.
- ✔ Имеет сертификаты ФСБ, ФСТЭК, Минобороны.

Слабые стороны
- ✘ Поддержка оборудования только «Сигма-ИС», которое не всегда является оптимальным для тех или иных типов объектов. Ограниченные возможности встроенной видеосистемы. Нет возможности интеграции уже установленных на объекте систем.
- ✘ Нет функций по организации реагирования на инциденты и управления силами охраны.
- ✘ Нет поддержки ГИС.
- ✘ Нет информации о поддержке популярных операционных систем.

ПО RM-3 — распределенная программная интеграционная платформа

sigma-is.ru/products/software/rm-3.html/

ПО RM-3 является аналогом СПО «Индигирка» для коммерческого рынка. Отличается от СПО «Индигирка» тем, что обеспечивает работу по ОС Windows и интеграцию СВН «Интеллект».

Интеграционная платформа Securix

www.asteros.ru/solutions/security/securix/

Securix — интеграционная платформа безопасности, которая обеспечивает тесную взаимосвязь между подсистемами контроля и управления доступом, аналогового и IP-видеонаблюдения, охранно-тревожной сигнализации, пожарной сигнализации и других подсистем.

Продукт известен на российском рынке уже более 15 лет.

Сильные стороны
- ✔ Большой перечень интегрированного оборудования, гибкие возможности настройки системы (интерфейсов и бизнес-логики) под задачи заказчика, обработка инцидентов, настройка регламентов обработки инцидентов.

Слабые стороны
- ✘ Нет поддержки ГИС и 3D-изображений.
- ✘ Нет поддержки ОС Linux.

Интеграционная система безопасности и управления инженерной инфраструктурой Building Integration System (BIS) от Bosch

resource.boschsecurity.com/documents/BIS_Commercial_Brochure_all_18673346571.pdf/

Программная платформа BIS, производимая компанией BOSCH (Германия), является основой для создания интегрированных систем безопасности и систем управления инженерной инфраструктурой зданий.

В рамках создания ИСБ обеспечивается интеграция систем видеонаблюдения, СКУД и ОПС производства Bosch либо других производителей, которые имеют возможность интеграции по протоколу OPC.

В рамках создания систем управления инженерной инфраструктурой зданий обеспечивается поддержка множества общеотраслевых стандартов и инженерных систем популярных производителей.

Система рассчитана на объекты различного масштаба, позволяет выводить операторам инструкции по действиям в нештатных ситуациях, однако не является PSIM-платформой.

Сильные стороны

- ✔ Популярный во всем мире производитель с высоким уровнем репутации.
- ✔ Поддержка интеграции разнообразных инженерных систем, что может быть востребовано при обеспечении безопасности некоторых видов объектов, например высотных зданий, торговых центров и т. п.
- ✔ Вывод операторам инструкций по тревогам для действий в данной ситуации.

Слабые стороны

- ✘ Нет возможности интеграции уже установленных на объекте систем безопасности и применения СВН и СКУД других производителей.
- ✘ Нет функций по организации реагирования на инциденты и управления силами охраны.
- ✘ Нет поддержки ГИС.
- ✘ Инструкции по реагированию являются линейными, без возможности адаптации под развитие ситуации.
- ✘ Система не мультиплатформенная.

PSIM-система Situator Situation Management Software (Qognify, бывшая Nice, Израиль/США)

qognify.com/situation-management-psim/

Qognify Situator — программная платформа, разработанная израильской компанией для создания систем управления безопасностью предприятий с повышенными требованиями к уровню защищенности и потребностью в создании ситуационного центра. Поддерживает все функции PSIM-систем. Позволяет анализировать BigData. На сайте производителя представлена информация о реализации как минимум двух проектов в России: «Безопасный город Сочи» и ситуационный центр «Аэроэкспресс».

При этом Qognify ранее являлась подразделением компании NICE Systems, которое было продано американской венчурной фирме Battery Ventures. Данные из открытых источников позволяют связать учредителей NICE Systems с подразделением радиотехнической войсковой разведки Израиля, а венчурную фирму Battery Ventures — с Министерством обороны США.

Сильные стороны

- ✔ Интеграция оборудования и систем различных производителей в части всех систем (видеонаблюдение, СКУД, охранно-пожарная сигнализация, защита периметра).
- ✔ Вывод операторам пошаговых инструкций по верификации тревожных событий и координации реагирования на инциденты.
- ✔ Интеграция с системами телефонной связи.
- ✔ Координация и управление полевым персоналом из центра мониторинга с использованием мобильных устройств.
- ✔ Создание центров мониторинга и ситуационных центров.
- ✔ Поддержка ГИС, интеграция в системы спутникового мониторинга.
- ✔ Анализ больших данных с использованием алгоритмов искусственного интеллекта, включая мониторинг социальных сетей и форумов на предмет выявления потенциальных угроз безопасности.

Слабые стороны

- ✘ Система предназначена для сбора значимой информации о состоянии защищенности объектов и передвижениях важных персон, при этом в открытом доступе можно проследить связь со спецслужбами иностранных государств.
- ✘ В России отсутствуют квалифицированные технические специалисты.
- ✘ Решение направлено исключительно на проектные решения, система не предназначена для объектов, где требуются простые и низкобюджетные решения.
- ✘ Высокая стоимость внедрения системы.
- ✘ Система не кроссплатформенная.

PSIM-система IP Security Center (CNL, Великобритания)

cnlsoftware.com/ipsecuritycenter/ipsecuritycenter/

CNL является одним из лидеров PSIM-систем. IP Security Center представляет собой платформу для интеграции систем безопасности различных производителей. Система обладает большинством функций PSIM-систем.

Сильные стороны

- ✔ Интеграция оборудования и систем различных производителей в части видеонаблюдения, СКУД, охранно-пожарной сигнализации, защиты периметра.
- ✔ Возможен вывод операторам пошаговых инструкций по верификации тревожных событий и координации реагирования на инциденты.
- ✔ Доступна координация и управление полевым персоналом из центра мониторинга с использованием мобильных устройств.
- ✔ Поддержка ГИС, интеграция с системами спутникового мониторинга.
- ✔ Возможно создание на базе платформы центров мониторинга и ситуационных центров.

Слабые стороны

- ✘ Одна из немногих PSIM-систем, не имеющая интеграции с системами телефонной связи.
- ✘ Направленность — на системы общественной безопасности (112, 911).
- ✘ Вероятно, самая высокая стоимость внедрения из всех рассмотренных вариантов.
- ✘ Система не мультиплатформенная.
- ✘ Не имеет представителей в России.