УДК 654.026

ПОСТРОЕНИЕ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Чернов П.С.

ФГБОУ ВО «Пензенский государственный университет»
Пенза, Российская Федерация

Аннотация. Рассмотрена актуальная проблема построения информационно-измерительных комплексов и систем, защищенных от внешних угроз. Предложена математическая модель архитектуры таких комплексов и алгоритм ее оптимизации.
Ключевые слова: информационно-измерительная система, архитектура, защита информации.

CONSTRUCTION OF SECURE MEASURING AND CONTROL SYSTEMS

Chernov P.S.

Penza State University,
Penza, Russian Federation

Abstract. We discuss the problem of creating information-measuring complexes and systems protected from external threats. A mathematical model of the architecture and an algorithm for its optimization are proposed.
Key words: measurement system, architecture, information security.

Адрес для переписки: Чернов П.С., ул. Красная, 40, г. Пенза, 440026, Российская Федерация
e-mail: pvllvp@yandex.ru

Типичная информационно-измерительная и управляющая система (ИИУС) состоит из множества физических, логических и программных составляющих, каждая из которых является объектом интереса с точки зрения оптимизации технических характеристик и информационной безопасности.

В настоящее время к ИИУС предъявляются высокие требования к безопасности и защите информации, которая осуществляется на каждом из физических и логических уровней. Защита на физическом уровне обычно осуществляется шифрованием дисков системы хранения данных (СХД) и серверного оборудования (СО), защитой каналов связи центров обработки данных (ЦОД) и вычислительных кластеров (ВК). Основной проблемой является отсутствие отечественного оборудования и низкоуровневого ПО отечественной разработки для зарубежного оборудования (BIOS, UEFI, драйверы).

На следующем уровне происходит виртуализация физических ресурсов. В РФ она регламентируется ГОСТ Р 56938-2016 [1]. Стандартом рассмотрены такие угрозы как: атаки на гипервизор; атаки на защищаемые виртуальные устройства и виртуальные машины; угрозы выхода процесса за пределы виртуальной машины; угрозы несанкционированного доступа к данным за пределами зарезервированного адресного пространства; нарушения изоляции данных внутри виртуальной машины; нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия; перехвата управления гипервизором; угрозы неконтролируемого роста числа виртуальных машин или зарезервированных вычислительных ресурсов; угрозы несанкционированного внесения изменений в образы виртуальных машин; угрозы ошибок обновления гипервизора.

Средства администрирования и мониторинга следующего уровня иерархии представляют собой операционные системы и высокоуровневые программные средства не так сильно привязанные к аппаратной составляющей [2]. В РФ единственной операционной системой, имеющей сертификат ФСТЭК, является ОС Astra Linux. Реализуемая в настоящее время программа перехода на отечественное ПО подразумевает замену ОС семейства Windows на ОС Astra Linux и прикладное ПО под данную ОС.

Клиентские стационарные устройства также могут работать под управлением ОС Astra Linux. Для мобильных платформ полноценно заменить ОС Android на отечественное ПО пока не удается. Хотя существуют дистрибутивы Astra Linux под архитектуры ARM и Эльбрус и несколько альтернативных ОС, например, ОС Аврора, большая номенклатура быстро меняющихся аппаратных компонент зарубежного производства не позволяют оперативно разрабатывать драйвера для периферии и оперативно выпускать обновления ОС.

С малогабаритными интеллектуальными датчиками в плане импортозамещения ситуация обстоит несколько лучше. Существуют отечественные микроконтроллеры и операционные системы реального времени. Однако имеется и ряд проблем, таких как отсутствие единых стандартов.

Классические облачные решения связаны с задачами резервирования, скрытия внутренней сетевой инфраструктуры, приоретизации трафика, резервирования данных. Существует ряд проблем, возникающих при попытке построения защищенных ИИУС: отсутствие унифицированного протокола информационного взаимодействия; средств защиты информации, учитывающих специфику маршрутизации в современных беспроводных сетях;

доступа к распределенным информационным ресурсам и базам данных.

Архитектура оказывает огромное влияние на важнейшие технические характеристики ИИУС: защищенность, быстродействие, надежность, цена. Разработка архитектуры, которая удовлетворяет всем требованиям технического задания, является сложной задачей. Использование эвристического метода в настоящее время не оправдано, а поиск и оптимизацию архитектуры целесообразно проводить посредством математических методов системного анализа, которые в данном случае сводятся к многокритериальной оптимизации.

Предлагаемая модель архитектуры A ИИУС, описывается множеством ее узлов N и их взаимосвязей $R = \{N_i,N_j\}$, то есть представляет собой граф:

$$A = \{N_1, N_2, \dots, N_n, R_{12}, R_{13}, \dots, R_{mk}\}. \quad (1)$$

Сами узлы N_i могут быть достаточно сложными элементами, также описываемыми множеством:

$$N = \begin{Bmatrix} RT_1, RT_2, .., RT_n \\ CC_1, CC_2, \dots, CC_m \\ DC_1, DC_2, .., DC_k \end{Bmatrix}, \quad (2)$$

где RT_1-RT_n – маршрутизаторы; C_1–C_m – вычислительные кластеры; DC_1-DC_k – датацентры.

Архитектура может изменяться в некоторых пределах без изменения функционального назначения комплекса. Такими степенями свободы могут быть: количество узлов N, количество связей R, топология сети, распределение программного обеспечения по узлам, замена программного обеспечения узлов на альтернативное, замена аппаратной составляющей узлов, и др.

Таким образом, в рамках данной модели задача оптимизации сводится к поиску архитектуры A, удовлетворяющей наложенным ограничениям (цена, производительность, надежность и пр.), описываемым соответствующими целевыми функциями f:

$$\min\{f_1(A), f_2(A), \dots, f_n(A)\}. \quad (3)$$

Целевые функции представляют собой функции вида $mem{:}A\to\mathbb{N}$, $proc{:}A\to\mathbb{N}$, $stor{:}A\to\mathbb{N}$ и др. Где *mem*, *proc*, *stor* находят объемы памяти, хранилища, количество процессоров. Аналогично определяются функции, характеризующие связи между элементами: $bw{:}\{N_i,N_j\}\to\mathbb{R}$, $lat{:}\{N_i,N_j\}\to\mathbb{R}$, где *bw* и *lat* обозначают пропускную способность и временную задержку. В качестве критерия оптимальности предлагается использовать эффективность по Парето.

Особенностью таких систем является то, что на многие технические характеристики значительное влияние оказывает не только архитектура, но и работа отдельного узла, вплоть до оконечного датчика. У каждого элемента системы также имеется набор параметров по которым возможно проведение оптимизации вследствие чего перед поиском эффективности по Парето для архитектуры предлагается производить оптимизации узлов N по своим собственным критериям r и целевым функциям g:

$$\forall N \forall R \in A: \min\{g_1(\overline{r}), g_2(\overline{r}), \dots, g_n(\overline{r})\}. \quad (4)$$

Конкретный вид целевых функций f и g зависит от типа критерия и технических требований к системе. Так стоимость является простой суммой цен на комплектующие в то время как, например, критерий защищенности системы обычно является сложной функцией множества величин:

$$S = \sum_i p_i(A) = \sum_i\left(\sum_j p_i(N_j) + \sum_{jk} p_i(R_{jk})\right), \quad (5)$$

где p_i – вероятность реализации i-й угрозы при использовании архитектуры A, узла N, связи R между двумя узлами;

Для исследования математической модели и поиска оптимальной архитектуры предлагается использовать генетический эволюционный алгоритм, обобщенный вид которого приведен на рисунке 1.

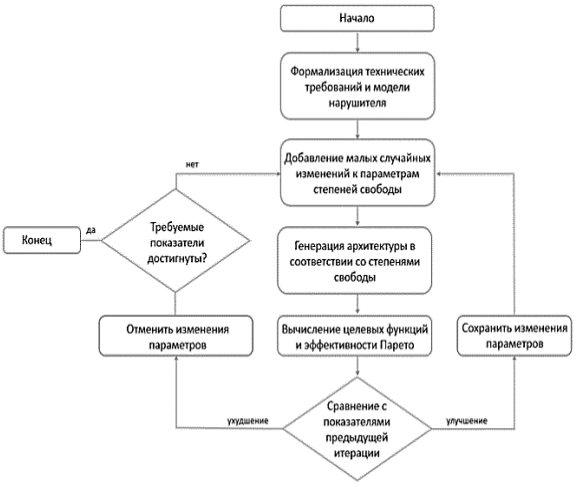

Рисунок 1 – Генетический алгоритм поиска оптимальной архитектуры

Литература

1. Защита информации при использовании технологий виртуализации : ГОСТ Р 56938-2016. – 2016.

2. Reese, G. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud / G. Reese. – O'Reilly Media. – 2009.