РАЗМЕЩЕНИЕ КОМПОНЕНТОВ СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Г.Б. Ходасевич, кандидат технических наук, доцент;
А.А. Панов. Санкт-Петербургский университет ГПС МЧС России

Рассмотрены вопросы, связанные с синтезом системы мониторинга информационного пространства МЧС России. Предложена методика построения такой системы на основе оценочной модели и методов размещения объектов в дискретных пространствах.

Ключевые слова: информационное пространство, угрозы безопасности, мониторинг, сеть массового обслуживания, размещение объектов

COMPONENT DISPOSITION OF MONITORING SYSTEM OF INFORMATION SPACE

G.B. Hodasevich; A.A. Panov.
Saint-Petersburg university of State fire service of EMERCOM of Russia

This article discusses problems connected with monitoring system of information space of EMERCOM of Russia synthesis. Constructive procedure of such a system based on using estimating model and methods of object disposition in discrete spaces.

Key words: information space, security threats, monitoring, mass service net, object disposition

В настоящее время активно разрабатывается концепция информационного пространства МЧС России [1]. Под этим сложным образованием понимают взаимосвязанную совокупность информационных ресурсов, ведущихся в интересах автоматизированного управления силами и средствами в операциях по предупреждению и ликвидации последствий чрезвычайных ситуаций. Рост угроз безопасности информационного пространства, в том числе и угроз внутреннего происхождения, ставит перед специалистами в области защиты информации задачу поиска их источников. Одним из направлений решения этой задачи выступает реализация мониторинга информационного пространства.

Мониторингом называют систему наблюдений и контроля, проводимых регулярно по определенной программе для оценки состояния контролируемой среды, анализа происходящих в ней процессов и своевременного выявления тенденций ее изменения [2]. Существенным атрибутом мониторинга, отличающим его от других видов наблюдения и контроля, например от аудита, является то, что мониторинг проводится в режиме реального времени [3]. Этот фактор имеет решающее значение при организации мониторинга в интересах обеспечения безопасности информации, поскольку задержки в обнаружении угроз чреваты серьезными последствиями.

Реализация мониторинга информационного пространства возможна при наличии аппаратно-программных комплексов, ориентированных на сканирование пространства с целью обнаружения «слабых» мест (уязвимостей) или признаков аномальной деятельности объектов безопасности. Такие комплексы получили название «сенсоры» [4]. Очевидно, что большой масштаб информационного пространства требует наличия множества подобных комплексов, каждому из которых выделяется некоторая часть пространства для мониторинга (рис. 1).

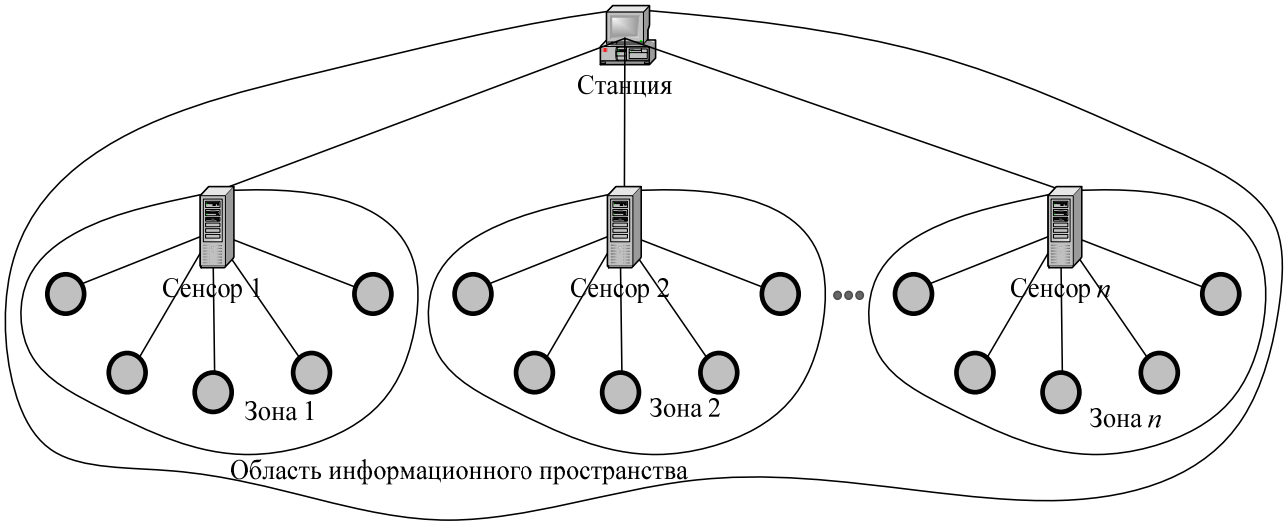

Рис. 1. **Структура системы мониторинга информационного пространства**

Данные мониторинга подлежат обработке на некоторых узлах (станциях), которые осуществляют сбор информации от нескольких сенсоров. При обнаружении признаков угроз безопасности эти станции решают задачу поиска мишеней в своей зоне информационного пространства с целью предварительного обоснования решения администратора безопасности на применение инструментальных средств обнаружения и нейтрализации выявленных источников угроз.

Модель для оценки системы мониторинга информационного пространства

Поскольку мониторинг должен выполняться в реальном времени, доминирующим свойством системы мониторинга признается оперативность. Это свойство можно оценить через суммарные временные задержки в реализации процедур контроля, которые складываются из следующих составляющих:

– задержки при передаче запросов от сенсоров к узлам информационного пространства;

– задержки при выполнении операций на узлах (сканирование портов, чтение системных журналов и т.п.);

– задержки при первичной обработке данных на сенсорах;

– задержки при обработке данных на станциях мониторинга.

Эти величины зависят от множества факторов и, следовательно, являются случайными величинами. Такое положение приводит к необходимости рассмотрения процесса мониторинга как случайного и исследования его в рамках теории вероятностей и теории массового обслуживания.

Стохастическая сеть массового обслуживания (СеМО), определяется следующей совокупностью характеристик:

1) множеством систем массового обслуживания (СМО) $\{S_1,S_2,...,S_n\}$, образующих сеть;

2) числом каналов $K_1,K_2,..,K_n$ в системах $S_1,S_2,...,S_n$, соответственно;

3) матрицей траекторий движения заявок $R=\|r_{ij}\|$, где r_{ij} – номер СМО, на которую переходит заявка, продвигающаяся по i-му пути на j-й фазе обслуживания при детерминированной процедуре маршрутизации, или матрицей вероятностей перехода заявок из одной СМО в другую $P=\|p_{ij}\|$, где p_{ij} – вероятность того, что заявка, покидающая S_i, поступает в S_j;

4) числом заявок, циркулирующих в замкнутой сети (Z);

5) интенсивностью источников заявок в разомкнутой сети $\Lambda=\{\lambda_i\}$, где i – адрес источника заявки;

6) законами распределения времени $F_1(t), F_2(t), \ldots, F_n(t)$ и дисциплинами обслуживания заявок в системах $S_1, S_2, \ldots, S_n$.

Системы $S_1, S_2, \ldots, S_n$ и связи между ними определяют структуру сети. Интенсивность источников заявок, интенсивность обслуживания, длины очередей и режим работы приборов характеризуют нагрузку и производительность СеМО.

Элементами, участвующими в мониторинге и представляющими различные СМО, являются (рис. 2):

– сенсоры (СМО 1);

– станции мониторинга (СМО 2);

– узлы информационного пространства (СМО 3);

– каналы передачи данных (СМО 4).

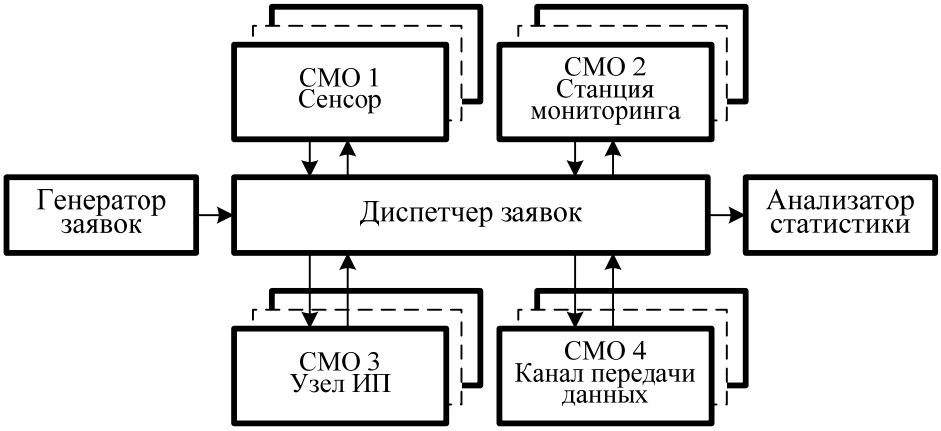

Рис. 2. **Представление процесса мониторинга в виде обслуживания заявок в СеМО**

Модель, представленная в виде СеМО, может быть исследована аналитическим или имитационным методами. Сравнительный анализ показывает, что метод имитационного моделирования при исследовании разработанной модели является более предпочтительным по следующим причинам:

1) большая размерность задачи, выступающая критическим фактором при построении аналитических моделей;

2) нарушение свойств стационарности, ординарности и отсутствия последействия входного потока в процессе обслуживания заявок в СМО, образующих СеМО, приводящее к тому, что входной поток заявок на очередной фазе обслуживания в сети (за исключением начальной) отличается от простейшего.

В результате моделирования возможно получение вероятностно-временных характеристик комплекса операций, связанных с мониторингом информационного пространства. Это позволяет оценить соответствие исследуемой системы требованиям, а при выявлении несоответствия – определить возможные направления модификации системы.

Метод размещения компонентов системы мониторинга информационного пространства

Построение системы мониторинга информационного пространства, осуществляемого в целях поиска источников внутренних угроз безопасности, требует определения числа и мест размещения компонентов этой системы. К наиболее важным и многочисленным компонентам следует отнести сенсоры. Насыщение информационного пространства большим количеством сенсоров приводит к существенному увеличению стоимости системы мониторинга. С другой стороны, снижение их числа относительно некоторого значения, способно привести к увеличению времени сбора и обработки информации мониторинга. В

такой ситуации возникает необходимость решения задачи размещения сенсоров в информационном пространстве.

Эта задача относится к классическим задачам размещения с дискретным пространством решений – задачам о покрытии множества, тоесть определения числа и мест размещения некоторых объектов [5]. Ее формулировка выглядит следующим образом.

найти

$$\min C = \sum_{j=1}^{n} c_j f_j \tag{1}$$

при ограничениях

$$\sum_{j=1}^{n} k_{ij} f_j \geq 1, \quad i = 1...m, \tag{2}$$

$$f_j = (0,1), \quad j = 1...n. \tag{3}$$

где k_{ij} – коэффициент покрытия, причем k_{ij} =1, если i-й узел информационного пространства располагается в пределах j-й зоны и k_{ij} =0 в противном случае; f_j =1, если в j-й зоне расположен некоторый сенсор и f_j =0 в противном случае. Указанные ограничения требуют, чтобы каждый из m узлов попадал в зону ответственности, по крайней мере, одного из n сенсоров. В этом случае цель состоит в том, чтобы обеспечить попадание узлов в зону ответственности с минимальными затратами, причем c_j – затраты на размещение сенсора в j-й зоне.

При этом i-й узел считается «покрытым» зоной ответственности j-го сенсора (j-й зоной), если время получения информации j-м сенсором от i-го узла не превышает некоторого допустимого значения t_0, т.е. $t_{ij} \leq t_0$.

Рассматриваемая задача является задачей целочисленного линейного программирования и может быть с помощью любого приемлемого метода [5–7]. Однако для ее решения разработан ряд методов, таких как методы неявного перебора, методы секущей плоскости, методы отсечения и эвристические методы [5].

Обычно задача о покрытии множества при решении проблемы размещения объектов состоит в определении минимального количества указанных объектов, которые удовлетворяют потребности множества потребителей. В этом случае задача (1–3) сводится к задаче о полном покрытии. Для этого полагают c_j =1, j=1…n.

В общей постановке решение задачи о покрытии множества состоит в определении минимального количества сенсоров, необходимых для удовлетворения (покрытия) потребностей некоторого заданного множества пользователей. Тогда решаемая задача является задачей о полном покрытии. На практике не всегда возможно разместить в сети такое количество сенсоров, которое полностью удовлетворяло бы потребности всех узлов (например, из-за ограничений на стоимость системы мониторинга). Обычно реальное количество сенсоров способно удовлетворить только некоторое подмножество узлов. Тогда целесообразно вести речь о частичном покрытии.

Если задача о полном покрытии состоит в определении минимального числа и мест размещения сенсоров, при котором своевременно удовлетворяются потребности всех узлов, то задача о частичном покрытии связана с определением размещения заданного сенсоров, при котором своевременно удовлетворяются потребности максимального числа узлов.

Математическое описание этой задачи представляется в следующем виде.

найти

$$\max Z = \sum_{i=1}^{m} \max k_{ij} f_i, \quad 1 \le j \le n, \tag{4}$$

при ограничениях

$$\sum_{j=1}^{n} f_j \le K, \tag{5}$$

$$f_j = (0,1), \quad j = 1...n. \tag{6}$$

где K – максимальное количество сенсоров, подлежащих размещению.

В выражении для целевой функции $\max k_{ij} f_i$ означает, что если некоторое место размещения узла информационного пространства накрывается более чем одним сенсором, то при вычислении Z учитывается только максимальная величина k_{ij}. Ограничения показывают, что в лучшем случае можно использовать K сенсоров для размещения. Если Z равно m – числу узлов, это означает, что величина K достаточно велика, чтобы удовлетворены были все потребители (узлы). Таким образом, задача о полном покрытии может быть сведена к задаче о частичном покрытии для различных значений K. В этом случае решение задачи (4)–(6) с наименьшим значением величины K для которого $Z=m$, будет оптимальным решением задачи о полном покрытии.

Методика построения системы мониторинга информационного пространства

Задача построения системы мониторинга информационного пространства МЧС России по своей сущности является задачей синтеза, направленной на отыскание структуры и параметров названной системы в зависимости от ее характеристик, значения которых определяются требованиями по оперативности выдачи результатов мониторинга.

Система мониторинга информационного пространства относится к классу сложных систем. Такое положение обязывает тщательно подходить к выбору методов ее синтеза, поскольку строгие формальные методы не всегда могут быть применимы в силу того, что они имеют ограниченную область использования, что связано с их ориентацией на узкий круг задач малой размерности с полностью формализуемыми характеристиками.

Основная проблема решения задач синтеза сложных систем состоит в их неоднозначности. Это объясняется необходимостью получения двух групп характеристик, первая из которых описывает структуру системы, а вторая – параметры ее элементов. Такая неоднозначность порождается в результате взаимозависимости характеристик обеих групп. Для ее устранения, тоесть для выделения некоторой альтернативы среди других используется принцип оптимальности. Последнее означает, что из допустимых вариантов решения задачи один признается более предпочтительным, чем остальные [8].

Правило предпочтения задается критерием оптимальности, формирование которого само по себе является нетривиальной задачей. Известные требования, предъявляемые к критерию оптимальности, носят общий характер и имеют высокую степень неопределенности [9].

Критерий оптимальности должен отражать различные факторы, влияющие на эффективность функционирования системы. Число этих факторов может быть довольно большим. Выделение множества значимых факторов в принципе может оказаться нереализуемым. Не менее сложной задачей является ранжирование факторов по их важности. В результате обе задачи решаются на основе опыта, знаний и интуиции.

Но даже если выделение значимых факторов возможно, то следствием этого является

очередная проблема. Если каждый подобный фактор рассматривать в качестве критерия, то задача синтеза становится многокритериальной, методы решения которой далеки от полной проработки [10]. Поэтому на практике такие задачи стремятся свести к однокритериальным, что достигается скаляризацией векторного критерия. К настоящему времени известны многие способы скаляризации. Однако отсутствуют строгие правила их выбора, соответственно успех решения задачи не всегда очевиден.

Решение задачи построения системы мониторинга информационного пространства с помощью точных математических методов, например, методов математического программирования, может встретить существенные трудности в силу, по крайней мере, двух причин. Во-первых, это высокая размерность задачи, определяемая необходимостью учета большого числа факторов. Во-вторых, невозможность исчерпывающей формализации ряда факторов и, как следствие, риск получения решения, не ориентированного на конкретную обстановку.

В такой ситуации рациональным представляется использование подхода, известного под названиями «итеративный синтез» или «синтез через анализ» [8]. Традиционный способ решения задач синтеза через анализ предполагает построение итеративной процедуры. В каждой итерации помимо расчета величины критерия проводится модификация очередного варианта построения системы, после чего вариант подвергается оценке.

Тогда методика построения системы мониторинга имеет структуру, представленную на рис. 3.

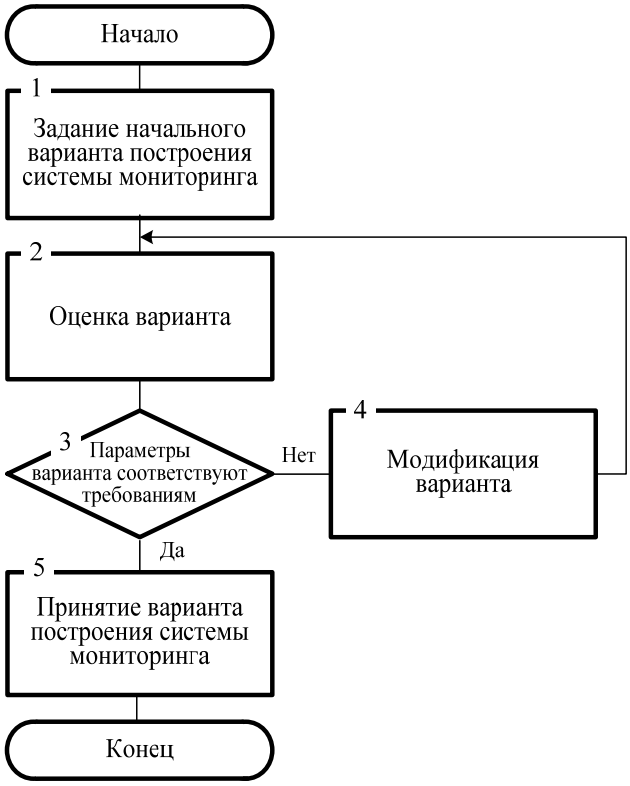

Рис. 3. **Структурное представление методики построения системы мониторинга в виде блок-схемы алгоритма**

Методика может быть представлена в виде некоторой последовательности этапов, каждый из которых направлен на решение частных задач по построению системы мониторинга.

Первый этап связан с формированием начального построения системы мониторинга информационного пространства.

На этом этапе осуществляется зонирование информационного пространства. Исходными данными для определения количества зон могут выступать ресурсы, выделяемые

на построение системы мониторинга, что позволяет рассчитать число сенсоров, допустимое для реализации. Формирование топологического построения каждой зоны и определение числа и положения ее узлов следует строить с учетом принадлежности узлов к автоматизированным системам или их территориальным подсистемам, входящим в информационное пространство. Если ресурсные ограничения отсутствуют, то решается задача о полном покрытии (1)–(3), в результате решения которой получают число сенсоров, требуемых для построения системы. Если же речь идет о частичном покрытии, то задаются некоторым допустимым к использованию числа $K' < K$ сенсоров и решают задачу (4)–(6) для определения максимального числа узлов, охватываемых системой мониторинга.

На *втором этапе* осуществляется оценка полученного варианта системы мониторинга.

Для этого строится модель системы в виде СеМО. Структура этой модели должна отражать структуру полученного на предыдущем этапе варианта системы мониторинга. Результатом моделирования выступают значения вероятностно-временных характеристик варианта системы.

Третий этап заключается в проверке соответствия полученных значений параметров системы мониторинга и их требуемых величин.

В случае недопустимо большого расхождения осуществляется переход к четвертому этапу методики. Если же расхождение укладывается в допустимые пределы, то рассматриваемый вариант системы мониторинга принимается в качестве окончательного результата.

Содержание *четвертого этапа* составляет изменение варианта построения системы мониторинга.

Для этого либо формируют отличное от предыдущего зоновое построение информационного пространства (при решении задачи о полном покрытии), либо увеличивают число сенсоров $K' = \left(K' + \Delta K\right) < K$, где $\Delta K = 1,2,...$ (при решении задачи о частичном покрытии).

Разработанная методика построения системы мониторинга рекомендуется к применению должностными лицами, ответственными за разработку и сопровождение комплексной системы обеспечения безопасности информационного пространства МЧС России, в частности, средств защиты от угроз внутреннего происхождения.

Методика может быть использована на всех стадиях жизненного цикла систем и средств защиты информации. Так на стадии проектирования она может выступать в качестве инструмента разработки требований к названным системам и средствам и формирования предварительных и рабочих решений на их построение. Также с помощью методики возможно проведение экспертизы проектных решений и формирование альтернативных вариантов.

На стадии эксплуатации методика может быть использована для выявления так называемых «слабых» мест в функционирующих системах и выработки рекомендаций по их устранению. В качестве дополнительного направления применения методики может быть указана ее реализация при формировании вариантов модификации ранее созданных систем защиты информации в автоматизированных системах с целью их адаптации к изменившимся условиям функционирования.

Выводы

Реализация мониторинга информационного пространства МЧС России требует построения соответствующей системы, способной к сбору и обработке данных о подозрительных объектах или процессах. В состав системы мониторинга предполагается включать аппаратно-программные комплексы, называемые сенсорами.

Существенный территориальный размах информационного пространства МЧС России определяет необходимость задействования при его мониторинге множества сенсоров. Это порождает задачу нахождения оптимального или близкого к нему (рационального) числа сенсоров и мест их размещения. Также предполагается, что мониторинг должен отвечать

требованиям оперативности осуществления контрольных функций и экономичности с точки зрения затрат на оборудование.

На основе предложенных в статье оценочной модели и методов размещения объектов разработана методика построения системы мониторинга информационного пространства, реализующая схему синтеза через анализ. Итеративная процедура методики позволяет находить приемлемый вариант структурного построения системы мониторинга с учетом требований по оперативности реализации контрольных функций.

Литература

1. Артамонов В.С., Кадулин В.Е., Козленко Р.Н. Информационное обеспечение государственной пожарно-спасательной службы в условиях чрезвычайных ситуаций // Вестник Санкт-Петербургского университета ГПС МЧС России. 2003. № 3. С.58–59.

2. Концепция создания Единой автоматизированной системы антикризисного управления жизнедеятельностью государства в условиях повседневной деятельности, предупреждения и ликвидации чрезвычайных ситуаций. М.: МЧС России, 2008. 137 с.

3. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003. 752 с.

4. Лукацкий А.В. Обнаружение атак. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2003. 608 с.

5. Исследование операций: в 2 т: пер. с англ. / Под ред. Дж. Моудера, С. Элмаграби. М.: Мир, 1981.

6. Куватов В.И., Величко Г.А. Исследование операций. Петродворец.: ВМИРЭ, 2000. 374 с.

7. Таха Х. Введение в исследование операций: в 2 кн: пер. с англ. М.: Мир, 1985.

8. Иванов А.Ю., Полковников С.П., Ходасевич Г.Б. Военно-технические основы построения и математическое моделирование перспективных средств и комплексов автоматизации. СПб.: ВАС, 1997. 419 с.

9. Системный анализ в управлении: учеб. пособ. / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин; под ред. А.А. Емельянова. М.:Финансы и статистика, 2002. 368 с.

10. Бусленко Н.П. Моделирование сложных систем. М.: Наука, 1978. 399 с.