

Р. Р. ФАТКИЕВА, Е. Л. ЕВНЕВИЧ

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, Санкт-Петербург

УПРАВЛЕНИЕ ПЕРИМЕТРОМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ

Мониторинг информационной безопасности промышленных объектов производится с участием средств, порождающих наборы гетерогенных данных, что не всегда согласуется с использованием различных нормативных документов. Формирование характеристик безопасности на основании данных периметра мониторинга и определения его уровня безопасности осуществляется чаще всего с помощью вычисления интегрального показателя, недостаточно отражающего отдельные аспекты обеспечения безопасности. Предложен метод гармонизации взаимодействия ПмО и формирования набора показателей безопасности на основе формализации описания предметной области и унификации схемы описания данных.

Введение. Одна из основных проблем гармонизации систем мониторинга и управления промышленными объектами (ПмО) – это отсутствие методологических рекомендаций по измерению, интерпретации и оценке параметров функционирования, которые представляют собой разнородные данные, полученные как прямым измерением, так косвенным.

Решение проблемы для большого количества разнообразных средств мониторинга, включенных в периметр ПмО, требует введения ведомственных законодательных актов в отрасли, или внесения изменений в существующие правила функционирования в пределах группы предприятий ПмО [1]. Однако обоснование подобных изменений в регламентирующих документах чаще всего основывается на оценке интегрального показателя по критерию максимизации целевой функции, что не всегда может обеспечить заданный уровень управляемости и устойчивости комплекса ПмО. Это подтверждает необходимость введения процедуры гармонизации [2], задачей которого является построение непротиворечивого формального описания предметной области и разработки прикладного программного обеспечения для поддержки унифицированной схемы данных, включая построение терминологических таксономий, предикативных отношений, дескриптивных ограничений для вывода новых данных о функционировании показателей и расширение множества правил вывода.

Характеристика подходов к управлению ПмО. К настоящему времени сложились следующие подходы к управлению группой распределенных ПмО: семантический – на основе анализа терминологического и понятийного аппарата описаний продукции, процессов и ресурсов ПмО и построения онтологий предметной области; проектно-системообразующий – на основе логического анализа происходящих процессов на разных стадиях жизненного цикла ПмО; динамический – на основе текущего мониторинга состояния и оценки показателей ПмО, таких как надежность, безопасность, эффективность использования ресурсов.

С другой стороны, в связи с развитием индустриального Интернета требования к системам мониторинга, обладающим единым центром управления, только начинает формироваться. Так, в ГОСТ'e [3] уже явным образом указано о возможности применения как централизованного, так и полицентрического способов организации систем мониторинга и управления. В этих условиях остро встает вопрос о единстве методов измерений, обработки и передачи информации, необходимой для принятия решений в области управления при взаимодействии ПмО. Для достижения необходимого уровня функционирования требуется системное согласование всех используемых мер, методов и средств управления, а также разработка методов и алгоритмов согласования операционных процессов ПмО.

Метод формирования системы гармонизации взаимодействия ПмО. Пошаговое описание предлагаемого метода:

Шаг 1. Формализация процесса операционной деятельности и процедур согласования набора показателей, оценивающих эту деятельность (рис. 1).

Шаг 2. Определение периметра обеспечения выполнения заданных целевых показателей, сформированных на шаге 1, с возможностью изменения их в процессе функционирования, для чего необходимо (рис. 2):

2.1. Сформировать группу ПмО и операционных процессов для мониторинга. Определить границы периметра и методы идентификации его нарушения.

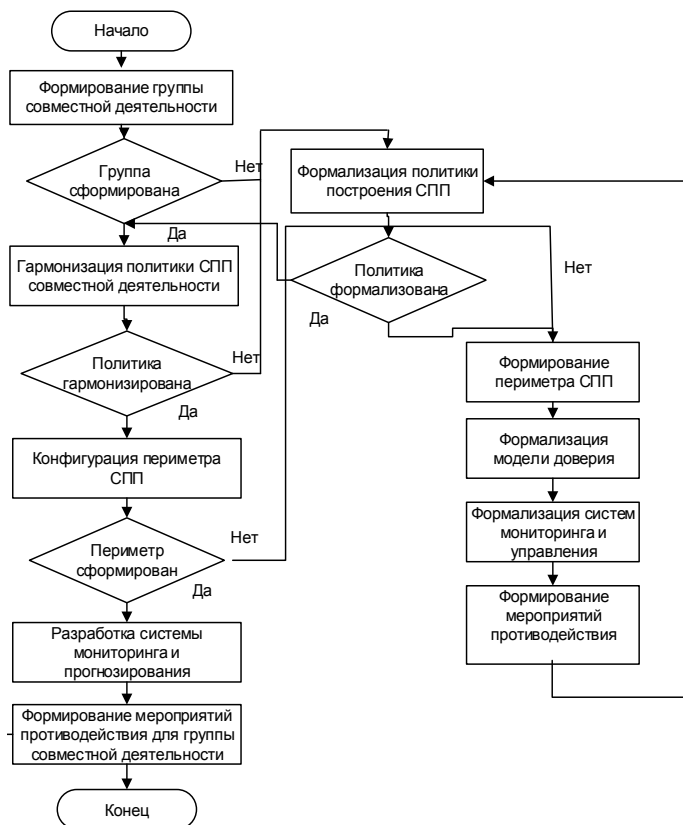


Рис. 1. Метод формирования системы гармонизации взаимодействия систем, входящих в ПмО



Рис. 2. Метод формирования периметра показателей мониторинга группы ПмО

2.2. Осуществить определение политики идентификации элементов, входящих в ПмО (ЭЦП, хеширование идентификатора, туннелирование), с присвоением уникального идентификатора (метаданных платформы, ключей и т. п.) согласно политике идентификации. Это позволит отслеживать перемещения элементов мониторинга в заданном периметре.

2.3. Произвести аттестацию ПмО.

2.4. Осуществить инициализацию набора данных для мониторинга согласно сформированной политике взаимодействия.

Шаг 3. Разработка системы реагирования как для каждой из систем ПмО, так и для деятельности в целом, состоит из следующих этапов (рис. 3):

3.1. Измерение и сбор данных о системе (определение периода мониторинга сбора данных о динамике изменения периметра динамических объектов).

3.2. Обработка данных (агрегирование, определение ключевой информации, поиск сигнатур по текущему множеству изменения показателей, классификация типа показателей).

3.3. Анализ текущего состояния (сравнение с заранее созданным шаблоном (поиск строк, регулярных выражений и т. д.), распознавание (последовательное сравнение со всеми сигнатурами, дерево сравнений, декомпозиция, ассоциативный доступ).

3.4. Оценка результатов (анализ изменений функции распределения, изменения топологии системы, изменения производительности системы и др.

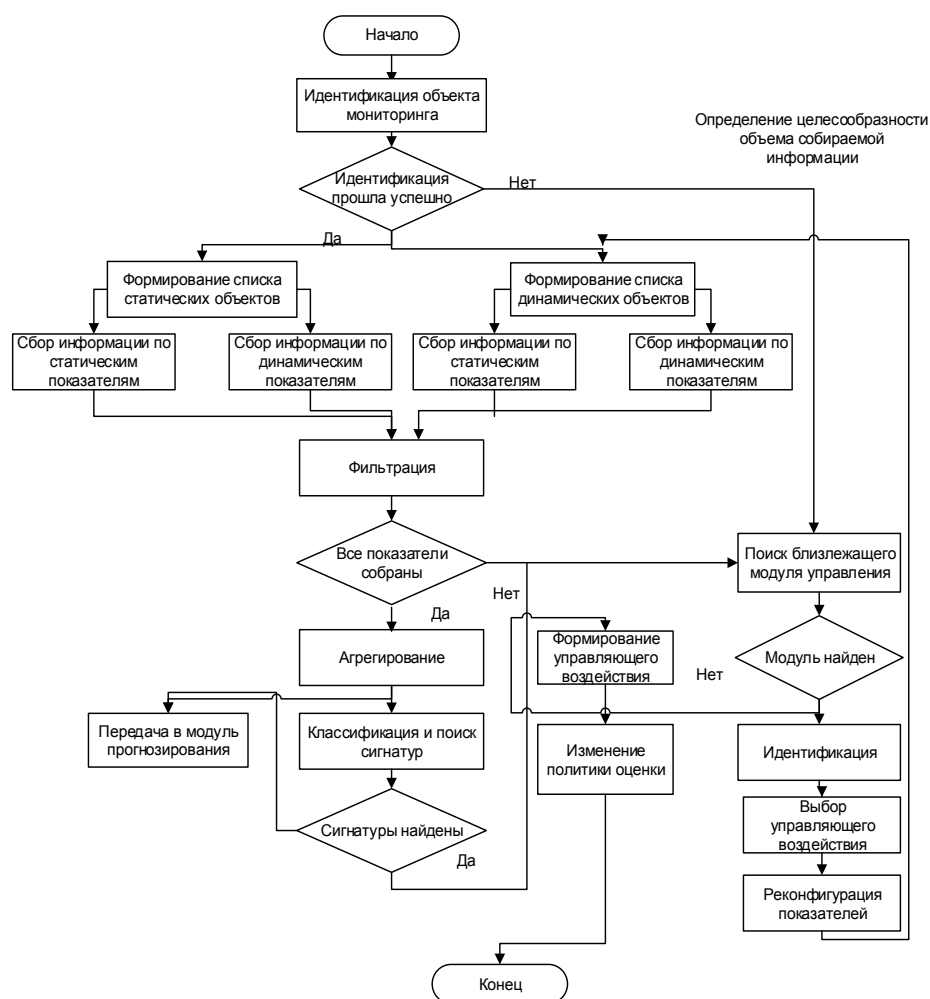


Рис. 3. Алгоритм формирования системы мониторинга

3.5. Прогнозирование состояния (анализ и выбор алгоритма прогнозирования в зависимости от уровня, глубины, горизонта и изменения функции распределения, построение прогноза).

3.6. Выработка мероприятий по обеспечению информационной безопасности.

Заключение. Анализ результатов по структурно-параметрическому синтезу ПМО и операционных процессов, в них протекающих, продемонстрировал необходимость введения системы показателей, отражающих на каждом уровне структуры предприятия динамику изменения характеристик. Показано, что в интересах совершенствования выпуска изделий на предприятии целесообразно внедрение совокупности взаимосвязанных показателей достижения стратегических целей, позволяющих оценивать динамику взаимодействия объектов и производить реконфигурацию операционных процессов.

ЛИТЕРАТУРА

1. Воробьев В.И., Фаткиева Р.Р., Шичкина Ю.А. Автоматизация процесса корректировки регламентирующих документов в соответствии со стандартами информационной безопасности // Известия СПбГЭТУ «ЛЭТИ», № 3, 2016. С. 20–25.
2. Воробьев В.И., Фаткиева Р.Р., Евневич Е.Л., Марков В.С. Приведение результатов сетевых измерений информационной безопасности в соответствии с рекомендациями ФСТЭК на основе процедуры гармонизации // Управление экономическими системами: электронный научный журнал, № 12(84), 2015. С. 22–23.
3. ГОСТ Р 56875-2016. Информационные технологии (ИТ). Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 26.02.2016 N 81-ст; дата введения 2017-01-01.

R.R. Fatkueva, E.L. Evnevich (St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg)

Management of the Perimeter for Monitoring the Information Security of Industrial Facilities

Information security monitoring of industrial facilities is carried out with the participation of tools that generate sets of heterogeneous data, which is not always consistent with the use of various regulatory documents. The formation of safety characteristics based on the data of the monitoring perimeter and the determination of its safety level is most often carried out by calculating an integral indicator that does not sufficiently reflect certain aspects of safety. A method is proposed for harmonizing the interaction of PMO and forming a set of safety indicators based on the formalization of the description of the subject area and the unification of the data description scheme.