REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 5, Number 315 (2017), 28 – 37

B. Ahmetov[1], A. Korchenko[2], Zh. Alimseitova[3], N. Zhumangalieva[3]

[1]International Kazakh-Turkish University named after H. A. Yasavi, Turkestan, Kazakhstan
[2]National aviation University, Kiev, Ukraine;
[3]Kazakh national research technical University named after K. I. Satpayev, Almaty, Kazakhstan

A SYSTEM FOR IDENTIFYING ABNOPRMAL STATE IN INFORMATIONAL SYSTEMS

Abstract. Computer systems are increasingly exposed to impacts of threats, new types of which give rise to new cyber attacks on their resources. For increasing the security level it needs appropriate special counteraction that can be effective in the emergence of new types of threats and allow in fuzzy terms to identify cyber attacks targeted at a variety of resources of informational systems. There are a number of models, methods and approaches used for solving protection tasks in fuzzy conditions. For their effective implementation it requires an appropriate system implements technology to identify the abnormal condition. For this aim a system focused on the tasks detect cyber attacks in the informational systems, which is based on mathematical models and methods of fuzzy logics and is implemented through sub-systems: the formation of fuzzy standards, the formation of decision rules, primary processing, as well as modules: fuzzy arithmetic, logical deduction, visualization and control module.

Keywords: cyberattacks, anomalies, intrusion detection system, anomaly detection systems, intrusion detection system.

УДК 004.056.53(045)

Б.Ахметов[1], А.Корченко[2], Ж.Алимсеитова[3] , Н.Жумангалиева[3]

[1]Международный казахско-турецкий университет имени Х.А. Ясави, Туркестан, Казахстан
[2]Национальный авиационный университет, Киев, Украина;
[3]Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан

СИСТЕМА ВЫЯВЛЕНИЯ АНОМАЛЬНОГО СОСТОЯНИЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация. Компьютерные системы все больше подвергаются воздействиям угроз, новые виды которых порождают новые кибератаки на их ресурсы. Для повышения уровня безопасности необходимы соответствующие специальные средства противодействия, которые способны оставаться эффективными при появлении новых видов угроз и позволяющие в нечетких условиях выявить кибератаки, ориентированные на множество ресурсов информационных систем. Известны ряд моделей, методов и подходов, используемые для решения задач защиты в нечетких условиях. Для их эффективного применения необходима соответствующая система реализующая технологию выявления аномального состояния. С этой целью разработана система, ориентированная на решение задач выявления кибератак в информационных системах, которая базируется на математических моделях и методах нечеткой логики и реализуется посредством подсистем: формирования нечетких эталонов, формирования решающих правил, первичной обработки, а также модулей: нечеткой арифметики, логического вывода, визуализации и управляющего модуля. Система дает возможность эффективно выявлять определенные типы кибератак относительно конкретной среды окружения в заданный временной промежуток, а также позволит расширить функциональные возможности современных систем обнаружения вторжений за счет эффективной идентификации новых и несигнатурных типов кибератак.

Ключевые слова: кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак.

НОМЕНКЛАТУРА

I_i $(i=\overline{1,n})$ – идентификатор вторжений (intrusion); V_i $(i=\overline{1,m})$ – идентификатор величин (value); NVC – Numbers of Virtual channels; VCA – Virtual Channel Age; NCC – Number of concurrent connections to the server SPR – Speed of processing requests from the clients; SPR – Speed of processing requests from the clients; DBR – The delay between requests from the single user; NPSA – Number of packages with the same sender and receiver address; НЧ – нечеткое число; T_{ij} – множество термов отображаемое r НЧ, т.е. $T_{ij}=\bigcup_{f=1}^{r}\underset{\sim}{T}_{ij}^{f}=\{\underset{\sim}{T}_{jj}^{1},\ \ldots,\ \underset{\sim}{T}_{ij}^{r}\}$, $(f=\overline{1,r})$; $\underset{\sim}{T}_{ij}^{e}$ – эталонные нечеткие числа; $\underset{\sim}{T}_{ij}^{ef}$ – эталоны величин; $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{SPR}$, $\underset{\sim}{t}_{DBR}$, $\underset{\sim}{t}_{NPSA}$, $\underset{\sim}{t}_{NVC}$, $\underset{\sim}{t}_{VCA}$ – текущие значения величин.

I. АКТУАЛЬНОСТЬ

Использование систем выявления вторжений непосредственно связано со стремительным развитием киберпространства, в котором появляются новые виды угроз ресурсам информационных систем (РИС), например, такие как атаки 0-day и несигнатурные типы кибератак. Расширение воздействий кибератак, направленных на различные РИС, инициирует создание таких средств противодействия, которые способны оставаться эффективными при появлении новых видов угроз с неустановленными или нечетко определенными свойствами и фактически функционировать в слабоформализованной, нечеткой среде окружения [1]. Использование методов, моделей и систем, основанных на нечетких множествах [1–19] для построения средств обнаружения аномалий, порожденных реализацией киберугроз, позволит усовершенствовать существующие системы выявления вторжений в компьютерных системах и сетях. В этой связи, разработка соответствующих технических решений, функционирующих в нечетких условиях и позволяющих выявлять новые и модифицированные типы кибератак, является актуальной научной задачей.

II. АНАЛИЗ СУЩЕСТВУЮЩИХ ИССЛЕДОВАНИЙ

Известны отдельные, достаточно эффективные разработки, используемые для решения указанных задач выявления кибератак, например, такие как: нечеткие подходы к обнаружению вторжений [2, 3] и детектированию аномалий [4]; соответствующие нечеткие модели [1, 5], методы [6, 7]; технология [6]; системы обнаружения вторжений [8–15]; наборы нечетких правил [2, 3, 7, 9, 10, 12–17]; методы построения лингвистических переменных [16, 18] и нечетких эталонов [16], а также другие разработки, используемые для решения задач защиты в нечетких условиях [19]. Указанные исследования показали эффективность соответствующего применения математического аппарата нечетких множеств, а его использование для формализации подхода к выявлению кибератак, позволит усовершенствовать процесс создания соответствующих систем обнаружения вторжений. Однако в указанных работах нет структурированного подхода и обобщенного решения относительно построения соответствующих средств выявления вторжений.

III. ОСНОВНАЯ ЦЕЛЬ ИССЛЕДОВАНИЯ

Исходя из анализа существующих исследований и актуальности поставленной задачи, а также для эффективного применения известных моделей, методов, технологии [1, 5, 6] целью данной работы является разработка системы, реализующей технологию выявления аномального состояния для систем обнаружения вторжений, которую можно использовать для совершенствования средств сетевой безопасности, ориентированных на контроль активности в среде окружения.

С помощью такой системы (при решении задач выявления кибератак) можно эффективно выявлять определенные типы кибератак относительно конкретной среды окружения в заданный временной промежуток, а также расширить функциональные возможности современных систем обнаружения вторжений за счет эффективной идентификации новых (0-day) и несигнатурных типов кибератак.