УДК 004.052
DOI: 10.21869/2223-1560-2019-23-1-118-129

Организация системы сетевого мониторинга и оценки состояния информационной безопасности объекта

Марухленко А. Л. [1] ✉, Селезнёв К. Д. [1], Таныгин М. О. [1], Марухленко Л. О. [1]

[1] ФГБОУ ВО «Юго-Западный государственный университет», Россия, 305040, Курск, ул. 50 лет Октября, 94

✉ e-mail: proxy33@mail.ru

Резюме

Цель исследования *заключается в построении модели системы для эффективного сбора информации об объекте сетевого доступа на базе современных методов защиты информации, а также в создании варианта среды реконфигурации в случае возникновения отказа элементов вычислительной сети или необходимости перераспределения серверной нагрузки.*

Методы. *Для процессов сбора информации об исследуемом объекте предложен гибкий, управляемый вариант построения системы, позволяющий в автоматизированном режиме выявлять потенциальные уязвимости в области информационной безопасности [1]. Предложено использование анализа состояния объекта на базе метода черного ящика, так как он позволяет воспроизвести действия внешнего злоумышленника, не имеющего информации об объекте на начальном этапе подготовки (что является наиболее распространенным сценарием при добавлении новых сервисов) и провести типовые атаки с последующей оценкой защищенности [2]. Предложена математическая модель, обеспечивающая повышение отказоустойчивости системы и балансирование нагрузки в масштабе реального времени.*

Результаты. *Итогом проведенных исследований является разработка эффективного построения системы для оценки состояния защищенности объекта. Разработана математическая модель, обеспечивающая возможность реконфигурации среды вычислительных модулей в масштабе реального времени. Проведены экспериментальные исследования, подтверждающие полноту и корректность предложенных решений.*

Заключение. *Предложенная система предназначена для анализа соответствия объекта защиты требованиям политики информационной безопасности, она включает в себя этапы системного анализа с использованием метода черного ящика и выполняет задачи автоматизированного процесса тестирования, распределенности компонентов системы, взаимозаменяемости модулей системы. В совокупности с разработанной математической моделью по повышению отказоустойчивости и перераспределения нагрузки на вычислительные мощности в случае сбоев работы оборудования и обходов, в случае полной загруженности элементов показала снижение времени на проведение комплексной оценки состояния информационной безопасности сетевого объекта доступа.*

Ключевые слова: *системный анализ; оценка защищенности; метод черного ящика; математическая модель; информационная безопасность; отказоустойчивость.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Организация системы сетевого мониторинга и оценки состояния информационной безопасности объекта / А.Л. Марухленко, К.Д. Селезнёв, М.О. Таныгин, Л.О. Марухленко // Известия Юго-Западного государственного университета. 2019. Т. 23, № 1. С. 118-129. **DOI:** 10.21869/2223-1560-2019-23-1-118-129.

UDC 004.052
DOI: 10.21869/2223-1560-2019-23-1-118-129

Arrangement of the System of Network Monitoring and Assessment of the State of Information Security of an Object

Anatoliy L. Marukhlenko [1]✉, Kirill D. Seleznyov [1], Maksim O. Tanygin [1], Leonid O. Marukhlenko [1]

[1] Southwest State University, 94, 50 Let Oktyabrya str., Kursk, 305040, Russian Federation

✉ e-mail: proxy33@mail.ru

Abstract

Purpose of reseach *is to develop a model of the system for effective collection of information about the network access object based on modern information protection methods as well as to create a kind of the reconfiguration environment in the event of a failure of computer network elements or the need to redistribute the server load.*

Methods. *A flexible, controlled version of developing a system has been proposed for the process of collecting information about the object under study; it makes it possible to automatically identify potential vulnerabilities in the field of information security [1]. It is proposed to use the analysis of the state of an object based on the black box technique, since it makes it possible to reproduce the actions of an external intruder who does not have any information about the object at the initial stage of preparation (which is the most common scenario when adding new services) and conduct typical attacks with subsequent security evaluation [2]. A mathematical model that improves system fault-tolerance and real-time load balancing is proposed.*

Results. *The result of the research is the development of an effective construction of a system for assessing the state of object security. A mathematical model that makes it possible to reconfigure the environment of computing modules in real time has been developed. Experimental studies confirming the completeness and correctness of the proposed solutions have been carried out.*

Conclusion. *The proposed system is designed to analyze the compliance of the protection object with the requirements of an information security policy; it includes the stages of system analysis using the black box technique and performs the tasks of an automated testing process, system components distributions, system modules interchangeability. Together with the developed mathematical model for improving fault-tolerance and redistributing the load on computational power in the event of equipment malfunctions and bypasses in the case of complete load of the elements, the system demonstrated a decrease in the time for conducting a comprehensive assessment of the information security state of the network access object.*

Key words*: system analysis; security assessment; black box technique; mathematical model; information security; fault-tolerance.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Marukhlenko A. L., Seleznyov K.D., Tanygin M. O., Marukhlenko L.O. Arrangement of the System of Network Monitoring and Assessment of the State of Information Security of an Object. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019: 23(1): 118-129 (in Russ.). **DOI:** 10.21869/2223-1560-2019-23-1-118-129.

***

Введение

Обзор современного состояния в области киберпреступности показал, что каждая вторая крупная организация сталкивается с целевыми атаками и обнаруживает следы присутствия злоумышленников в своей инфраструктуре. Стремительный рост числа атак связан с тем, что в качестве злоумышленника может выступать ботнет. Например, статистика атаки отказа в обслуживании по данным газеты РБК (рис. 1) в сфере совершения онлайн-платежей показывает увеличение числа нападений всего за один год более чем на 800 %.

Рис. 1. Динамика атак по отраслям в 2018 году (относительно 2017 г.)

Целью работы является построение варианта отказоустойчивой организации системы оценки состояния защищенности объекта сетевого доступа на базе целевых атак с использованием метода черного ящика. Как правило, первым этапом целевой атаки является сбор информации об инфраструктуре, сотрудниках и внешнем сетевом периметре атакуемой организации. В свою очередь, при анализе защищенности специалист по информационной безопасности (эксперт) имитирует действия злоумышленника, поэтому важно собрать как можно больше информации об исследуемом объекте, причем процесс сбора информации должен быть управляемым, гибким, распределенным и автоматизированным, так как в настоящее время компании имеют массивные и защищенные инфраструктуры, предотвращающие активные методы сканирования. Применение неавтоматизированных средств сбора информации об объекте влечет за собой существенное увеличение продолжительности и стоимости оценки, а так же, как правило, значительное снижение качества и применимости полученных результатов [3]. В связи с этим, построение отказоустойчивой модели системы, обеспечивающей вышеописанные требования, является актуальной задачей.

Задача оценки защищенности встает при вводе в эксплуатацию новой информационной системы, которая хранит важные данные или данные, доступ к которым должен быть разграничен [4]. Также к ее решению приходят при обнаружении попыток несанкционированного вторжения, при добавлении новых функций системы, изменения архитектуры среды и т.д. Для определения показателей, определяющих состояние

защищенности информационного объекта, необходимо проведение последовательного ряда этапов, а именно: сформулировать общую концепцию модели программного обеспечения, выбрать общие подходы к проектированию и заданию требований к модели программного обеспечения, формализовать элементы модели, формализовать общий вид модели и взаимосвязь элементов.

Материалы и методы решения задачи

Особенностью предлагаемой схемы построения системы для оценки защищенности объекта является использование легковесной виртуализации, которая позволяет изолированно запускать требуемые инструменты (сканеры портов, сканеры веб приложений и т.п.) для проведения анализа и сбора информации о внешнем периметре цели. С помощью контейнеров достигаются требуемые характеристики системы: горизонтальное масштабирование, изоляция инструментов, взаимозаменяемость инструментов и сетевых параметров, переносимость инструментов. Эксперт имеет возможность выстраивать логику процесса сбора информации, делая её индивидуальной для каждой системы. Для решения задачи контроля и распределенного запуска все контейнеры с инструментами объединяются в кластеры [5]. На рисунке 2 показан вариант построения системы.

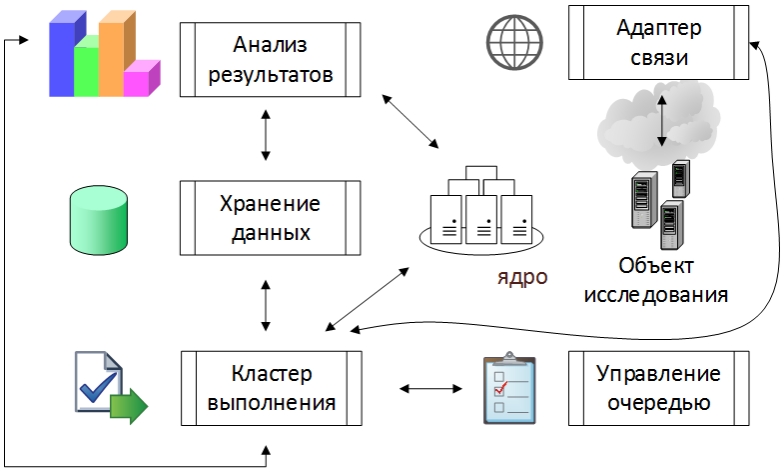

Рис. 2. Общая схема работы системы

В центре находится управляющий модуль ядра. Его основные функции: управление связанными элементами, задачами сканирования, формирование и изменение шаблонов для построения распределенного процесса сбора информации, отображение совокупности проанализированных данных результата выполнения задачи. Входными данными являются: список доступных контейнеров, информация о завершении работы текущей задачи, о завершении анализа результатов, шаблоны для процесса анализа защищенности, проанализированный результат работы задачи. Результатом работы модуля являются: данные об изменении работы контейнера (или

создании нового), шаблон с порядком и приоритетом запуска контейнеров.

При создании задачи для сканирования ядро предоставляет возможность создания шаблона для процесса сбора информации на основе доступных контейнеров в модуле кластера выполнения или выбор шаблона из модуля хранилища данных [6]. В шаблоне сбора информации указывается порядок и приоритет запуска контейнеров для модуля управления очередью, а также сетевой адаптер контейнеров для модуля адаптера связи. По завершении работы задачи, модуль ядра получает информацию от модуля управления очередью. Модуль ядра использует модель данных задачи сканирования, модель данных шаблона сканирования. Модель данных задачи должна содержать в себе шаблон выполнения подзадач (контейнеров) и сетевые адаптеры контейнеров. Модель шаблона сканирования должна содержать в себе порядок запуска контейнеров, их приоритеты, входные и выходные параметры.

Следующий элемент системы – модуль управления порядком запуска контейнеров (управление очередью). В функции данного модуля входят кроме создания очередей выполнения - контроль над их выполнением и оповещение в случае завершения. Входными данными являются: шаблон с порядком и приоритетом запуска контейнеров, информация о завершении работы определенного контейнера. Выходные данные – информация о завершении работы задачи (всех контейнеров в шаблоне сканирования). Модуль управления очередью взаимодействует с модулем ядра и модулем кластера выполнения. После создания задачи ядро отправляет шаблон с порядком и приоритетом запуска контейнеров модулю управления очередью, который обрабатывает полученные данные и передает команды в модуль кластера выполнения для параллельного или последовательного запуска соответствующих подзадач. По завершении работы контейнера модуль управления очередью получает соответствующую информацию от модуля кластера выполнения, а также оповещает модуль ядра при завершении последней подзадачи в шаблоне сканирования [7].

Функциями модуля кластера выполнения являются: создание, удаление, изменение контейнеров на основе команд, полученных от модуля ядра, получение и временное хранение результата работы контейнера, обработка информации о недоступности или нарушении сетевой связи с объектом исследования. Входными данными являются: информация о новом контейнере или изменении имеющихся контейнеров, параметры для запуска контейнера, информация о недоступности или нарушении сетевой связи с объектом исследования. Выходными данными являются: информация о наличии контейнеров в кластере, информация о завершении работы контейнера, результат работы контейнеров. При создании шаблона сканирования модуль ядра запрашивает доступные для использования контейнеры в модуле кластера выполнения и передает задачу в модуль управления очереди. После формирования последовательности сбора информации модуль управления очередью отправляет ко-

манды запуска с необходимыми параметрами модулю кластера выполнения.

Модуль адаптера связи используется для управления связью контейнеров с объектом исследования [8]. Функциями модуля адаптера связи являются построение инфраструктуры распределенного сетевого доступа. Входные данные – сетевые параметры контейнеров, выходные – информация о сетевой доступности объекта исследования. При запуске определенного контейнера кластер выполнения передает сетевые параметры адаптеру связи для формирования распределенного сетевого доступа к объекту исследования. В случае недоступности или нарушения связи формирует отчет с детализацией причины, передавая информацию модулю кластера выполнения. Модуль адаптера связи использует модель отчета недоступности или нарушения сетевой связи (с детализацией причины) [9].

Модуль анализа результатов сканирования производит анализ и обработку результатов работы контейнеров. Как правило, реализуется с использованием технологий и приемов статистического и корреляционного анализа или машинного обучения. Требованиями для модуля анализа результатов являются: скорость выполнения анализа, прослеживаемость выводов на основе результатов тестирования и достоверность представляемых данных в случае, если произошло зашумление данных или отказ элемента вычислительной среды.

Требованиями для модулей рассмотренной среды является отказоустойчивость, способность выдерживать высокие нагрузки при приеме входных и отправке выходных данных, возможность реализации гибко настраиваемых очередей задач за счет параллельных запусков подзадач [10].

Поток данных в широком смысле можно представить совокупностью каналов взаимодействия, по которым непрерывно передаются двоичные данные. При отказе на уровне адаптера связи или кластера выполнения необходимо разрешение проблемы обеспечения отказоустойчивой логической среды, позволяющей в том числе распараллелить однотипные блоки вычислителей. Учитывая, что каждый элемент кластера вычислений (сервер или виртуальная машина) выполняет однотипные функции – нет смысла хранить копии программных модулей в каждом элементе. Реконфигурация такой сети сводится к построению непересекающихся маршрутов от отказавших элементов к резервным, восстанавливающих логическую структуру или обход элементов, загруженность которых уже максимальна [11]. Критерием оптимальности при этом является минимизация длин маршрутов, что позволяет свести к минимуму временные задержки. В связи с этим, для обеспечения отказоустойчивой параллельной обработки нескольких блоков входного потока данных разработана универсальная среда элементов (ячеек), расположенных в узлах кристаллической решетки. Особенностью структурной организации среды кластера выполнения является наследование возможностей автоматической реконфигурации. Маршрут достижимости строится в соответствии с системой логических уравнений (1):

$$x_{1s}^{i,j-1,k} = \left(x_{11}^{ijk} \vee x_{12}^{ijk} \vee x_{13}^{ijk} \vee x_{14}^{ijk} \vee \right.$$
$$\left. \vee x_{15}^{ijk} \vee x_{16}^{ijk} \vee x_{r}^{ijk}\right) \cdot \bar{x}_{0}^{ijk} \cdot \bar{q}_{s}^{ijk}, \quad (1)$$

где x_{1s}^{ijk} – достижимость ячейки (ijk), s=1..6;

q_s^{ijk} – значение первого n-D-триггера ячейки (ijk), s=1..6;

x_r^{ijk} – резервная ячейка;

x_0^{ijk} – отказавшая ячейка.

В связи с тем, что необходимо исключить ситуации пересечения маршрутов перестройки введены специальные триггеры:

$$\begin{cases} D_1^{ijk} = x_{21}^{i,j-1,k} \cdot x_l^{ijk} \cdot \left(x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j,k-1} \vee x_{25}^{i,j,k+1} \vee x_{26}^{i,j+1,k}\right) \vee q_1^{ijk} \\ D_2^{ijk} = x_{22}^{i+1,j,k} \cdot \left(\begin{array}{l} (x_{23}^{i-1,j,k} \vee x_{24}^{i,j,k-1} \vee x_{25}^{i,j,k+1} \vee x_{26}^{i,j+1,k}) \cdot x_l^{ijk} \vee \\ (x_{23}^{i-1,j,k} \vee x_{24}^{i,j,k-1} \vee x_{25}^{i,j,k+1} \vee x_{21}^{i,j-1,k}) \cdot \bar{x}_l^{ijk} \end{array} \right) \vee q_2^{ijk} \\ D_3^{ijk} = x_{23}^{i-1,j,k} \cdot \left(\begin{array}{l} (x_{24}^{i,j,k-1} \vee x_{25}^{i,j,k+1} \vee x_{26}^{i,j+1,k}) \cdot x_l^{ijk} \vee (x_{24}^{i,j,k-1} \vee \\ x_{25}^{i,j,k+1} \vee x_{21}^{i,j-1,k}) \cdot \bar{x}_l^{ijk} \end{array} \right) \vee q_3^{ijk} \\ D_4^{ijk} = x_{24}^{i,j,k-1} \cdot \left((x_{25}^{i,j,k+1} \vee x_{26}^{i,j+1,k}) \cdot x_l^{ijk} \vee (x_{25}^{i,j,k+1} \vee x_{21}^{i,j-1,k}) \cdot \bar{x}_l^{ijk}\right) \vee q_4^{ijk} \\ D_5^{ijk} = x_{25}^{i,j,k+1} \cdot \left(x_{26}^{i,j+1,k} \cdot x_l^{ijk} \vee x_{21}^{i,j-1,k} \cdot \bar{x}_l^{ijk}\right) \vee q_5^{ijk} \\ D_6^{ijk} = x_{26}^{i,j+1,k} \cdot \bar{x}_l^{ijk} \cdot \left(x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j,k-1} \vee x_{25}^{i,j,k+1}\right) \vee q_6^{ijk}, \end{cases} \quad (2)$$

где D_n^{ijk} – функция установления значения n-D-триггера ячейки (ijk), где n=1..6.

Таким образом, модель реконфигурации задает правило обхода перегруженного или отказавшего элемента и примет вид:

$$\begin{cases} x_{21}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{11}^{ijk} \cdot \left(x_l^{ijk} \vee \bar{x}_l^{ijk} \cdot \bar{x}_{12}^{ijk} \cdot \bar{x}_{13}^{ijk} \cdot \bar{x}_{14}^{ijk} \cdot \bar{x}_{15}^{ijk} \cdot \bar{x}_{16}^{ijk}\right) \cdot \bar{x}_r^{ijk} \\ x_{22}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{12}^{ijk} \cdot \left(x_l^{ijk} \cdot \bar{x}_{11}^{ijk} \vee \bar{x}_l^{ijk} \cdot \bar{x}_{16}^{ijk}\right) \cdot \bar{x}_r^{ijk} \\ x_{23}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{13}^{ijk} \cdot \bar{x}_{12}^{ijk} \cdot \left(x_l^{ijk} \cdot \bar{x}_{11}^{ijk} \vee \bar{x}_l^{ijk} \cdot \bar{x}_{16}^{ijk}\right) \cdot \bar{x}_r^{ijk} \\ x_{24}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{14}^{ijk} \cdot \bar{x}_{12}^{ijk} \cdot \bar{x}_{13}^{ijk} \cdot \left(x_l^{ijk} \cdot \bar{x}_{11}^{ijk} \vee \bar{x}_l^{ijk} \cdot \bar{x}_{16}^{ijk}\right) \cdot \bar{x}_r^{ijk} \\ x_{25}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{15}^{ijk} \cdot \bar{x}_{12}^{ijk} \cdot \bar{x}_{13}^{ijk} \cdot \bar{x}_{14}^{ijk} \cdot \left(x_l^{ijk} \cdot \bar{x}_{11}^{ijk} \vee \bar{x}_l^{ijk} \cdot \bar{x}_{16}^{ijk}\right) \cdot \bar{x}_r^{ijk} \\ x_{26}^{ijk} = \left(x_0^{ijk} \vee x_{21}^{i,j-1,k} \vee x_{22}^{i+1,j,k} \vee x_{23}^{i-1,j,k} \vee x_{24}^{i,j+1,k} \vee x_{25}^{i,j,k-1} \vee x_{26}^{i,j,k+1}\right) \cdot \\ x_{16}^{ijk} \cdot \left(x_l^{ijk} \cdot \bar{x}_{11}^{ijk} \cdot \bar{x}_{12}^{ijk} \cdot \bar{x}_{13}^{ijk} \cdot \bar{x}_{14}^{ijk} \cdot \bar{x}_{15}^{ijk} \vee \bar{x}_l^{ijk}\right) \cdot \bar{x}_r^{ijk}, \end{cases} \quad (3)$$

где x_{2y}^{ijk} – передача функций, выполняемых y-ячейкой (ijk), y=1..6; x_l^{ijk} – расположение элемента (ijk) относительно резерва.

Результаты и их обсуждение

В соответствии с разработанной моделью, в рамках экспериментальных исследований проведены типовые проверки на базе метода черного ящика, включающие сканирование портов, подбор паролей, возможности инъекций в запросы к БД и т.д. Экспериментальный образец включает 8 серверов с одинаковыми мощностями. Результаты моделирования, динамика производительности системы показаны на рисунке 3, здесь за 99% производительности принимается уровень, соответствующий этапу полной загрузки до внесения искусственных изменений в режим работы вычислительной среды.

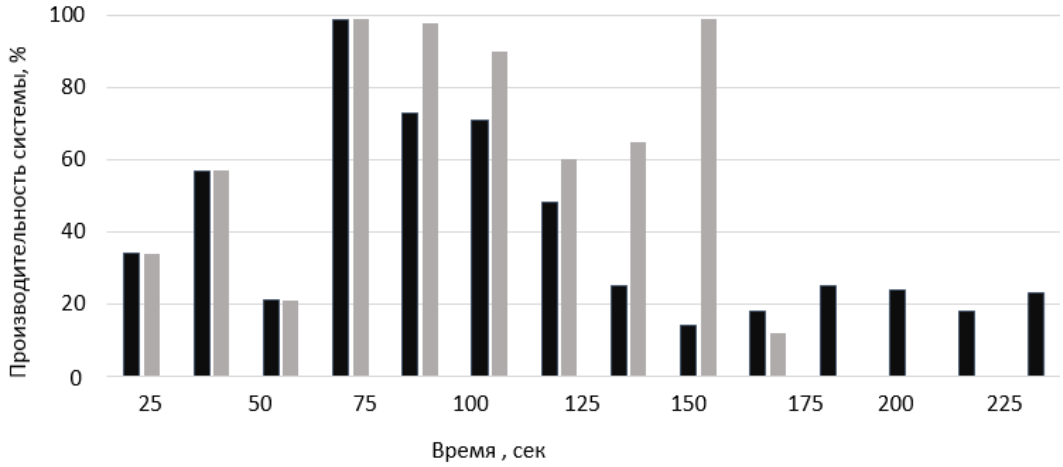

Рис. 3. Экспериментальные исследования

Из графика следует, что первые 50 секунд происходила плавная загрузка аппаратных ресурсов и на 75-секунде она завершилась успешной загрузкой вычислительных мощностей (5 серверов). Далее был отключен один из серверов – случай без использования модели реконфигурации (показан черным цветом) показал закономерное снижение производительности на 27 пунктов, а второй график остался на высоком уровне за счет переключения на свободный сервер. На 120 секунде 3 сервера были отключены (два резервных и 1 загруженный изначально) – в итоге падает производительность обоих графиков, т.к. нет резерва, но уровень отказоустойчивой системы остается выше [12]. На 150 секунде резервный сервер становится доступен, что обеспечивает рост производительности на сером графике, на 175 секунде загрузка которого составляет всего 12%, что ниже уровня черного графика. Это связано с тем, что ядро системы не дает новых задач и этап системного анализа завершен. Интеграл по мощности для эксперимента с отказоустойчивой средой превышает вариант без реконфигурации за счет периодических этапов опроса доступности оборудования и постоянной синхронизации.

Выводы

Предложенная система предназначена для анализа соответствия объекта защиты требованиям политики информационной безопасности, включает в себя этапы системного анализа с использованием метода черного ящика и выполняет задачи автоматизированного процесса тестирования, распределенности компонентов системы, взаимозаменяемости модулей системы. В совокупности с разработанной математической моделью по повышению отказоустойчивости и перераспределения нагрузки на вычислительные мощности в случае сбоев работы оборудования и обходов, в случае полной загруженности элементов показала снижение времени на проведение комплексной оценки состояния информационной безопасности объекта с привлечением пяти основных и трех резервных серверов на 23%, что особенно актуально в режиме мониторинга.

Список литературы

1. Марухленко А.Л., Мирзаханов П.С. Программный комплекс для моделирования процесса передачи и обработки сетевых потоков данных // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2012. № 2-3. С. 175-180.

2. Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, The late Shon Harris. Gray Hat Hacking: The Ethical Hacker’s Handbook, Fifth Edition. McGraw-Hill Education, 2018. 640 с.

3. Программно-аппаратный комплекс "токси+метео" для оценки последствий возможных аварий с учетом данных о текущих погодных условиях / А.А. Агапов, И.О. Хлобыстова, С.Л. Марухленко, А.Л., Марухленко А.С. Софьин // Безопасность труда в промышленности. 2011. № 1. С. 22-25.

4. Пат. RUS 2421805 РФ. Устройство поиска нижней оценки размещения в полносвязных матричных системах при двунаправленной передаче информации / Д.Б. Борзов, Е.О. Чеснокова, А.Л. Марухленко, М.М.Я. Аль-Ашвал. 24.11.2008.

5. Программный модуль для оценки криптостойкости симметричных методов шифрования с использованием параллельных вычислений / В.П. Добрица, А.Л. Марухленко, Л.О. Марухленко, А.В. Плугатарев // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 33-38.

6. Анализ потенциальных уязвимостей и современных методов защиты многопользовательских ресурсов / М.О. Таныгин, А.Л. Марухленко, Л.О. Марухленко, Е.Е. Конорева // Инфокоммуникации и космические технологии: состояние, проблемы и

пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 136-140.

7. Технология и программная реализация программного модуля для локализации потенциально опасных объектов на графической подложке с использованием нейронных сетей / М.О. Таныгин, А.Л. Марухленко, Л.О. Марухленко, А.Н. Романов // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 23-28.

8. Администрирование информационных систем / Д.О. Бобынцев, Л.А. Лисицин, А.Л. Марухленко, С.А. Кужелева. Курск, 2019. 201 с.

9. Разработка защищенных корпоративных систем на базе клиент-серверной технологии / М.А. Ефремов, Ю.А. Халин, А.Л. Марухленко, Л.О. Марухленко. Курск, 2018. 176 с.

10. Комплексная оценка информационной безопасности объекта с применением математической модели для расчета показателей риска / М.А. Ефремов, А.Л. Марухленко, А.В. Плугатарев, Л.О. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 34-40.

11. Вариант обеспечения информационной безопасности за счет повышения отказоустойчивости работы аппаратного межсетевого экрана / Л.О. Марухленко, А.Л. Марухленко, К.М. Керимбаева, А.А. Шамина // Инфокоммуникации и космические технологии: состояние, проблемы и пути решения: сборник научных статей по материалам II Всероссийской научно-практической конференции / отв. ред. В. Г. Андронов. Курск, 2018. С. 10-14.

12. Установление доверительного канала обмена данными между источником и приёмником информации с помощью модифицированного метода одноразовых паролей / М.О. Таныгин, Х.Я. Алшаиа, В.А. Алтухова, А.Л. Марухленко // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2018. Т. 8. № 4 (29). С. 63-71.

Поступила в редакцию 15.01.2019
Подписана в печать 07.02.2019

Reference

1. Maruhlenko A.L., Mirzahanov P.S. Programmnyj kompleks dlja modelirovanija processa peredachi i obrabotki setevyh potokov dannyh. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie*, 2012, no. 2-3, pp. 175-180.

2. Dr. Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, The late Shon Harris. Gray Hat Hacking: The Ethical Hacker’s Handbook, Fifth Edition. McGraw-Hill Education, 2018, 640 p.

3. Agapov A.A., Hlobystova I.O., Maruhlenko S.L., Maruhlenko A.L., Sof'in A.S. Programmno-apparatnyj kompleks "toksi+meteo" dlja ocenki posledstvij vozmozhnyh avarij s uchetom dannyh o tekushhih pogodnyh uslovijah. *Bezopasnost' truda v promyshlennosti*, 2011, no. 1, pp. 22-25.

4. Borzov D.B., Chesnokova E.O., Maruhlenko A.L., Al'-Ashval M.M.Ja. Ustrojstvo poiska nizhnej ocenki razmeshhenija v polnosvjaznyh matrichnyh sistemah pri dvunapravlennoj peredache informacii. Patent RF, no. 2421805, 24.11.2008.

5. Dobrica V.P., Maruhlenko A.L., Maruhlenko L.O., Plugatarev A.V. Programmnyj modul' dlja ocenki kriptostojkosti simmetrichnyh metodov shifrovanija s ispol'zovaniem parallel'nyh vychislenij. Infokommunikacii i kosmicheskie tehnologii: sostojanie, problemy i puti reshenija. Sbornik nauchnyh statej po materialam II Vserossijskoj nauchno-prakticheskoj konferencii. Kursk, 2018, pp. 33-38.

6. Tanygin M.O., Maruhlenko A.L., Maruhlenko L.O., Konoreva E.E. Analiz potencial'nyh ujazvimostej i sovremennyh metodov zashhity mnogopol'zovatel'skih resursov. Infokommunikacii i kosmicheskie tehnologii: sostojanie, problemy i puti reshenija. Sbornik nauchnyh statej po materialam II Vserossijskoj nauchno-prakticheskoj konferencii. Kursk, 2018, pp. 136-140.

7. Tanygin M.O., Maruhlenko A.L., Maruhlenko L.O., Romanov A.N. Tehnologija i programmnaja realizacija programmnogo modulja dlja lokalizacii potencial'no opasnyh ob#ektov na graficheskoj podlozhke s ispol'zovaniem nejronnyh setej. Infokommunikacii i kosmicheskie tehnologii: sostojanie, problemy i puti reshenija. Sbornik nauchnyh statej po materialam II Vserossijskoj nauchno-prakticheskoj konferencii. Kursk, 2018, pp. 23-28.

8. Bobyncev D.O., Lisicin L.A., Maruhlenko A.L., Kuzheleva S.A. Administrirovanie informacionnyh sistem. Kursk, 2019, 201 p.

9. Efremov M.A., Halin Ju.A., Maruhlenko A.L., Maruhlenko L.O. Razrabotka zashhishhennyh korporativnyh sistem na baze klientservernoj tehnologii. Kursk, 2018, 176p.

10. Efremov M.A., Maruhlenko A.L., Plugatarev A.V., Maruhlenko L.O. Kompleksnaja ocenka informacionnoj bezopasnosti ob#ekta s primeneniem matematicheskoj modeli dlja rascheta pokazatelej riska. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie*, 2018, vol. 8, no. 4 (29), pp. 34-40.

11. Maruhlenko L.O., Maruhlenko A.L., Kerimbaeva K.M., Shamina A.A. Variant obespechenija informacionnoj bezopasnosti za schet povyshenija otkazoustojchivosti raboty apparatnogo mezhsetevogo jekrana. Infokommunikacii i kosmicheskie tehnologii: sostojanie,

problemy i puti reshenija. Sbornik nauchnyh statej po materialam II Vserossijskoj nauchno-prakticheskoj konferencii. Kursk, 2018, pp. 10-14.

12. Tanygin M.O., Alshaia H.Ja., Altuhova V.A., Maruhlenko A.L. Ustanovlenie doveritel'nogo kanala obmena dannymi mezhdu istochnikom i prijomnikom informacii s pomoshh'ju modificirovannogo metoda odnorazovyh parolej. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie*, 2018, vol. 8, no. 4 (29), pp. 63-71.

Received 15.01.2019

Accepted 07.02.2019

Информация об авторах / Information about the Authors

Анатолий Леонидович Марухленко, кандидат технических наук, доцент, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация
e-mail: proxy33@mail.ru

Anatoliy L. Marukhlenko, Candidate of Engineering Sciences, Associate Professor, Southwest State University, Kursk, Russian Federation
e-mail:proxy33@mail.ru

Кирилл Дмитриевич Селезнёв, студент, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: mhmwq10@gmail.com

Kirill D. Seleznev, Student, Southwest State University, Kursk, Russian Federation
e-mail: mhmwq10@gmail.com

Максим Олегович Таныгин, кандидат технических наук, доцент, завкафедрой информационной безопасности, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: tanygin@yandex.ru

Maksim O. Tanygin, Candidate of Engineering Sciences, Associate professor, Head of the Department of Information Security, Southwest State University, Kursk, Russian Federation
e-mail: tanygin@yandex.ru

Леонид Олегович Марухленко, старший преподаватель, ФГБОУ ВО «Юго-Западный государственный университет», г. Курск, Российская Федерация, e-mail: leonid.marukhlenko@mail.ru

Leonid O. Marukhlenko, Senior Lecturer, Southwest State University, Kursk, Russian Federation
e-mail:leonid.marukhlenko@mail.ru