Целевые функции концептуальной модели адаптивного мониторинга комплексной безопасности в интересах противодействия социо-киберфизическим угрозам «умному городу»

И. В. Котенко[1,2], И. Б. Паращук[1,2]
[1]Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)
[2]Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
Санкт-Петербург, Россия
ivkote@comsec.spb.ru, parashchuk@comsec.spb.ru

***Аннотация*. Статья нацелена на исследование вопросов адаптивного мониторинга, который служит задачам противодействия комплексным угрозам безопасности «умному городу». Рассматриваются вопросы математической формулировки частных и обобщенной целевых функций в интересах формального описания проблемы адаптивного мониторинга комплексной безопасности сложных социо-киберфизических систем. Определяются уровни адаптации, описаны группы оптимизируемых параметров. Особое внимание уделяется параметрам в рамках процедур наблюдения, оценивания и прогнозирования комплексной безопасности.**

Ключевые слова: целевая функция; мониторинг; параметр; показатель качества; комплексная безопасность; состояние; наблюдение; оценивание; прогнозирование

I. Введение

Концепцию «умного города» («smart city», «города будущего») следует рассматривать как одно из направлений развития современных больших социо-киберфизических систем (Cyber-Physical-Social Systems, CPSS) и как новое поколение сетевых распределенных социальных, физических и кибернетических инфраструктур. Они нацелены на реализацию приоритетов научно-технологического развития России, на обеспечение высокого качества жизни людей за счет применения инновационных технологий, предусматривающих экономичное, экологичное и безопасное функционирование объектов «умного города» и использование городских систем жизнедеятельности [1–3].

Проблемы социо-киберфизической (Cyber-Physical-Social, CPS) безопасности «умного города» – проблемы комплексного использования совокупности методов и средств безопасности систем и сетей управления транспортом, коммерческих и государственных услуг, цифрового образования и электронного правительства, автоматизированных аграрных предприятий, средств массовой информации, компьютеризированных промышленных предприятий, энергетики, образования, медицины. Вплоть до каждого «умного дома», «умного офиса» и отдельного человека в «умном городе».

Характер современных угроз безопасности «умного города» усложняется – они могут обретать статус комплексных социо- и (или) кибер- и (или) физических угроз одновременно или в разных сочетаниях. Они могут исходить или от человека (группы людей) или от государства – в рамках концепции информационного (гибридного) противоборства между странами, нацеленного на поражение критических инфраструктур друг друга [4–6].

«Умный город» – взаимоувязанная по месту и во времени, в социальной, био- и технологической среде совокупность CPS подсистем жизнеобеспечения, здравоохранения, образования, транспорта и т.д. Поэтому к проблеме комплексности угроз добавляется проблема их многоуровневости. Она проявляется в том, что уровень угроз разный на разных пространственных, социальных, физических и кибернетических участках, а также в разных временных координатах функционирования «умного города».

К основным направлениям обеспечения противодействия CPS угрозам «умному городу», наряду с организационными мерами по обеспечению комплексной безопасности, мерами по обеспечению безопасности подсистемы управления CPS системой и управлением безопасностью, относят мониторинг комплексной безопасности.

При этом процедуры мониторинга CPS в интересах противодействия угрозам «умному городу» на современном этапе также должны быть комплексными, многоуровневыми и интеллектуальными. Чтобы обнаружить и распознать угрозы современному «умному городу», мониторинг безопасности должен быть адаптивным и оптимальным. Он должен охватывать

Это исследование было поддержано грантом РНФ (проект № 18-11-00302) в СПИИРАН.

социальную, кибернетическую и физическую сферу жизнедеятельности города одновременно.

II. Релевантные работы

Проблемам организации и синтеза оптимальных алгоритмов мониторинга сложных систем посвящен ряд работ [7–10]. Они направлены на повышение эффективности процедур наблюдения, оценивания и прогнозирования в рамках мониторинга систем подобного класса. Целевые функции находят применение как идентификаторы экстремальных задач [7, 8] при мониторинге безопасности. Но они не гарантируют высокой точности при оценке качества процесса безопасности. В работе [7] предложен подход, основанный на адаптивном мониторинге параметров безопасности. Однако такой подход требует рассмотрения вспомогательных процедур анализа с точки зрения адаптации, что не всегда возможно. В работе [8] изложен расширенный подход к сетевому мониторингу. Но этот подход применим для сетей связи, что сужает область применения. Работа [9] посвящена подходу к мониторингу, как к процедуре регистрации кибербезопасности. Но этот подход очень сложный для практической реализации в рамках адаптивных процедур.

Одним из основных критериев качества мониторинга комплексной безопасности (КБ) является адаптируемость (лат. adaptatio – приспособление) данного процесса. Это свойство мониторинга изменять свои режимы с целью сохранения, улучшения или приобретения новых характеристик в условиях воздействий изменяющейся среды [10]. Адаптивность процесса мониторинга характеризует его способность приспосабливать (согласовывать) алгоритмы своего поведения, структуру и функции к условиям существования, к непредвиденным изменениям свойств КБ, целей КБ, задач управления КБ и окружающей среды путем смены режима или поиска оптимальных методов наблюдения, оценивания и прогнозирования (НОП) [10].

III. Теоретическая часть – общая формулировка задачи

Основное содержание концептуальной модели адаптивного мониторинга (АМ) КБ составляют ответы на вопросы: какие параметры КБ и (или) показатели качества (ПК) свойств КБ, как (в соответствии с какими критериями и на основе каких методов) и когда наблюдать, оценивать и прогнозировать на различных этапах жизненного цикла CPSS и в различных условиях обстановки. А также возможные пути и методы приспособления (согласования) режимов мониторинга КБ в условиях конструктивных и деструктивных воздействий. Концептуальная модель АМ КБ представляет собой формальное обобщенное описание системы взглядов, идей и принципов, определяющих общую методологию адаптивного мониторинга систем такого класса. Известно, что мониторинг представляет собой комплекс процедур НОП системных характеристик КБ. Используя подходы теории декомпозиции, будем рассматривать адаптацию данных процедур последовательно, исходя из специфических условий их реализации и опираясь на критерии оптимизации, присущие данным процедурам.

Итак, имеется объект мониторинга – КБ. Она подвержена влиянию внешних конструктивных и деструктивных факторов – окружающая среда; цели функционирования и применения, определяемые метасистемой и т.д. И внутренних факторов – количество потребителей услуг КБ и их требования; текущие цели управления КБ; управляющие воздействия; поток отказов элементов КБ и поток восстановления системных ресурсов; интенсивность потока инцидентов КБ и т.д.).

Элементами автоматизированной системы управления (АСУ) КБ являются система технической эксплуатации (СТЭ) и система принятия решений (СПР) [11]. Подсистема измерений входит в состав СТЭ АСУ КБ. Она реализует комплекс технических, системных и технико-технологических измерений, причем технические измерения составляют основу процесса технической диагностики КБ. Результатом технической диагностики является вектор текущих диагностируемых параметров $\vec{Y}_{\text{дп}}(k)$ КБ. Он представляющий собой набор данных измерения параметров технического состояния элементов КБ. Комплекс системных и технико-технологических измерений реализуется непосредственно в интересах мониторинга КБ, результатом его реализации является вектор текущих измеряемых параметров системных характеристик КБ $\vec{Y}_{\text{ип}}(k)$ – набор данных о результатах измерений параметров существенных свойств КБ в целом.

IV. Формулировка целевых функций

Реализация сбора по каналам наблюдения перечисленных данных, их обработка (систематизация, обобщение) является задачей процедуры наблюдения (ПН) в рамках АМ КБ. Сбор данных осуществляется на первом уровне адаптации, когда оптимизируются параметры ПН. Однако, перечень и номенклатура наблюдаемых параметров КБ $\vec{Y}^{\text{н}}_{\text{п}}(k)$ должны быть оптимизированы (адаптированы) в соответствии с требованиями текущих задач управления КБ. Они должны соответствовать объему и номенклатуре параметров и ПК, оценочные значения которых необходимы АСУ на данном шаге реализации КБ для принятия информационного решения о состоянии (качестве) безопасности. С этой целью, на втором уровне, когда в рамках АМ оптимизируются параметры процедуры оценивания (ПО), принимается решение по выбору (формированию) оптимальной системы оцениваемых параметров (СОП) КБ:

$$F_{\text{СОП}}(k): \rightarrow \underset{\substack{\varpi(k)\in\Omega;\vec{v}(k)\in V;\\ \vec{Y}'_{\text{п}}(k)\in\vec{Y}^{\text{н}}_{\text{п}}(k)}}{opt} f(\vec{Y}'_{\text{п}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\vec{v}(k)\in V;\\ \vec{Y}'_{\text{п}}(k)\in\vec{Y}^{\text{н}}_{\text{п}}(k)}}{opt} f(q_{\text{п}}(k); s_{\text{п}}(k); \Delta\tau_{\text{п}}(k)); \quad (1)$$

$$q_{\text{п}}(k) \in Q_{\text{п}};\ s_{\text{п}}(k) \in S_{\text{п}};\ \Delta\tau_{\text{п}}(k) \in \Delta T_{\text{п}}, \qquad (2)$$

где в выражении (1) $f(\vec{Y}'_{\text{п}}(k))$ – функция выбора оптимального вектора параметров $\vec{Y}'_{\text{п}}(k)$, которые необходимо НОП на k-ом шаге мониторинга КБ. Наблюдать, оценивать и прогнозировать нужно с учетом: факторов неопределенности $\varpi(k)$, принадлежащих множеству неопределенности Ω; факторов внешних и внутренних воздействий (вектора воздействий) $\vec{v}(k)$ на систему, принадлежащих множеству возможных воздействий (матрице воздействий) V (окружающая среда, условия эксплуатации и т.д.); объема и номенклатуры параметров, необходимых АСУ КБ $\vec{Y}'_{\text{п}}(k) \in \vec{Y}^{\text{н}}_{\text{п}}(k)$. На данном шаге осуществляется адаптация, имеющая целью поиск оптимальных (2): $q_{\text{п}}(k)$ – объема системных параметров КБ, которые необходимо НОП на k-ом шаге мониторинга, принадлежащих множеству возможных системных параметров КБ $Q_{\text{п}}$; $s_{\text{п}}(k)$ – номенклатуры (структуры, иерархии) системных параметров КБ, которые необходимо НОП на k-ом шаге мониторинга, принадлежащих множеству возможных наборов (номенклатур) системных параметров КБ $S_{\text{п}}$; $\Delta\tau_{\text{п}}(k)$ – периодичности НОП параметров КБ на k-ом шаге мониторинга, принадлежащей множеству возможных интервалов НОП $\Delta T_{\text{п}}$.

Результатом реализации АМ КБ на данном шаге является оптимальный для данных условий вектор параметров $\vec{Y}'_{\text{п}}(k)$, которые необходимо НОП на k-ом шаге мониторинга комплексной безопасности. Элементы данного вектора используются в дальнейшем для реализации процедур НОП состояния (качества) КБ.

Определив, какие параметры нужно наблюдать, адаптируются параметры ПН. Этот этап реализуется в соответствии с целевыми функциями (3) при условиях (4):

$$\begin{aligned} F_{\text{ПН}}(k) :\rightarrow & \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r'(k)\in R'\\ \vec{Y}_{\text{п}}(k)\in\vec{Y}_{\text{нп}}(k)\in\vec{Y}'_{\text{п}}(k)}}{opt} f(\vec{Y}'_{\text{нп}}(k)) = \\ = & \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r'(k)\in R'\\ \vec{Y}_{\text{п}}(k)\in\vec{Y}_{\text{нп}}(k)\in\vec{Y}'_{\text{п}}(k)}}{opt} f(q_{\text{нп}}(k); s_{\text{нп}}(k); \Delta\tau_{\text{нп}}(k); \end{aligned} \qquad (3)$$

$$q_{\text{нп}}(k) \in Q_{\text{нп}};\ s_{\text{нп}}(k) \in S_{\text{нп}};\ \Delta\tau_{\text{н}}(k) \in \Delta T_{\text{н}};\ m_{\text{н}}(k) \in M_{\text{н}}, \qquad (4)$$

где $f(\vec{Y}'_{\text{нп}}(k)$ в выражении (3) – функция выбора оптимального вектора наблюдаемых параметров $\vec{Y}_{\text{нп}}(k)$ на k-ом шаге мониторинга КБ с учетом ряда факторов. Факторы: неопределенности $\varpi(k)$; воздействий $\vec{v}(k)$; ошибок измерения и диагностики $r'(k)$, принадлежащих множеству возможных ошибок такого класса R', а также объема и номенклатуры реально наблюдаемых системных параметров $\vec{Y}_{\text{п}}(k) \in \vec{Y}_{\text{нп}}(k) \in \vec{Y}'_{\text{п}}(k)$. Это параметры, наблюдение за которыми реально осуществимо и принадлежит множеству (вектору) $\vec{Y}'_{\text{п}}(k)$ параметров, в оценочных значениях которых нуждается АСУ КБ. В общем случае, выражение (4), на данном шаге адаптации происходит поиск оптимальных: $q_{\text{нп}}(k)$ и $s_{\text{нп}}(k)$ – объема и номенклатуры наблюдаемых на k-ом шаге мониторинга параметров КБ, $\Delta\tau_{\text{н}}(k)$ – периодичности наблюдения параметров на k-ом шаге мониторинга, принадлежащей множеству возможных интервалов наблюдения $\Delta T_{\text{н}}$; $m_{\text{н}}(k)$ – методов (режимов) наблюдения на k-ом шаге мониторинга параметров КБ, принадлежащих множеству возможных режимов наблюдения $M_{\text{н}}$.

Результатом АМ на данном уровне адаптации является оптимальная для данных условий СОП КБ, т.е. вектор существенных системных параметров КБ, подлежащих оцениванию, элементы которого принадлежат множеству (вектору) наблюдаемых параметров $\vec{Y}_{\text{п}}(k) \in \vec{Y}_{\text{нп}}(k)$ системных свойств КБ. Элементы вектора $\vec{Y}_{\text{п}}(k)$ используются в дальнейшем для реализации синтеза оптимальной системы показателей качества (СПК) КБ, реализации процедур оценивания и прогнозирования состояния (качества) комплексной безопасности CPSS.

Реализация процесса формирования оптимальной СПК, получения частных и обобщенных оценочных значений параметров (состояния) или качества КБ, является задачей ПО в рамках АМ безопасности. На этом уровне адаптации параметров ПО выполняется двухэтапная оптимизация: вначале решается задача получения оптимальной для данных условий, состоятельной и не избыточной СПК, затем принимается решение по выбору оптимального для данных условий метода оценивания состояния (качества) КБ. Процедура оптимизации объема и номенклатуры СПК в рамках АМ КБ может быть реализована в соответствии с целевой функцией (5) при условиях (6):

$$\begin{aligned} F_{\text{СПК}}(k) :\rightarrow & \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r''(k)\in R''\\ \vec{Y}_{\text{п}}(k)\in\{Y_{\text{п}}\}}}{opt} f(\vec{Y}_{\text{пк}}(k)) = \\ = & \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r''(k)\in R''\\ \vec{Y}_{\text{п}}(k)\in\{Y_{\text{п}}\}}}{opt} f(q_{\text{пк}}(k); s_{\text{спк}}(k); \vec{Y}_{\text{кпк}}(k)); \end{aligned} \qquad (5)$$

$$q_{\text{пк}}(k) \in Q_{\text{пк}};\ s_{\text{спк}}(k) \in S_{\text{спк}};\ \vec{Y}_{\text{кпк}}(k) \in \{Y_{\text{кпк}}\}, \qquad (6)$$

где $f(\vec{Y}_{\text{пк}}(k))$ – функция выбора оптимального (состоятельного и не избыточного) вектора $\vec{Y}_{\text{пк}}(k)$ ПК КБ. Эти показатели подлежат оцениванию с учетом факторов неопределенности $\varpi(k)$, факторов внешних и внутренних воздействий (вектора воздействий) $\vec{v}(k)$ на систему, ошибок измерения, диагностики и наблюдения $r''(k)$, принадлежащих множеству возможных ошибок данного класса R'' и состава элементов вектора параметров $\vec{Y}_{\text{кпк}}(k)$, элементы которого принадлежат множеству

возможных реально наблюдаемых параметров КБ $\{Y_{\text{кпк}}\}$. При этом в рамках АМ КБ принимается решение по выбору оптимального метода оценивания (МО) состояния (качества) КБ в соответствии с целевой функцией (7) и при условиях (8):

$$F_{\text{мо}}(k): \rightarrow \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r(k)\in R\\ \vec{Y}_{\text{п(пк)}}(k)\in\{Y_{\text{п(пк)}}\}}}{opt} f(m_{\text{ос(к)}}(k)) = \underset{\substack{\varpi(k)\in\Omega;\,\vec{v}(k)\in V;\\ r(k)\in R\\ \vec{Y}_{\text{п(пк)}}(k)\in\{Y_{\text{п(пк)}}\}}}{opt} f(\delta_{\text{ош}}(k);t_{\text{оц}}(k);\vec{Z}_{\text{оц}}(k)); \quad (7)$$

$$\delta_{\text{ош}}(k)\in\Delta_{\text{ош}};\ t_{\text{оц}}(k)\in T_{\text{оц}};\ \vec{Z}_{\text{оц}}(k)\in\{Z_{\text{оц}}\}. \quad (8)$$

На данном этапе адаптации осуществляется поиск оптимальных параметров ПО: $\delta_{\text{ош}}(k)$ – значения дисперсии ошибки оценивания параметров (ПК) на k-ом шаге мониторинга КБ, принадлежащего множеству возможных значений $\Delta_{\text{ош}}$, характеризует точность оценивания; $t_{\text{оц}}(k)$ – значения времени оценивания параметров (ПК) на k-ом шаге мониторинга, функционально связанного с периодичностью наблюдения и возможностями вычислительных средств по реализации задач оценивания с конкретной вычислительной сложностью, принадлежащего множеству возможных значений $T_{\text{оц}}$ и характеризующего своевременность оценивания; $\vec{Z}_{\text{оц}}(k)-$ элементов вектора затрат вычислительных ресурсов на осуществление процедуры оценивания параметров (ПК) на k-ом шаге мониторинга, принадлежащего матрице (множеству) вычислительных затрат $\{Z_{\text{оц}}\}$. Результатом реализации АМ на этом этапе является оптимальный для данных условий вектор оценок параметров или ПК, характеризующих общесистемные свойства КБ $\hat{\vec{Y}}_{\text{п}}(k);\hat{\vec{Y}}_{\text{пк}}(k)$. На основе оценок этих параметров принимаются административные и оперативно-технические решения по управлению КБ CPSS.

Кроме того, текущие оценочные значения состояния (качества) КБ являются отправной точкой, исходными данными для процедуры прогнозирования (ПП). Взаимосвязанную систему целевых функций АМ КБ можно записать в общем виде, как комплексную функцию совместной последовательной адаптации, имеющей целью оптимизацию параметров ПН, ПО и ПП в интересах управления КБ:

$$F_{\text{АМ}}(k): \rightarrow \{F_{\text{СОП}}(k)\}\cup\{F_{\text{ПН}}(k)\}\cup \cup\{F_{\text{ПО}}(k): \rightarrow \{F_{\text{СПК}}(k)\}\cup\{F_{\text{мо}}(k)\}\}\cup\{F_{\text{ПП}}(k)\}. \quad (9)$$

В данном случае, комплексная целевая функция АМ КБ может представлять собой объединение целевых функций адаптации параметров соответствующих процедур мониторинга (9): формирования СОП, необходимых АСУ $F_{\text{СОП}}(k)$ (1); ПН $F_{\text{ПН}}(k)$ (3) и (4), ПО $F_{\text{ПО}}(k)$, которая, в свою очередь, является объединением целевых функций оптимизации СПК КБ $F_{\text{СПК}}(k)$ (5) и (6), метода оценивания $F_{\text{мо}}(k)$ (7) и (8), а также целевой функции оптимизации параметров ПП состояния (качества) КБ.

V. Выводы

Таким образом, выражение (9) имеет физический смысл совместной динамической адаптации параметров комплекса процедур наблюдения, оценивания и прогнозирования (т.е. параметров мониторинга) состояния (качества) КБ CPSS в условиях воздействия изменяющихся эволюционных и эксплуатационных факторов.

Практическая реализация предложенной концептуальной модели, позволит, на наш взгляд, повысить эффективность системного мониторинга КБ CPSS. Это произойдет за счет повышения безызбыточности, достоверности и точности получаемых оценок и прогнозов состояния (качества) КБ, за счет снижения затрат ресурсов АСУ КБ, выделяемых в интересах контроля безопасности. Что, в свою очередь, позволит добиться снижения расходов финансовых, временных и иных управленческих ресурсов в процессе проектирования, разработки и эксплуатации систем КБ CPSS, а также повышения степени обоснованности принимаемых решений по управлению структурой, параметрами и режимами работы систем такого класса.

Список литературы

[1] Strategic Opportunities for 21st Century Cyber-Physical Systems. // Foundations for Innovation in Cyber-Physical Systems workshop. Chicago, IL, March 13-14, 2012. p. 231.

[2] Graham S., Baliga G., Kumar P.R. Abstractions, Architecture, Mechanism, and Middleware for Networked Control. // IEEE Transactions on Automatic Control, July 2009, vol. 54, no. 7, pp. 1490-1503.

[3] Lee E.A. Cyber-Physical Systems – Are Computing Foundations Adequate. // NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap. Austin, October 16-17, 2006, pp. 342-353.

[4] Ruiz J.F., Desnitsky V.A., Harjani R., Manna A., Kotenko I.V., Chechulin A.A. A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components // 20th International Euromicro Conference on Parallel, Distributed and Network-based Processing (PDP 2012). Garching/Munich, February, 2012. pp. 261-268.

[5] Desnitsky V.A., Kotenko I.V. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices. // Lecture Notes in Computer Science, 8708(1): 2014. pp.194–210.

[6] Kotenko I.V., Levshun D.S., Chechulin A.A.. Event correlation in the integrated cyber-physical security system. // Proceedings of the 2016 XIX IEEE International Conference on Soft Computing and Measurements (SCM-2016), IEEE, St. Petersburg, Russia, May 2016. pp. 484-486.

[7] Fry C., Nystrom M. Security Monitoring. – Sebastopol, USA, O'Reilly Media Inc., 2009. p. 227.

[8] Bejtlich R. The Practice of Network Security Monitoring. Understanding Incident Detection and Response./ Networking & Cloud Computing, 2013. p. 376.

[9] Creasey J., Glover I. Cyber Security Monitoring and Logging Guide. / CREST Published, 2015. p. 60.

[10] Parashchuk I.B. Parametrization principles of states space of Telecommunications network in the framework of formulation of problem of optimal adaptive networking monitoring. // Modern Science: Development Tendencies. VII International Science-Practical Conference. Part II. Krasnodar, 2014. pp. 142-144.

[11] Al-Shaer E., Ou X., Xie G. Automated Security Management. Berlin. Springer Science & Business Media. 2013. p. 187.