Между PSIM и КСБ

Место физических систем информационного управления защитой объектов в иерархии систем безопасности до сих пор окончательно не определено. Одни компании отводят для PSIM самостоятельную нишу. Другие склонны включать их в состав комплексных и интегрированных решений. Так как регулирующих норм все еще нет — правы, судя по всему, и те и другие.

PSIM — это дорого, но очень эффективно

Андрей Скворцов
директор по развитию,
ООО ПСЦ «Электроника»

Системы PSIM имеют следующие основные особенности.

1 Интеграция — интеграция разнородных систем различных производителей, которые являются источником информации об угрозах.

2 Анализ — анализ тревожных событий с целью определения типа угрозы (инцидента) и степени ее влияния на безопасность и назначения приоритета реагирования.

3 Верификация — предоставление оператору всесторонней информации об инциденте с целью помощи оператору в выполнении правильной ее оценки.

4 Реагирование — предоставление оператору пошаговых инструкций и автоматизация процесса реагирования на инцидент, в том числе управление силами охраны.

5 Отчетность — сбор и консолидация всех данных об инциденте и реагировании на него, автоматизация формирования отчетов по инцидентам.

6 Расследование — отслеживание системой каждого оператора, насколько он правильно и своевременно реагирует на каждый инцидент.

При внедрении PSIM-систем используется системный подход. Сам процесс внедрения состоит из следующих этапов: планирование, эксплуатация, анализ, совершенствование.

ПЛАНИРОВАНИЕ

На этапе планирования определяется перечень актуальных угроз и вероятных способов их реализации, определяются наиболее оптимальные способы обнаружения угроз, разрабатывается перечень мер реагирования на угрозы, оценивается достаточность человеческих и материальных ресурсов для отражения и ликвидации угроз, даются рекомендации по совершенствованию организационно-штатной структуры, нормативно-правового и материально-технического обеспечения.

ЭКСПЛУАТАЦИЯ

На этапе эксплуатации осуществляется выявление инцидентов безопасности, их верификация и реагирование на них. В штатном режиме работы PSIM-системы обеспечивают автоматизацию следующих процессов:

Two Sides of One Platform. PSIM-Solutions Through the Lens of PSC Electronika and ITRIUM SPb Companies / By Andrew Skvortsov, Business Development Director, PSC Electronika, Mikhail Rybakov, CEO, ITRIUM SPb

The place of PSIM solutions in security systems hierarchy has not been defined yet. Some think that PSIM is a standalone market segment. Others include it as a component of complex and integrated security systems. As fas as there are no regulatory documents, all of them seem to be right.

- выявление тревожных событий, которые могут свидетельствовать о наличии угрозы безопасности;
- помощь оператору в верификации тревожных событий;
- поддержание операторов, контролирующих технические средства охраны, в состоянии высокой бдительности;
- сохранение результатов верификации тревожных событий с указанием причин принятия того или иного решения;
- помощь в расстановке и эффективном использовании сил и средств охраны;
- выявление отклонений в расстановке сил и средств от плана.

В рамках **реагирования на инциденты** PSIM-системы обеспечивают автоматизацию следующих процессов:

- выбора наилучшего сценария реагирования на угрозу с онлайн-корректировкой пошаговой инструкции по реагированию в соответствии с развитием ситуации;
- управления системами физической безопасности;
- управления силами и средствами обеспечения безопасности (мониторинг местоположения сил и средств, автоматизация назначения им заданий и отслеживание статуса выполнения заданий, обмен информацией между центральным постом охраны и силами реагирования);
- оповещения должностных лиц, ответственных за обеспечение безопасности, дежурных и оперативных служб (интеграция средств телефонной связи, выполнение автоматических и автоматизированных оповещений, запись фонограмм разговоров с привязкой к карточкам инцидентов).

АНАЛИЗ

На этом этапе выполняется анализ совершенных и предотвращенных инцидентов безопасности. На основе анализа результатов делаются выводы и составляются рекомендации по совершенствованию системы обеспечения безопасности.

СОВЕРШЕНСТВОВАНИЕ

На этапе совершенствования осуществляется планирование и реализация мероприятий по совершенствованию процессов обеспечения безопасности и реагирования на инциденты.

Требования к функциям	Системы общественной безопасности	Системы объектовой безопасности
Основной источник информации об инцидентах	Звонки граждан. Требуется создание call-центра. Интеграция информационных систем федерального масштаба СМИС, Стрелец-Мониторинг, ЭРА-ГЛОНАСС, ГИС ЭКХ, СС-ТМК и т.д.	Тревожные события от систем безопасности. Требуется интеграция систем различных производителей, как правило, по проприетарным протоколам. Информация об инцидентах, выявленная силами охраны, в том числе полученная от персонала или посетителей объекта
Доступная оператору информация об инциденте	Информация, полученная от звонящего абонента, онлайн-видеоизображение при наличии камер	Доступна информация от различных систем, в т.ч. онлайн-видеоизображение и видеозапись момента возникновения тревожного события
Достоверность инцидентов	Высокая или выше средней. Существуют ложные вызовы, но есть возможность их привязать к номеру абонента, который о них сообщает. Информация в информационных системах поступает в целом либо из относительно надежных источников, либо вводится после проверки	Низкая от систем безопасности. Большинство тревожных сигналов не связано с реальной угрозой безопасности. Требуется поддержание бдительности операторов и помощь в верификации событий
Знание оператором специфики местности	Нет. Все данные запрашиваются у звонящего абонента	Хорошее знание особенностей местности
Геоинформационная система	Карта города, области	План территории объекта с переходом на поэтажные планы зданий
Необходимость управления системами безопасности	Нет	Да
Архитектура	Архитектура унифицирована. ЕДДС принимает вызов и заполняет карточку инцидента и передает ее на реагирование в ДДС 01, 02, 03, 04, ЖКХ. Оператор ЕДДС контролирует своевременность прибытия сил и средств к месту инцидента	Архитектура подстраивается под масштаб объекта. Оператор выполняет верификацию инцидента, при подтверждении реагирование может передаваться оператору с большим уровнем полномочий по привлечению ресурсов. Доступен контроль реагирования со стороны диспетчеров верхнего уровня и оповещение о допущенных нарушениях при реагировании
Силы реагирования	ЕДДС не имеет собственных сил реагирования. Используется полиция, скорая помощь, МЧС, которые действуют по своим инструкциям. Как правило, обеспечивается автоматизация специфических функций ДДС 01, 02, 03, 04, ЖКХ, в том числе создание базы данных сил и средств, автоматизация документооборота, оформление путевых листов и т.д.	Собственные силы, действующие по своим инструкциям, возможность полноценного управления силами и средствами
Использование мобильных устройств для автоматизации управления силами	Нет, используются только штатные системы, принятые на снабжение в экстренных и оперативных службах	Да, что повышает эффективность управления и контроля

Системы PSIM-класса широко используются в мире при построении систем общественной безопасности **«911» и «112»**

PSIM-интеграторы отличаются от инсталляторов систем физической безопасности тем, что ставят во главу угла не установку видеокамер, датчиков и электронных замков, а выявление и устранение актуальных угроз безопасности. При этом PSIM-интеграторы выходят за рамки классических систем безопасности и работают со всем имеющимся перечнем угроз. Например, на объектах нефтегазового комплекса актуальна защита не только периметров предприятий, но и трубопроводов; на спортивных объектах востребована активация разных уровней безопасности в зависимости от проводимого спортивного мероприятия.

Понятие PSIM не является стандартом, но производители PSIM-систем выделяют следующие **обязательные составляющие правильного PSIM-решения**.

1 PSIM должна иметь возможность интегрировать уже имеющиеся системы безопасности, а также должна обеспечивать возможность получения информации об актуальных угрозах от любых других систем: жизнеобеспечения, кибербезопасности, экологической безопасности и других.

2 PSIM должна обрабатывать информацию обо всех угрозах безопасности, в том числе выявленных людьми и по которым не поступало тревожных сигналов.

3 PSIM должна быть интегрирована со средствами телефонной связи для обеспечения автоматизации вызовов.

4 PSIM должна выводить операторам пошаговые инструкции по реагированию на угрозы. При этом инструкция должна быть интерактивна и выполнение оператором шагов инструкции должно автоматизировать управление системами безопасности, выполнение оповещений и телефонных вызовов, сбор дополнительных сведений об инциденте, корректировку самой инструкции в соответствии с развитием ситуации.

5 PSIM должна иметь мобильные устройства для автоматизации работы персонала охраны, работающего в «полевых условиях», включая назначение и контроль выполнения задач, мониторинг передвижения, голосовую связь, трансляцию видео с места инцидента.

6 PSIM должна сохранять всю информацию с привязкой к инцидентам, автоматически формировать и рассылать отчеты по инцидентам.

Системы PSIM-класса широко используются при построении систем общественной безопасности «911» и «112». При этом мировой опыт в этой сфере учтен в Концепции построения и развития аппаратно-программного комплекса «Безопасный город», утвержденной распоряжением Правительства Российской Федерации от 3 декабря 2014 г. № 2446-р, и Единых требованиях к техническим параметрам сегментов аппаратно-программного комплекса «Безопасный город».

Применение PSIM-систем также эффективно для создания систем безопасности объектового уровня, что наиболее актуально для объектов с повышенными требованиями к уровню защиты различных зданий и объектов.

Внедрение PSIM, с одной стороны, многократно дороже внедрения классического программного обеспечения ИСБ за счет более высокой стоимости программного обеспечения, более сложного процесса внедрения и привлечения высококвалифицированных специалистов. С другой стороны, в рамках реализации ИСБ крупного объекта PSIM позволит повысить эффективность защиты объекта и не приведет к существенному увеличению стоимости системы в целом. PSIM-решения востребованы на объектах, где предъявляются повышенные требования к уровню защиты или требуется эффективный контроль состояния защищенности сети распределенных объектов. PSIM-решение находится в премиум-сегменте рынка, и его невозможно внедрить на объекте, где служба безопасности финансируется по остаточному принципу.

PSIM — лишь подсистема КСБ

Михаил Рыбаков
генеральный директор,
ООО «ИТРИУМ СПб»

PSIM — это класс программного обеспечения, которое представляет платформу и приложения для интеграции разных функциональных приложений и технических средств безопасности, а также для управления ими через единый интерфейс или группу взаимосвязанных интегрированных пользовательских интерфейсов.

Особенности и возможности PSIM представлены ниже в обобщенном перечне (по зарубежным источникам).

1 **Сбор данных и интеграция:** программное обеспечение собирает и интерпретирует (интегрирует) данные из любого числа разнородных устройств или систем безопасности.

2 **Анализ:** программное обеспечение анализирует, объединяет и сопоставляет данные о событиях, состояниях технических средств, сигналах тревог для выявления реальных ситуаций и определения приоритетов реагирования.

3 Верификация: программное обеспечение предоставляет разностороннюю информацию о событиях в интуитивно понятном интерфейсе и удобной форме для проверки и подтверждения или отклонения.

4 Поддержка бизнес-процессов: программное обеспечение предоставляет стандартные операционные процедуры (SOP), пошаговые инструкции на основе рекомендаций и политик организации, а также инструменты для разрешения ситуации.

5 Отчеты: программное обеспечение отслеживает и накапливает всю поступающую информацию и информацию о действиях, решениях и командах, содержит встроенные средства построения разносторонних адаптивных отчетов для анализа, проведения тренингов и учебы.

6 Контрольный журнал: программное обеспечение отслеживает и регистрирует все действия операторов, принимаемые ими решения, управленческие команды, переговоры, а также время реакции на события и принятие решений.

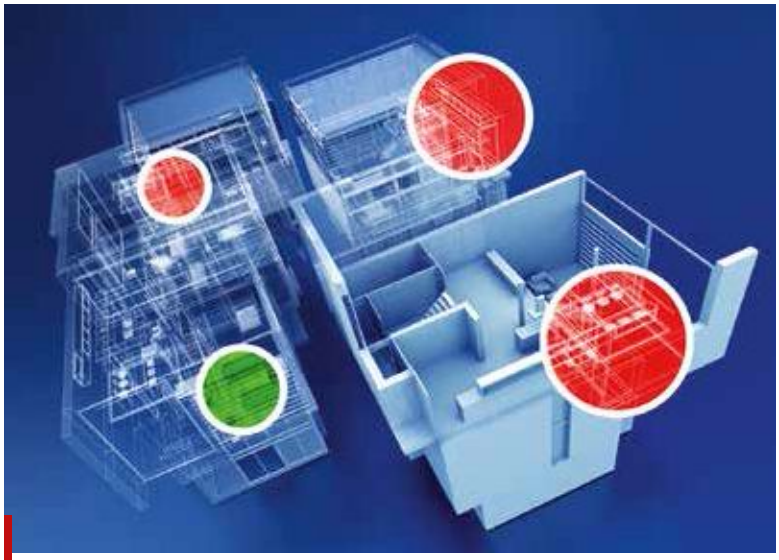
К примеру, **перечень заявленных функциональных особенностей ESM** (ПСЦ «Электроника», Ярославль) содержателен и по количеству решаемых задач коррелирует с представленным выше списком.

- Интеграция всех технических решений в единой информационной среде.
- Сценарный механизм обнаружения угроз; определение достоверности событий и критичности ситуации.
- Активация пошаговых инструкций, направленных на разрешение инцидента.
- Адаптация под заданный уровень угроз.
- Координация сил реагирования, своевременное оповещение всех заинтересованных лиц.
- Контроль работы оператора с системой, анализ эффективности принятых мер.
- Сбор доказательной базы и автоматическое формирование отчетов.

Обобщенно, **ключевыми задачами PSIM** являются:

- Интеграция и сбор данных от разнородных средств и систем.
- Обработка и анализ «внешних» данных от средств и систем, а также «внутренних» данных, в том числе поведенческих.
- Автоматизация бизнес-процессов мониторинга, управления и всестороннего контроля.

В этом контексте привнесенный акроним — PSIM — не отражает какой-то новой сущности, которой до сих пор не было на российском рынке. Программные средства систем пультовой охраны (например, «Андромеда») или программные средства автоматизированных рабочих мест (АРМ) операторов так называемых ССОИ (системы сбора и обработки информации) компаний «Элерон», «Алгонт», «ААМ Системз» и других поставщиков в той или иной степени решают те же задачи. Иными словами, PSIM — это хорошо известная система мониторинга и управления в составе комплексных систем безопасности (КСБ).



В части сбора данных PSIM играет ту же роль в области обеспечения физической безопасности, что SCADA-системы — в области промышленной автоматизации или автоматизации систем жизнеобеспечения зданий и сооружений. Но в отличие от систем автоматизации физическая безопасность имеет дело в первую очередь не с измерениями и контролем параметров, а с дискретными событиями, сообщениями и угрозами. Данные в SCADA — это тэги параметрических данных, в PSIM — извещения и сообщения о состояниях и событиях

Разные **системы мониторинга и управления КСБ отличаются друг от друга** не названием, а тем, как:

- эффективно, глубоко и «бесконфликтно»* интегрированы средства и подсистемы;
- система обрабатывает, объединяет, коррелирует и анализирует данные, снижая ложные тревоги и вызовы, удобно и эргономично предоставляет информацию и интерфейс операторам и ответственным лицам;
- обеспечивает деятельность операторов, поддерживает принятие решений, автоматизирует документооборот.
- насколько система современна, проста и удобна в развертывании, позволяет ли она гибко адаптировать бизнес-логику под бизнес-процессы потребителя, возможно ли ее использование, обслуживание, внесение «патчей», изменений и расширение без разработчика и производителя.

Таким образом, принципиальное отличие современной PSIM от традиционных систем мониторинга и управления состоит в процессной направленности не только и не столько в части реагирования, сколько в минимизации рисков, предсказании и профилактике происшествий и нарушений безопасности. Но все-таки следует учесть, что PSIM — это лишь одна из подсистем КСБ.

* Чаще всего именно здесь проявляются проблемы. Разработчики и производители «железа» не очень озабочены качеством предоставляемых API и свободно меняют протоколы в новых версиях продукта, а разработчики «интеграционного ПО» не могут позволить себе создавать масштабные зоны тестирования множества чужих систем.