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.

IV. ОСНОВНАЯ ЧАСТЬ ИССЛЕДОВАНИЯ

Для решения поставленной задачи предлагается система реализующая технологию выявления аномального состояния в информационных системах и сетях (СВАС), основу которой составляет ряд модулей и подсистем. Первая подсистема ориентирована на измерение текущих значений величин сетевого трафика, а вторая посредством формирования решающих правил (направленных на проверку истинности взаимосвязей эталонных и текущих величин, для оценивания сетевой активности), идентифицировать аномальное состояние. Система содержит:

1. Подсистему формирования нечетких эталонов (ПФНЭ) сетевых величин, ориентированную на получение всех необходимых термов для каждой нечеткой переменной [6] с целью измерения текущих значений сетевых величин, в которую входят:

1) регистр вторжений и величин (RGIV), предназначенный для приема и хранения текущих значений идентификаторов вторжений I_i $(i = \overline{1,n})$ и величин V_i $(i = \overline{1,m})$;

2) блок коммутации величин (БКV), осуществляющий формирование потоков величин соответствующих типу вторжения;

3) блок формирования пар вторжение и величины (БПIV), предназначенный для связывания пары идентификатора вторжения и соответствующих ему величин;

4) блок формирования совокупности термов (БФСТ), применяемый для генерирования заданного множества T_{ij}^{ef};

5) блок формирования эталонов (БФЭ), осуществляющий вычисление для каждого T_{ij}^{ef} соответствующего эталонного нечеткого числа (НЧ);

6) регистр эталонов (RGЭ), служащий для приема и временного хранения вычисленных эталонных НЧ;

7) процессор визуализации эталонов (ПВЭ), предназначенный для отображения в графическом виде полученных эталонных НЧ;

2. Подсистему формирования решающих правил (ПФРП), применяемую при создании множества правил для контроля сетевой активности [6], в которую входят:

1) регистр эталонов (RGЭ);

2) блок коммутации (БК), служащий для формирования потоков $\underset{\sim}{t}_j$ [1] на блок формирования сопряженных пар (БФСП);

3) БФСП, предназначенный для логического преобразования эталонных T_{ij}^{ef} [19];

4) блок ранжирования (БР), осуществляющий формирование коэффициентов важности (КВ);

5) блок инициализации правил (БИП), формирующий матрицы $FI(i, r_r)$ и $MP(i, r_r)$ [1];

6) базу правил (БП), служащую для хранения в соответствующих секторах данных ($СД_i$, $i = \overline{1,d}$) наборов правил SR_{ir_i} $(i = \overline{1,n})$ [1];

7) регистры текущих значений (RGTЗ) и нечетких идентификаторов (RGНИ), предназначенные соответственно для хранения в процессе всех вычислений значений $\underset{\sim}{t}$ и FI_i $(i = \overline{1,d})$;

8) регистр правил (RGП), предназначенный для приема и хранения подмножеств правил SR_i;

3. Подсистему первичной обработки (ППО), предназначенную для формирования множеств вторжений, величин и их фаззификации [6];

4. Модули нечеткой арифметики (МНА), логического вывода (МЛВ) и визуализации (МВ), предназначенные для формирования результата в нечетком и графическом представлении [6];

5. Управляющий модуль (УМ), служащий для управления коммутацией (УК), а также переводом системы в режим корректировки эталонов (РКЭ) и корректировки правил (РКП).

Система функционирует следующим образом (см. рис. 1).

На вход регистра вторжений (RGI) и регистра величин (RGV), обозначаемый RGIV ПФНЭ предварительно заносятся и хранятся на протяжении всего процесса вычислений соответственно текущие значения идентификаторов I_i $(i = \overline{1,n})$ и входных величин V_j $(j = \overline{1,m})$.

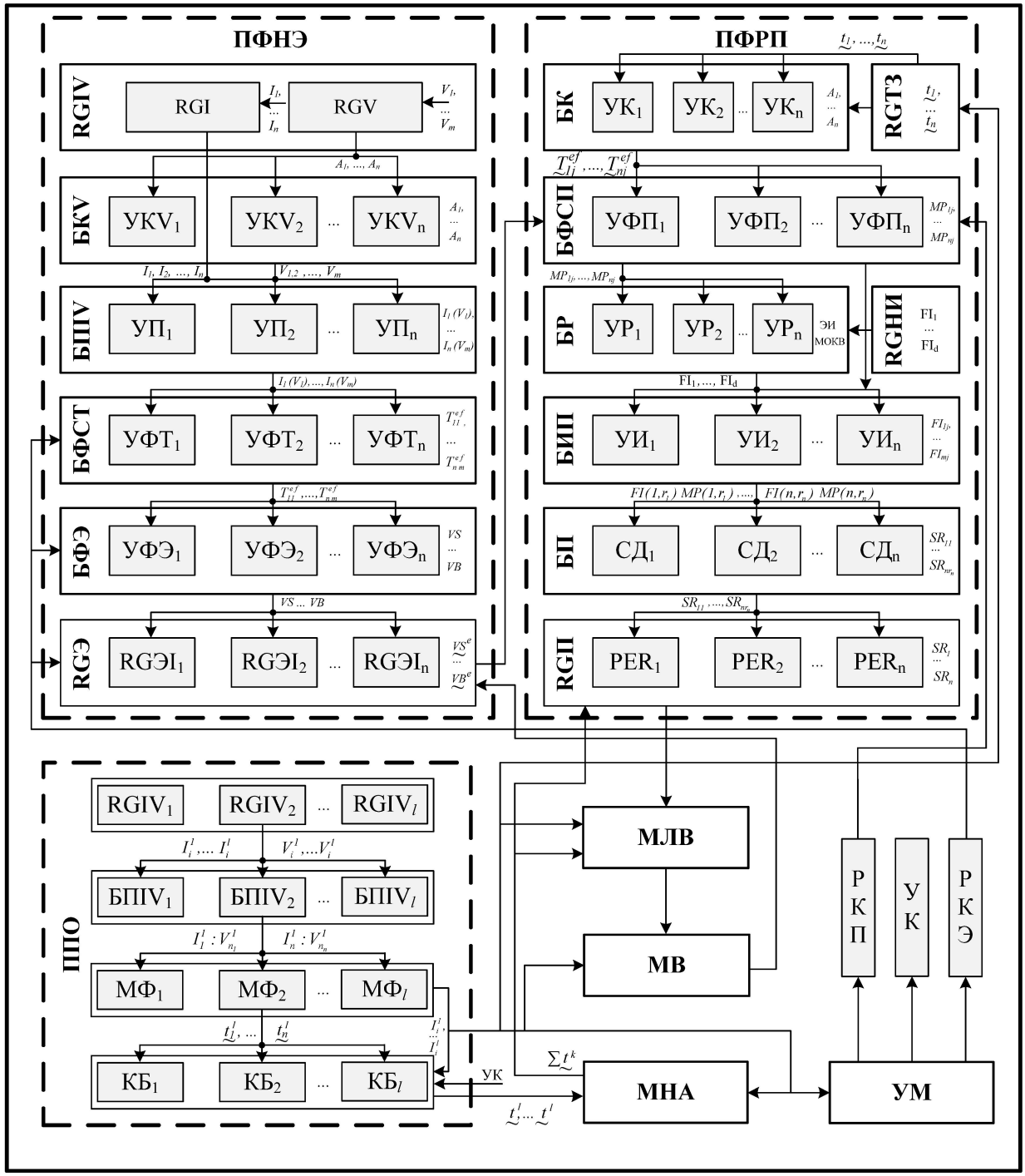

Рисунок 1 - Система выявления аномального состояния

На основе идентификаторов I_i $(i=\overline{1,n})$ (поступивших с RGI RGIV) и наборов величин V_j ($j=\overline{1,m}$), (поступивших с RGV RGIV через соответствующий узел коммутации величин ($УКV_i$, $i=\overline{1,n}$) БКV по сигналу I_i $(i=\overline{1,n})$) в БПIV на узлах пар ($УП_i$, $i=\overline{1,n}$) осуществляется формирование массивов (векторов) I_i $(V(A_i))$ $(i=\overline{1,n})$ (при этом по каждому фиксированному значению i сигнала A_i коммутируется свой набор величин $V(A_i)$, **например**, при $i=1$ на $УП_1$ с RGI поступает I_1, а с RGV по сигналу A_1 через $УКV_1$ на $УП_1$ группа величин $V(A_1)=V_{1,2}=\{V_1, V_2\}=\{NVC, VCA\}$ аналогично при $i=2$, $V(A_2)=V_{3,4,5}=\{V_3, V_4, V_5\}=\{NCC, SPR, DBR\}$, а при $i=3$, $V(A_3)=V_{3,6}=\{V_3, V_6\}=\{NCC, NPSA\}$, то есть $I_1 (V(A_1))=I_1 (V_{1,2})=SCANNING (NVC,VCA)$,

$I_2\ (V(A_2))=I_2\ (V_{3,4,5})=DOS\ (NCC,SPR,DBR)$, а $I_3\ (V(A_3))=I_3\ (V_{3,6})=SPOOFING\ (NCC, NPSA)$, где:

1) «Scanning of ports (*SCANNING*)» – «Сканирование портов»;
2) «Denial of service (*DOS*)» – «Отказ в обслуживании»;
3) «Spoofing (*SPOOFING*)» – «Спуфинг»;
4) «Numbers of Virtual channels (*NVC*)» – «Количество виртуальных каналов»;
5) «Virtual Channel Age (*VCA*)» – «Возраст виртуального канала»;
6) «Number of concurrent connections to the server (*NCC*)» – «Количество одновременных подключений к серверу»;
7) «Speed of processing requests from the clients (*SPR*)» – «Скорость обработки запросов от клиентов»;
8) «The delay between requests from the single user (*DBR*)» – «Задержка между запросами от одного пользователя»;
9) «Number of packages with the same sender and receiver address (*NPSA*)» – «Количество пакетов с одинаковым адресом отправителя и получателя».

Именам этих массивов соответствуют идентификаторы типа вторжения, а элементами – являются величины используемые для выявления аномалии, порожденной соответствующим вторжением.

Далее, в соответствующих узлах формирования термов (УФТ$_i$, $i=\overline{1,n}$) БФСТ генерируется значения T_{ij}^{ef} $(f=\overline{1,r};\ i=\overline{1,n};\ j=\overline{1,m})$ [6] для всех V_i $(i=\overline{1,m})$.

Количество таких термов и их нечеткая интерпретация определяется по экспертной информации (ЭИ), полученной на основе суждений специалистов соответствующей предметной области [19].

Для каждого УФТ$_i$ БФСТ относительно ЭИ определяются свои значения j' и f', согласно которых формируются требуемые наборы T_{ij}^{ef} для всех V_i. **Например**, при $m=j'=2$ и $f'=5$ и при $i=3$, $j'=2$ и $f'=3$ на выходе УФТ$_1$ формируется массив (вектор):

УФТ$_1$ $(\{T_{11}^{e1},\ T_{11}^{e2},\ T_{11}^{e3},\ T_{11}^{e4},\ T_{11}^{e5}\},\{T_{12}^{e1},\ T_{12}^{e2},\ T_{12}^{e3}\})=$

УФТ$_1$ $(\{T_{NVC}^{e1},\ T_{NVC}^{e2},\ T_{NVC}^{e3},\ T_{NVC}^{e4},\ T_{NVC}^{e5}\},\{T_{VCA}^{e1},\ T_{VCA}^{e2},\ T_{VCA}^{e3}\})$.

После получения требуемого набора термов для каждой I_i в УФЭ$_i$ определяются конкретные значения НЧ по каждому T_{ij}^{ef}. При реализации этой процедуры необходимо задать граничные значения для всех V_i $(i=\overline{1,m})$ т.е. $min\,v_i$ и $max\,v_i$ (**например**, для V_1 и V_2 границы $min\,v_1=min(NVC)$, $max(v_1)=max(NVC)$ и $min\,v_2=min(VCA)$, $max(v_2)=max(VCA)$), а также выбрать метод формирования функций принадлежности (МФФП) (см. этап 1 в [6]) согласно установленных критериев [19].

Таким образом, на входе УФЭ$_i$ сформируется массив (вектор) T_{ij}^{ef}, **например**, при значениях n, j' и f' аналогичных для T_{ij}^{ef} в БФСТ будут следующие:

УФЭ$_1$ $(\{\underset{\sim}{T}_{NVC}^{e1},\ \underset{\sim}{T}_{NVC}^{e2},\ \underset{\sim}{T}_{NVC}^{e3},\ \underset{\sim}{T}_{NVC}^{e4},\ \underset{\sim}{T}_{NVC}^{e5}\},\{\underset{\sim}{T}_{VCA}^{e1},\ \underset{\sim}{T}_{VCA}^{e2},\ \underset{\sim}{T}_{VCA}^{e3}\})=$

УФЭ$_1$ $(\{\underset{\sim}{VS}^{e},\ \underset{\sim}{S}^{e},\ \underset{\sim}{A}^{e},\ \underset{\sim}{B}^{e},\ \underset{\sim}{VB}^{e}\},\{\underset{\sim}{Y}^{e},\ \underset{\sim}{A}^{e},\ \underset{\sim}{O}^{e}\})$ (см. этап 4 в [6]).

Далее сформированные наборы НЧ для всех T_{ij}^{ef} перезаписываются в RGЭ, при этом значения эталонов соответствующие величинам i-го вторжения заносятся в соответствующий регистр эталонов i-го вторжения (RGЭI$_i$) и хранятся там в течение всего вычислительного процесса.

Для каждого T_{ij}^{ef} посредством сопроцессоров визуализации (СВ$_i$, $i=\overline{1,n}$) ПВЭ формируется графическое изображение эталонов величин для каждого I_i. Другими словами СВ$_1$ визуализирует эталон для I_1, СВ$_2$ – для I_2, а СВ$_n$ – для I_n, **например**, при $n=3$ СВ$_1$ визуализирует эталоны для *SCANNING* (СВ*SCANNING*), СВ$_2$ – для *DOS* (СВ*DOS*), а СВ$_3$ – *SPOOFING* (СВ*SPOOFING*).

Также в каждый RGЭ i-го вторжения (RGЭI$_i$, $i=\overline{1,n}$) ПФРП заносятся и хранятся на протяжении всего вычислительного процесса значения группы эталонов $\underset{\sim}{T}_{ij}^{ef}$ $(i=\overline{1,n})$ соответствующих величин, характерных для i- го вторжения, а также в RGTЗ поступают текущие значения $\underset{\sim}{t}_j$ $(i=\overline{1,n})$.

В узлах формирования пар (УФП$_i$, $i=\overline{1,n}$) БФСП на основе эталонных значений $\underset{\sim}{T}_{ij}^{ef}$ $(i=\overline{1,n})$, поступающих с RGЭI$_i$ $(i=\overline{1,n})$ и подмножества текущих величин $\underset{\sim}{t}_j$ $(i=\overline{1,n})$, поступивших с RGTЗ через узлы коммутации (УК$_i$, $i=\overline{1,n}$) БК посредством управляющего сигнала A$_i$ $(i=\overline{1,n})$ (**например**, при значениях $i=1$, $i=2$ и $i=n$ в УФП$_1$, УФП$_2$ и УФП$_n$ с RGTЗ через УК$_1$, УК$_2$ и УК$_n$ поступят соответственно значения $t_{1,2}=\{\underset{\sim}{t}_1,\ \underset{\sim}{t}_2\}=\{\underset{\sim}{t}_{NVC},\ \underset{\sim}{t}_{VCA}\}$, $t_{3,4,5}=\{\underset{\sim}{t}_3,\ \underset{\sim}{t}_4,\ \underset{\sim}{t}_5\}=\{\underset{\sim}{t}_{NCC},\ \underset{\sim}{t}_{SPR},\ \underset{\sim}{t}_{DBR}\}$ и $t_{3,n}=\{\underset{\sim}{t}_3,\ \underset{\sim}{t}_n\}=\{\underset{\sim}{t}_{NCC},\ \underset{\sim}{t}_{NPSA}\}$) соответственно сформируются и поступят на выход УФП$_i$ сопряженные пары MP_{ij}, **например**, $MP_{21}=(\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^e\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VS}^e)$.

Отметим, что в RGHИ заносятся все значения FI_i $(i=\overline{1,d})$ и хранятся там на протяжении всего процесса формирования правил.

В каждом узле ранжирования (УР$_i$, $i=\overline{1,n}$) БР для каждой MP_{ij} $(i=\overline{1,n})$ в качестве возможного исхода поочередно ставятся в соответствие все нечеткие идентификаторы FI_i $(i=\overline{1,d})$, поступившие с RGHИ. Далее на основе метода определения КВ (МОКВ) (см. этап 2 в [6]) и ЭИ из сформированного таким образом множества альтернативных правил SR_{ij}^k определяется множество FI_{ij}, необходимое для инициализации РП.

Далее, в узлах инициализации (УИ$_i$, $i=\overline{1,n}$) БИП на базе данных УР$_i$ и УФП$_i$ попарно формируются элементы матриц $MP(1,\ r_1)$ и $FI(1,\ r_1)$, на основе которых осуществляется инициализация необходимых наборов правил.

Сгенерированные в УИ$_i$ матрицы попарно заносятся в сектора данных (СД$_i$, $i=\overline{1,n}$) БП, формируя таким образом наборы правил SR_{ij} $(i=\overline{1,n},\ j=\overline{1,r_i})$ предназначенные для выявления аномального состояния порожденного i-м вторжением. Далее эти правила SR_i $(i=\overline{1,n})$ перезаписываются в регистры SR_i (PER$_i$, $i=\overline{1,n}$) и хранятся там на протяжении всего процесса функционирования системы.

Перед началом вычислительного процесса, в ПФНЭ на основе величин сетевого трафика (VCT) согласно соответствующей модели базовых величин (см. этап 3 в [6]) формируется множеств вторжений I_i $(i=\overline{1,n})$ и величин V_i $(i=\overline{1,m})$, посредством которых, с использованием выбранного (согласно установленным критериям) МФФП (см. этап 1 в [6]), генерируются эталоны [5, 6] для определенных ЛП по каждому терму T_{ij}^{ef}.

Согласно полученных эталонов величин в ПФРП создаются шаблоны наборов решающих правил SR_i $(i=\overline{1,n})$, [6], используемых для контроля сетевой активности относительно возможных проявлений атакующих действий в компьютерной сети. Эти шаблоны и эталоны величин не изменяются на протяжении всего процесса функционирования СВАС, но при необходимости могут модифицироваться посредством их перевода в РКЭ или РКП.

Далее с учетом того, что СВАС ориентирована на контроль аномального, состояния в l узлах (рабочих станциях, серверах и др.) компьютерной сети, то параллельно в l регистров вторжений и величин (RGIV$_k$, $k=\overline{1,l}$) ППО заносятся идентификаторы вторжений I_i^k $(i=\overline{1,n},\ k=\overline{1,l})$ и (с установленной периодичностью) текущие значения величин V_i^k $(i=\overline{1,m},\ k=\overline{1,l})$.

Например, при $n=3$ и $m=6$ для k-го узла сети осуществляется формирование I_i, и V_i [6], позволяющих идентифицировать аномальное состояние, порожденное тремя видами вторжений I_1^k, I_2^k и I_3^k ($SCANNING^k$, DOS^k и $SPOOFING^k$) на основе шести величин V_1^k, V_2^k, V_3^k, V_4^k, V_5^k и V_6^k (NVC^k, VCA^k, NCC^k, SPR^k, DBR^k и $NPSA^k$). Следует отметить, что если узлы компьютерной сети разнородны по своим характеристикам, то для определенных типов аномалий, порожденных соответствующими атакующими действиями, значения эталонов будут отличаться.

Для формирования пары конкретного вторжения с необходимыми для ее выявления величинами [6] в ППО используется l блоков пар вторжения и величины БПIV$_k$ $(k=\overline{1,l})$, представляющие собой специальным образом организованное запоминающее устройство. **Например**, при тех же $n=3$ и $m=6$ для k-го узла с идентификаторами вторжения:

(I_1^k), (I_2^k) и (I_3^k)

соответственно образуются пары с величинами:

$V_{n_1}^k=(V_1^k, V_2^k)$, $V_{n_2}^k=(V_3^k, V_4^k, V_5^k)$ и $V_{n_3}^k=(V_3^k, V_6^k)$, т.е.

$SCANNING^k:\{NVC^k, VCA^k\}$, $DOS^k:\{NCC^k, SPR^k, DBR^k\}$ и

$SPOOFING^k:\{NCC^k, NPSA^k\}$, $(k=\overline{1,l})$.

В этом примере, относительно организации БПIV, можно отметить, что идентификаторы $SCANNING^k$, DOS^k и $SPOOFING^k$ будут адресами специально организованного запоминающего устройства, а $\{NVC^k, VCA^k\}$, $\{NCC^k, SPR^k, DBR^k\}$ и $\{NCC^k, NPSA^k\}$ соответственно содержимым по этим адресам.

По завершению в БПIV$_k$ $(k=\overline{1,l})$ процедуры формирования пар $I_i^k : V_{n_i}^k$ с помощью модулей фаззификации МФ$_k$ $(k=\overline{1,l})$ осуществляется преобразование (с использованием МФФП) [6] множества текущих значений величин (наблюдаемых за определенный промежуток времени) посредством одного нечеткого числа (НЧ) $(i=\overline{1,n})$, [6] и таким образом на выходе МФ$_k$ получаем n НЧ $\underset{\sim}{t}_i^k$ $(i=\overline{1,n})$ связанных с соответствующими I_i. **Например**, при $n=6$ значение $\underset{\sim}{t}_1^k=\underset{\sim}{t}_{NVC}^k$, $\underset{\sim}{t}_2^k=\underset{\sim}{t}_{VCA}^k$, $\underset{\sim}{t}_3^k=\underset{\sim}{t}_{NCC}^k$, $\underset{\sim}{t}_4^k=\underset{\sim}{t}_{SPR}^k$, $\underset{\sim}{t}_5^k=\underset{\sim}{t}_{DBR}^k$ и $\underset{\sim}{t}_6^k=\underset{\sim}{t}_{NPSA}^k$.

Далее, поочередно полученные $\underset{\sim}{t}_i^k$ $(i=\overline{1,n},\ k=\overline{1,l})$ посредством k-х коммутирующих блоков КБ$_k$ $(k=\overline{1,l})$ по сигналу управления коммутацией (УК) соответственно типу вторжения I_i^k ($i=\overline{1,n}$, $k=\overline{1,l}$) с ППО в модуль нечеткой арифметики (МНА) поступают текущие величины $\underset{\sim}{t}^k$ ($k=\overline{1,l}$) со всех КБ$_k$ $(k=\overline{1,l})$ для получения суммарных показателей $\sum \underset{\sim}{t}^k$, характеризующих активность во всех узлах компьютерной сети. Наиболее подходящий метод, который может использоваться для реализации операций нечеткой арифметики (из четырнадцати фиксированных) выбирается согласно заданным критериям и реализуется в МНА [6].

Если процесс обнаружения аномального состояния по данным VCT осуществляется только на одном узле вычислительной сети, то МНА является прозрачным, то есть никаких суммарных значений переменных в нем не образуется.

На основе полученных в МНА суммарных показателей $\underset{\sim}{t}^k$, а также с использованием инициированного в ПФРП множества правил SR_i $(i=\overline{1,n})$ соответствующих определенным I_i в МЛВ, а также согласно известной технологии [6] посредством FI_i $(i=\overline{1,d})$, осуществляется определение текущего уровня аномального состояния в VCT, которое может быть порождено определенным типом кибератак.

Например, идентификация аномального состояния порожденного I_2 будет инициироваться правилом $SR_{34}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^e \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^e) \to H$, которое буквально можно интерпретировать как: “Если $\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^e$ и при этом $\underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^e$, то уровень аномального состояния, который может быть порожден *SPOOFING* будет HIGH”.

Этот уровень может представляться в нечеткой форме (выделено темно-серым цветом с областью маркированной литерой H), а также посредством МВ быть идентифицирован в графической форме в виде соответствующего НЧ (рисунок 2), отображенного на фоне сформированных в ПФРП эталонных значений лингвистических переменных.

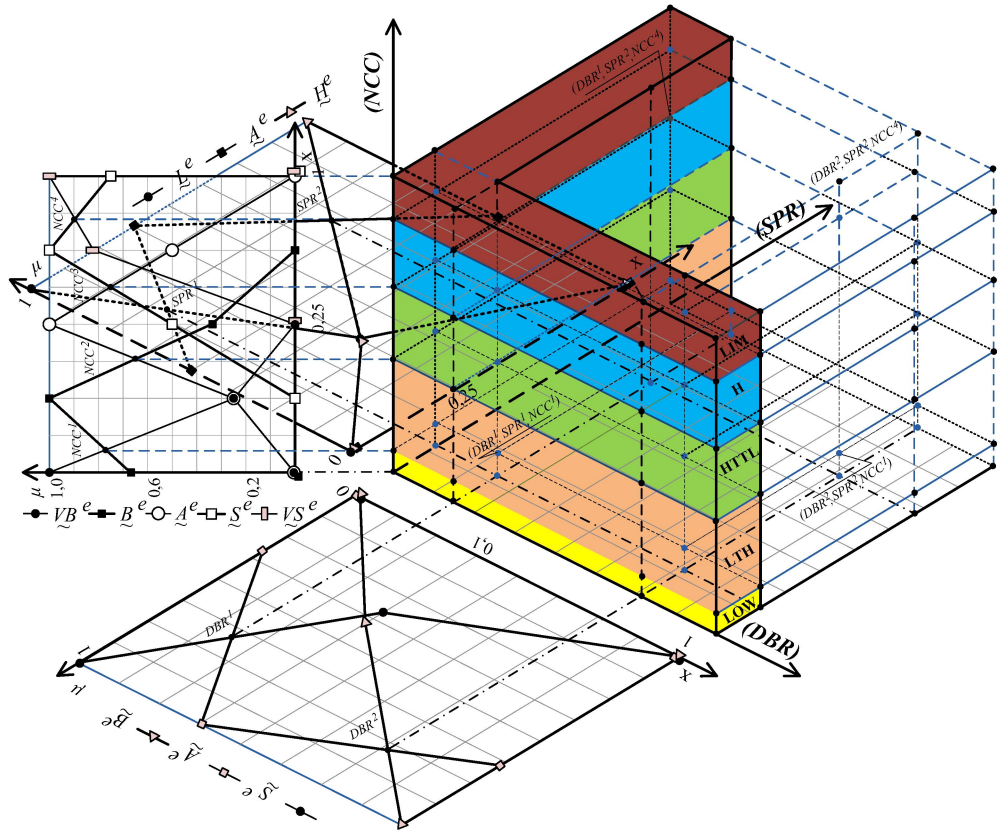

Рисунок 2 - Графическая интерпретация аномального состоянияпорожденного I_2

V. ВЫВОД

Таким образом, на основе предложений СВАС, базирующейся на подсистеме формирования нечетких эталонов, решающих правил и первичной обработки, а также модулей нечеткой арифметики, логического вывода, визуализации и управляющего модуля можно разрабатывать алгоритмическое, программное и программно-аппаратное обеспечение, применяемое для обнаружения аномального состояния, порожденного действиями несигнатурных кибератак. Такое обеспечение может использоваться автономно или в качестве расширителя функциональных возможностей современных систем обнаружения вторжений в компьютерных сетях.

ЛИТЕРАТУРА

[1] Model of decision rules to detect anomalies in information systems/ B.S. Akhmetov., A.A. Korchenko., N.K. Zhumangalieva// N E W S Of The National Academy Of Sciences Of The Republic Of Kazakhstan Physico-Mathematical Series // Volume 3, Number 307 (2016), pp. 91-100.

[2] Yao J.T., Zhao S.L., Saxton L.V. «A study on fuzzy intrusion detection» Proc. of SPIE Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, Vol. 5812, 2005, pp. 23-30.

[3] Fries P. «A Fuzzy-Genetic Approach to Network Intrusion Detection Terrence» Genetic and Evolutionary Computation Conference, GECCO (Companion) July 12-16, 2008, pp. 2141-2146.

[4] A Fuzzy Approach For Detecting Anomalous Behaviour in E-mail Traffic [Electronic resource] / Mark JynHuey Lim, Michael Negnevitsky, Jacky Hartnett // About Research Online @ ECU. – Electronic data. – Perth Western Australia] : Edith Cowan University, 2006. – Mode of access: World Wide Web. – URL: http://ro.ecu.edu.au/adf/29/. – Title from title screen. – Description based on home page (viewed on May 26, 2015).

[5] Base models reference values for intrusion detection system/ Akhmetov B.S., Abdrakhmanov R.B., Korchenko A.A., Zhumangalieva N.K.// Bulletin of International Kazakh-Turkish University named H.A. Yasawi //№5-6 (97-98), pp. 15-26.

[6] Technology of abnormal states for intrusion detection systems/ Akhmetov B.S., Korchenko A.A., Zhumangaliyeva N.K. // Al-Farabi Kazakh National University Kaznu Bulletin Mathematics, Mechanics, Computer Science Series//№1 (88), pp. 106-113.

[7] Wijayasekara D., Linda O., Manic M., Rieger C.G. Mining Building Energy Management System Data Using Fuzzy Anomaly Detection and Linguistic Descriptions. IEEE Trans. Industrial Informatics. Vol. 10, № 3, 2014, pp 1829-1840.

[8] Amin Einipour «Intelligent Intrusion Detection In Computer Networks Using Fuzzy Systems», Global Journal of Computer Science and Technology Neural & Artificial Intelligence (GJCST), Vol. 12, Issue 11 pp. 19-29, 2012.

[9] Shanmugavadivu R., Nagarajan N. «Network Intrusion Detection System Using Fuzzy Logic», Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp. 101-111, 2011.

[10] Linda O., Vollmer T., Wright J., Manic M. «Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor», in Proc. IEEE Symposium Series on Computational Intelligence, Paris, France, April, 2011, pp. 202-209.

[11] Linda O., Manic M., McJunkin T.R., «Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine» in Proc. IEEE Symposium on Resilience Control Systems, ISRCS 2011, Boise, Idaho, Aug. 9-11, 2011.

[12] Bridges S.M., Vaughn R.B. «Fuzzy data mining and genetic algorithms applied to intrusion detection». In: Proceedings of the 23rd National Information Systems Security Conference. October 2000, pp. 13-31.

[13] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha, Mat Kiah, Sanjay Misra «Anomaly Detection using Fuzzy Q-learning Algorithm» Acta Polytechnica Hungarica. Vol. 11, № 8, 2014, pp. 5-28.

[14] John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson «Fuzzy Intrusion Detection» IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 3, pp. 1506-1510.

[15] Chi-Ho Tsang, Sam Kwong, Hanli Wang « Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection » Pattern Recognition, Vol. 40, №. 9, Sept. 2007, pp. 2373-2391.

[16] Zadeh L.A. «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes» IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3, №. 1, January 1973, pp. 28-44.

[17] Gómez J., González F., Dasgupta D. «An Immuno-Fuzzy Approach to Anomaly Detection» The 12th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 25-28 May 2003, pp. 1219-1224.

[18] Zadeh L.A. «The concept of a linguistic variable and its application to approximate reasoning - I» Information Sciences, Vol. 8, №. 3, July 1975, pp. 199-249.

[19] 19. Корченко А.Г. Развитие систем защиты информации на основе нечетких множеств, Теория и практические решения, Киев, 2006, 320 с.

REFERENCES

[1] Model of decision rules to detect anomalies in information systems/ B.S. Akhmetov., A.A. Korchenko., N.K. Zhumangalieva// N E W S Of The National Academy Of Sciences Of The Republic Of Kazakhstan Physico-Mathematical Series // Volume 3, Number 307 (2016), pp. 91-100.

[2] Yao J.T., Zhao S.L., Saxton L.V. «A study on fuzzy intrusion detection» Proc. of SPIE Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, Vol. 5812, 2005, pp. 23-30.

[3] Fries P. «A Fuzzy-Genetic Approach to Network Intrusion Detection Terrence» Genetic and Evolutionary Computation Conference, GECCO (Companion) July 12-16, 2008, pp. 2141-2146.

[4] A Fuzzy Approach For Detecting Anomalous Behaviour in E-mail Traffic [Electronic resource] / Mark JynHuey Lim, Michael Negnevitsky, Jacky Hartnett // About Research Online @ ECU. – Electronic data. – Perth Western Australia] : Edith Cowan University, 2006. – Mode of access: World Wide Web. – URL: http://ro.ecu.edu.au/adf/29/. – Title from title screen. – Description based on home page (viewed on May 26, 2015).

[5] Base models reference values for intrusion detection system/ Akhmetov B.S., Abdrakhmanov R.B., Korchenko A.A., Zhumangalieva N.K.// Bulletin of International Kazakh-Turkish University named H.A. Yasawi //№5-6 (97-98), pp. 15-26.

[6] Technology of abnormal states for intrusion detection systems/ Akhmetov B.S., Korchenko A.A., Zhumangaliyeva N.K. // Al-Farabi Kazakh National University Kaznu Bulletin Mathematics, Mechanics, Computer Science Series//№1 (88), pp. 106-113.

[7] Wijayasekara D., Linda O., Manic M., Rieger C.G. Mining Building Energy Management System Data Using Fuzzy Anomaly Detection and Linguistic Descriptions. IEEE Trans. Industrial Informatics. Vol. 10, № 3, 2014, pp 1829-1840.

[8] Amin Einipour «Intelligent Intrusion Detection In Computer Networks Using Fuzzy Systems», Global Journal of Computer Science and Technology Neural & Artificial Intelligence (GJCST), Vol. 12, Issue 11 pp. 19-29, 2012.

[9] Shanmugavadivu R., Nagarajan N. «Network Intrusion Detection System Using Fuzzy Logic», Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp. 101-111, 2011.

[10] Linda O., Vollmer T., Wright J., Manic M. «Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor», in Proc. IEEE Symposium Series on Computational Intelligence, Paris, France, April, 2011, pp. 202-209.

[11] Linda O., Manic M., McJunkin T.R., «Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine» in Proc. IEEE Symposium on Resilience Control Systems, ISRCS 2011, Boise, Idaho, Aug. 9-11, 2011.

[12] Bridges S.M., Vaughn R.B. «Fuzzy data mining and genetic algorithms applied to intrusion detection». In: Proceedings of the 23rd National Information Systems Security Conference. October 2000, pp. 13-31.

[13] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha, Mat Kiah, Sanjay Misra «Anomaly Detection using Fuzzy Q-learning Algorithm» Acta Polytechnica Hungarica. Vol. 11, № 8, 2014, pp. 5-28.

[14] John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson «Fuzzy Intrusion Detection» IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 3, pp. 1506-1510.

[15] Chi-Ho Tsang, Sam Kwong, Hanli Wang « Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection » Pattern Recognition, Vol. 40, №. 9, Sept. 2007, pp. 2373-2391.

[16] Zadeh L.A. «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes» IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3, №. 1, January 1973, pp. 28-44.

[17] Gómez J., González F., Dasgupta D. «An Immuno-Fuzzy Approach to Anomaly Detection» The 12th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 25-28 May 2003, pp. 1219-1224.

[18] Zadeh L.A. «The concept of a linguistic variable and its application to approximate reasoning - I» Information Sciences, Vol. 8, №. 3, July 1975, pp. 199-249.

[19] Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.

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

[1] Х.А. Ясави атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан
[2]Ұлттық авиациялық университеті, Киев, Украина;
[3]Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕ АУЫТҚЫМА КҮЙЛЕРДІ АНЫҚТАУ ЖҮЙЕСІ

Аңдатпа. Компьютерлік жүйелерге деген қауіптер әсерлері көбейуде, олардың жаңа түрлері ресурстарға жаңа кибершабуылдарды тұйындатады. Қауіпсіздік деңгейін жоғарлату үшін жаңа қауіп түрлері пайда болғанда тиімді және ақпараттық жүйелердің көптеген ресурстарына бағытталған кибершабуылдарды анық емес жағдайларда анықтауға мүмкіндік беретін сәйкес арнайы қарсылық білдіру құралдары қажет. Анық емес жағдайларда қорғау есептерін шешуге қолданатын бірқатар үлгілер, әдістер белгілі. Оларды тиімді қолдану үшін ауытқыма күйін анықтау технологиясын жүзеге асыратын сәйкес жүйе қажет. Бұл мақсатпен ақпараттық жүйелерде кибершабуылдарды анықтау есептерін шешуге бағытталған жүйе құрылған. Жүйе анық емес логиканың математикалық әдістерінде және үлгілерінде негізделген және келесі ішкі жүйелер көмегімен: анық емес эталондарды қалыптастыру, шешуші ережелерді қалыптастыру, алғашқы өңдеу және келесі модульдер көмегімен: анық емес арифметика, логикалық шығару, визуализациялау және басқару жүзеге асырылады. Жүйе берілген уақыт аралығында нақты қоршау ортасында кибершабуылдардың анықталған типтерін тиімді табуға мүмкіндік береді, сонымен қатар заманауи басып кіруді табу жүйелерінің функционалды мүмкіндіктерін жаңа және сигнатурлы емес кибершабуылдар типтерін тиімді идентификациялау арқылы кеңейтуге мүмкіндік береді.

Тірек сөздер: кибершабуылдар, ауытқымалар, басып кіруді табу жүйелері, ауытқымаларды табу жүйелері, шабуылдарды табу жүйелері.

Сведения об авторах:

Ахметов Берик Бахытжанович - к.т.н., проректор Международного казахско-турецкого университета им. Х.А. Яссави.

Корченко Александр Григорьевич - д. т. н., профессор, Национальный авиационный университет, заведующий кафедрой Безопасности информационных технологий.

Алимсеитова Жулдыз Кенесхановна - лектор кафедры Информационной безопасности Казахского национального исследовательского технического университете имени К.И. Сатпаева, zhuldyz_al@mail.ru.

Жумангалиева Назым - м.т.н., докторант Казахского национального исследовательского технического университете имени К.И. Сатпаева.