ISSN 1991-346X

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Л А Р Ы

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

N E W S

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

ФИЗИКА-МАТЕМАТИКА СЕРИЯСЫ

♦

СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКАЯ

♦

PHYSICO-MATHEMATICAL SERIES

1 (305)

ҚАҢТАР – АҚПАН 2016 ж.
ЯНВАРЬ – ФЕВРАЛЬ 2016 г.
JANUARY – FEBRUARY 2016

1963 ЖЫЛДЫҢ ҚАҢТАР АЙЫНАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С ЯНВАРЯ 1963 ГОДА
PUBLISHED SINCE JANUARY 1963

ЖЫЛЫНА 6 РЕТ ШЫҒАДЫ
ВЫХОДИТ 6 РАЗ В ГОД
PUBLISHED 6 TIMES A YEAR

АЛМАТЫ, ҚР ҰҒА
АЛМАТЫ, НАН РК
ALMATY, NAS RK

«Известия НАН РК. Серия физико-математическая». ISSN 1991-346X
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5543-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год.
Тираж: 300 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел.: 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 1991-346X
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of information and archives of the Ministry of culture and information of the Republic of Kazakhstan N 5543-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 300 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
www:nauka-nanrk.kz / physics-mathematics.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 305 (2016), 26 – 33

THE MODEL OF BASE UNIT FOR CONTROL OF ABNORMAL CONDITION OF ENVIRONMENT

B. S. Akhmetov[1], A. A. Korchenko[2], N. K. Zhumangalieva[1]

[1]Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan,
[2]Department of Information Technology Security, National Aviation University, Kyiv, Ukraine.
E-mail: nazym_k.81@mail.ru

Key words: attack, anomaly intrusion, abnormal condition, fuzzy environment, intrusion detection system, the protection of information.

Abstract. There was suggested a generalized model of basic units, which is focused on building intrusion detection system based on the identification of abnormal state in the information system. Model based on three sets – the possible intrusion of possible values of conjugate pairs. For construction of the corresponding detection systems there are formed a plurality of pairs – «Invasion: the value» and «Invasion: the set of conjugate pairs», which are built on the basis of linguistic variables, reference values and logical rules aimed at detecting intrusions into the information system.

Systems based on a signature approach is usually possible to identify only certain forms of intrusion and detection of unknown largely carried out through a system of detection of attacks , based on the identification of abnormal state. They tend to be focused on functioning poorly formalized clearly defined environment for which you want to define a set of parameters required to detect attacks that gave rise to anomalies in the information system.

УДК 004.056.53 (045)

МОДЕЛЬ БАЗОВЫХ ВЕЛИЧИН ДЛЯ КОНТРОЛЯ АНОМАЛЬНОСТИ СОСТОЯНИЯ СРЕДЫ ОКРУЖЕНИЯ

Б. С. Ахметов[1], А. А. Корченко[2], Н. К. Жумангалиева[1]

[1]Казахский национальный исследовательский технический университет им. К. И. Сатпаева, Институт информационных и телекоммуникационных технологий, Алматы, Казахстан,
[2]Национальный авиационный университет, кафедра Безопасность информационных технологий, Киев, Украина

Ключевые слова: атака, аномалия, вторжение, аномальное состояние, нечеткая среда, системы обнаружения вторжений, защита информации.

Аннотация. Предложена обобщенная модель базовых величин, которая ориентирована на построение систем обнаружения вторжений, основанных на идентификации аномального состояния в информационной системе. Модель основывается на трех множествах – возможных вторжений, возможных величин и сопряженных пар. Для построения соответствующих систем обнаружения формируются множества пар – «вторжение : величины» и «вторжение : множество сопряженных пар», на основании которых строятся лингвистические переменные, эталоны величин и логические правила ориентированные на обнаружение вторжений в информационную систему. Системы, основанные на сигнатурном подходе, как правило, позволяют идентифицировать только известные формы вторжений, а обнаружения неизвестных в большей степени осуществляется с помощью системы выявления атак, основанных на идентификации аномального состояния. Они, как правило, направлены на функционирование в слабо формализованной нечетко определенной среде, для которой требуется определить набор параметров необходимый для выявления атак, породивших аномалии в информационной системе.

Введение. Интенсивное развитие информационных технологий оказало положительное влияние на все сферы человеческой деятельности. Вместе с тем наблюдаются и побочные эффекты, один из которых связан с увеличением вторжений на ресурсы информационных систем (РИС). Особого внимания заслуживают DoS-атаки, которые являются одними из самых опасных и простых в организации, дешевыми по стоимости и очень сложными в защите. Так, например, в Республике Казахстан они направлялись на сайты органов государственной власти (сайт комитета по правам интеллектуальной собственности Министерства юстиции Казахстана) [1], различные сетевые СМИ и др. Произошедшие события вскрыли неготовность систем безопасности к такого типа спланированным атакам, и даже на государственном уровне не оказалось (для реализации соответствующих выявляющих и блокирующих действий) достаточно эффективных средств защиты, к которым относятся и системы обнаружения вторжений (СОВ). В связи с этим создание методов и моделей, позволяющих разрабатывать эффективные СОВ, является актуальной научной задачей.

Методы исследования. Системы, основанные на сигнатурном подходе, как правило, позволяют идентифицировать только известные формы вторжений, а обнаружения неизвестных в большей степени осуществляется с помощью СОВ, основанных на идентификации аномального состояния. Они, как правило, направлены на функционирование в слабо формализованной нечетко определенной среде, для которой требуется определить набор величин необходимый для выявления вторжений, породивших аномалии в информационной системе (ИС). В работах [2-4] показана эффективность применения нечетких множеств для решения различных задач защиты информации, а также на основе логико-лингвистического подхода рассмотрен пример формирования нечетких величин для построения систем выявления такого вида вторжений, как сканирования портов. Использование математического аппарата нечетких множеств для формализации подхода к рациональному формированию необходимых (для решения подобных задач) величин, позволит повысить эффективность разрабатываемых СОВ. В этой связи целью данной работы является создание обобщенной модели величин, позволяющей синтезировать эффективно функционирующие СОВ по аномальному состоянию величин (например, сетевого трафика), характеризующих состояние среды окружения ИС.

Результаты исследования

Для создания базовой модели величин введем два множества – множество возможных вторжений (intrusion) ***I*** на РИС

$$\boldsymbol{I}=\bigcup_{i=1}^{n} I_i = \{I_1, I_2, I_3, \ldots, I_n\}, \ (i=\overline{1,n}) \tag{1}$$

и множество возможных величин (value) ***V***

$$\boldsymbol{V}=\bigcup_{i=1}^{m} V_i = \{V_1, V_2, V_3, \ldots, V_m\}, (i=\overline{1,m}) \tag{2}$$

характеризующих состояние среды окружения. По значениям величин из выражения (2) можно выявить аномальное состояние в ИС, порождаемое определенным элементом из множества ***I*** из формулы (1), где n определяет количество возможных вторжений, а m – общее количество возможных величин. Например, при $n=3$ (1) можно определить как:,

$$\boldsymbol{I}=\bigcup_{i=1}^{3} I_i = \{I_1, I_2, I_3\}=\{SCANNING, DOS, SPOOFING\}, \tag{3}$$

где $I_1=SCANNING$, $I_2=DOS$ и$I_3=SPOOFING$ соответственно являются идентификаторами и вторжений типа:

- «Scanning of ports (*SCANNING*)» – «Сканирование портов»,
- «Denial of service (*DOS*)» – «Отказ в обслуживании»,
- «Spoofing (*SPOOFING*)» – «Спуфинг».

Например, при $m=6$ выражение (2) принимает следующий вид:

$$\mathbf{V}=\bigcup_{i=1}^{6} V_i = \{V_1, V_2, V_3, V_4, V_5, V_6\}=\{NVC, VCA, NCC, SPR, DBR, NPSA\}, \quad (4)$$

где $V_1=NVC$, $V_2=VCA$, $V_3=NCC$, $V_4=SPR$, $V_5=DBR$, и$V_6=NPSA$ соответственно являются идентификаторами величин типа:

- «Numbers of Virtual channels (*NVC*)» – «Количество виртуальных каналов»,
- «Virtual Channel Age (*VCA*)» – «Возраст виртуального канала»,
- «Number of concurrent connections to the server (*NCC*)» – «Количество одновременных подключений к серверу»,
- «Speed of processing requests from the clients (*SPR*)» – «Скорость обработки запросов от клиентов»,
- «The delay between requests from the single user (*DBR*)» – «Задержка между запросами от одного пользователя»,
- «Number of packages with the same sender and receiver address (*NPSA*)» – «Количество пакетов с одинаковым адресом отправителя и получателя».

Каждому элементу (типу вторжения) множества $\boldsymbol{I}$ ставится в соответствие подмножество набора величин $\boldsymbol{V_n}$ (необходимого для обнаружения аномалий), составленного из элементов множества $\boldsymbol{V}$. Таким образом формируется, множество пар – «вторжение : величины», т.е.

$$\boldsymbol{I:V_n}=\bigcup_{i=1}^{n}\Big(I_i :\bigcup_{j=1}^{k_i} V_{ij} \Big)=\{(I_1:\{V_{11}, V_{12}, \ldots, V_{1k_1}\}),$$

$$\{(I_2:\{V_{21}, V_{22}, \ldots, V_{2k_2}\}), (I_3:\{V_{31}, V_{32}, \ldots, V_{3k_3}\}), \ldots, \quad (5)$$

$$(I_n:\{V_{n1}, V_{n2}, \ldots, V_{nk_n}\})\}, \ (i=\overline{1,n},\ j=\overline{1,k_i}).$$

Например, при $k_1=k_3=2$, и$k_2=3$,с учетом формулы (3) определим, что$V_{11}=V_1$, $V_{12}=V_2$, $V_{21}=V_3$, $V_{22}=V_4$, $V_{23}=V_5$, $V_{31}=V_3$, и$V_{32}=V_6$ и тогда выражение (5) с учетом формулы (4) будет иметь следующий вид:

$$\boldsymbol{I:V_n}=\bigcup_{i=1}^{3}\Big(I_i :\bigcup_{j=1}^{k_i} V_{ij} \Big)=\{(I_1:\{V_1, V_2\}), (I_2:\{V_3, V_4, V_5\}), (I_3:\{V_3, V_6\})\}=$$

$$\{(SCANNING:\{NVC, VCA\}), (DOS:\{NCC, SPR, DBR\}), (SPOOFING:\{NCC, NPSA\})\}. \quad (6)$$

Каждый V_{ij} (с учетом [2, 3]) удобно отображать лингвистическими переменными (ЛП), каждая из которых представляется кортежем

$$<V_{ij}, T_{ij}, U_{ij}> \ (i=\overline{1,n},\ j=\overline{1,k_i}), \quad (7)$$

где V_{ij} идентификатор (имя) ЛП, T_{ij} – базовое терм-множество (содержит термы $T_{ij}^{k}\ (k=\overline{1,r})$), U_{ij} – универсальное множество, являющееся областью определения для T_{ij}. Отметим, что m и V_{ij} определяются исходя из специфики реализации вторжения (атаки) и количества признаков, по которым можно определить аномальное состояние в среде окружения информационной системы. Например, с учетом выражений (6) и (7) набор кортежей, отображающих соответствующие значения ЛП для:

V_{11} и V_{12} имеет вид $<V_{11}, T_{11}, U_{11}>$, $<V_{12}, T_{12}, U_{12}>$, т.е. $<NVC, T_{NVC}, U_{NVC}>$, $<VCA, T_{VCA}, U_{VCA}>$;

V_{21}, V_{22} и V_{23}– $<V_{21}, T_{21}, U_{21}>$, $<V_{22}, T_{22}, U_{22}>$, $<V_{23}, T_{23}, U_{23}>$, т.е.

$<NCC, T_{NCC}, U_{NCC}>$, $<SPR, T_{SPR}, U_{SPR}>$, $<DBR, T_{DBR}, U_{DBR}>$;

V_{31} и V_{32}– $<V_{31}, T_{31}, U_{31}>$, $<V_{32}, T_{32}, U_{32}>$, т.е. $<NCC, T_{NCC}, U_{NCC}>$, $<NPSA, T_{NPSA}, U_{NPSA}>$.

Далее для каждой ЛП формируются r нечетких термов

$$T_{ij}=\bigcup_{k=1}^{r} T_{ij}^{k}=\{T_{ij}^{1},\ T_{ij}^{2},T_{ij}^{3},\ ...,\ T_{ij}^{k}\},(k=\overline{1,r}). \quad (8)$$

которые могут отображаться на универсальное множество *Uij* с областью определения $[V_{ij}^{min},\ V_{ij}^{max}]$, где V_{ij}^{min} и V_{ij}^{max} соответственно нижняя и верхняя границы значений T_{ij}. Например, если ЛП V_{11} определяется пятью термами *(r=5)*, а V_{12} тремя (*r=3),* то с учетом выражения (8) базовое терм-множество для V_{11} определяется как:

$$T_{11}=\bigcup_{k=1}^{5} T_{11}^{k}=\{T_{11}^{1},\ T_{11}^{2},T_{11}^{3},T_{11}^{4},T_{11}^{5}\}=\{T_{NVC}^{1},\ T_{NVC}^{2},T_{NVC}^{3},T_{NVC}^{4},T_{NVC}^{5}\}=$$

{«Very small» (VS), «Small» (S), «Average» (A), «Big» (B), «Very big» (VB)} (9)

и может быть отображено на универсальном множестве U_{ij}с областью определения $[V_{11}^{min},\ V_{11}^{max}]=[0,\ 256]$, где $T_{11}^{1}=T_{NVC}^{1}=$«*VS*», $T_{11}^{2}=T_{NVC}^{2}=$«*S*», $T_{11}^{3}=T_{NVC}^{3}=$«*A*», $T_{11}^{4}=T_{NVC}^{4}=$«*B*» и $T_{11}^{5}=T_{NVC}^{5}=$«*VB*» соответственно являются идентификаторами типа:

- «Very small (*VS*)» – «Очень малое»,
- «Small (*S*)» – «Малое»,
- «Average (*A*)» – «Среднее»,
- «Big (*B*)» – «Большое»,
- «Very big (*VB*)» – «Очень большое»,

а дляV_{12} – как:

$$T_{12}=\bigcup_{k=1}^{3} T_{12}^{k}=\{T_{12}^{1},T_{12}^{2},T_{12}^{3}\}=\{T_{VCA}^{1},T_{VCA}^{2},T_{VCA}^{3}\}=\{«Young» (Y), «Average» (A), «Old» (O)\}, \quad (10)$$

которые могут быть отображены на универсальном множестве U_{ij} с областью определения $[V_{12}^{min},\ V_{12}^{max}]=[0,\ 250]$, где $T_{12}^{1}=T_{VCA}^{1}=$«*Y*», $T_{12}^{2}=T_{VCA}^{2}=$«*A*» и $T_{12}^{3}=T_{VCA}^{3}=$«*O*» соответственно являются идентификаторами типа:

- «Young (*Y*)» – «Молодой»,
- «Average (*A*)» – «Средний»,
- «Old (*O*)» – «Старый».

Отметим, что множество термов T_{ij} $(i=\overline{1,n},\ j=\overline{1,m})$ отображается *r* нечеткими числами (НЧ)

$$T_{ij}\in\bigcup_{f=1}^{r}\underset{\sim}{T}_{ij}^{f}=\{\underset{\sim}{T}_{ij}^{1},\ \underset{\sim}{T}_{ij}^{2},\ \underset{\sim}{T}_{ij}^{3},\ \ldots,\ \underset{\sim}{T}_{ij}^{r}\},\ (f=\overline{1,r}) \quad (11)$$

для которых необходимо сформировать функции принадлежности (ФП) одним из известных методов [4]. Например, термы T_{11} *(при r=5)* и T_{12} (при *r=3*) с учетом формул (10) и (11) можно соответственно отобразить НЧ $\underset{\sim}{T}_{11}^{1},\ \underset{\sim}{T}_{11}^{2},\ \underset{\sim}{T}_{11}^{3},\ \underset{\sim}{T}_{11}^{4},\ \underset{\sim}{T}_{11}^{5}$ (т.е. $\underset{\sim}{VS},\underset{\sim}{S},\underset{\sim}{A},\underset{\sim}{B},\ \underset{\sim}{VB}$) и $\underset{\sim}{T}_{12}^{1},\ \underset{\sim}{T}_{12}^{2},\ \underset{\sim}{T}_{12}^{3}$ (т.е. $\underset{\sim}{Y},\ \underset{\sim}{A},\ \underset{\sim}{O}$), для которых формируются ФП. Получить ФП можно, например, на основе метода лингвистических термов с использованием статистических данных (МЛТС) [2], при помощи которого для любого из заданных термов определяется *l* номеров интервалов $N_{ij}^{1},\ N_{ij}^{2},\ ...,\ N_{ij}^{l}$ возможных значений с соответствующими граничными величинами V_{ij}^{min} и V_{ij}^{max}. Здесь в качестве исходных данных может использоваться статистическая, аналитическая, экспертная и другая информация, обычно применяемая для построения нечетких эталонов, т.е. эталонов

величин, с помощью которых осуществляется классификация текущего состояния величин в аномальной среде.

Например, для T_{11} при $l=5$ значениям номеров $N_{1j}^{1}=N_{11}^{1},\ N_{1j}^{2}=N_{11}^{2},\ N_{1j}^{3}=N_{11}^{3},\ N_{1j}^{4}=N_{11}^{4},$ $N_{1j}^{5}=N_{11}^{5}$ будут соответствовать интервалы $[V_{11}^{min}=V_{11}^{0},V_{11}^{1}],\ ]V_{11}^{1},\ V_{11}^{2}],\ ]V_{11}^{2},\ V_{11}^{3}],\ ...,\ ]V_{11}^{4},$ $V_{11}^{5}=V_{11}^{max}]$ т.е. *[0; 2],]2; 8],]8; 16],]16; 64],]64; 256]*, а для T_{12} при $l=3$ номерам интервалов $N_{1j}^{1}=N_{12}^{1},\ N_{1j}^{2}=N_{12}^{2}, N_{1j}^{3}=N_{12}^{3}$ соответствуют $[V_{12}^{min}=V_{12}^{0},\ V_{12}^{1}],\ ]V_{12}^{1},\ V_{12}^{2}],\ ]V_{12}^{2},\ V_{12}^{3}=V_{12}^{max}]$ т.е. *[0; 30],]30; 100],]100; 250]*.

На основе полученных значений ФПНЧ $\underset{\sim}{T}_{ij}^{f}\ \ (f=\overline{1,r})$ для каждой V_{ij} формируются эталоны величин $\underset{\sim}{T}_{ij}^{ef}\ (f=\overline{1,r},\ i=\overline{1,n},\ j=\overline{1,m})$, по принципу определенного класса НЧ на основе признаков нормальности, модальности, выпуклости, непрерывности и параметричности [2]. Например, для $V_{11}=NVC$ и $V_{12}=VCA$ значения $\underset{\sim}{T}_{11}^{ef}=\underset{\sim}{T}_{NVC}^{ef}$, $(f=\overline{1,5})$ и $\underset{\sim}{T}_{12}^{ef}=\underset{\sim}{T}_{VCA}^{ef}$, $(f=\overline{1,3})$ могут быть определены нормальными, унимодальными, выпуклыми, дискретными, непараметрическими НЧ с произвольным числом носителей [2], т.е.

$$\underset{\sim}{T}_{11}^{e1}=\underset{\sim}{T}_{NVC}^{e1}=\underset{\sim}{VS}^{e}=\{0/0{,}008;\ 1/0{,}008;\ 0{,}33/0{,}031;\ 0/0{,}063\},$$

$$\underset{\sim}{T}_{11}^{e2}=\underset{\sim}{T}_{NVC}^{e2}=\underset{\sim}{S}^{e}=\{0/0{,}008;\ 0{,}5/0{,}008;\ 1/0{,}031;\ 0{,}5/0{,}063;\ 0/0{,}25\},$$

$$\underset{\sim}{T}_{11}^{e3}=\underset{\sim}{T}_{NVC}^{e3}=\underset{\sim}{A}^{e}=\{0/0{,}008;\ 0{,}33/0{,}031;\ 1/0{,}063;\ 0{,}67/0{,}25;\ 0/1\},$$

$$\underset{\sim}{T}_{11}^{e4}=\underset{\sim}{T}_{NVC}^{e4}=\underset{\sim}{B}^{e}=\{0/0{,}063;\ 1/0{,}25;\ 0{,}75/1;\ 0/1\},$$

$$\underset{\sim}{T}_{11}^{e5}=\underset{\sim}{T}_{NVC}^{e5}=\underset{\sim}{VB}^{e}=\{0/0{,}063;\ 0{,}2/0{,}25;\ 1/1;\ 0/1\}$$

и соответственно

$$\underset{\sim}{T}_{12}^{e1}=\underset{\sim}{T}_{VCA}^{e1}=\underset{\sim}{Y}^{e}=\{1/0;\ 1/0{,}12;\ 0{,}5/0{,}4;\ 0{,}25/1\},$$

$$\underset{\sim}{T}_{12}^{e2}=\underset{\sim}{T}_{VCA}^{e2}=\underset{\sim}{A}^{e}=\{0{,}2/0;\ 0{,}2/0{,}12;\ 1/0{,}4;\ 0{,}4/1\},$$

$$\underset{\sim}{T}_{12}^{e3}=\underset{\sim}{T}_{VCA}^{e3}=\underset{\sim}{O}^{e}=\{0/0{,}12;\ 0{,}17/0{,}4;\ 1/1\}.$$

Принятие решения о том, что состояние среды характерно для процесса реализации вторжения удобно осуществлять на основе множеств сопряженных пар (matchedpair) ***MP***, множество которых обозначим через:

$$\boldsymbol{MP}=\bigcup_{i=1}^{n}\Big(\bigcup_{j=1}^{c_n}MP_{ij}\Big)=\{(\boldsymbol{MP_1}),\ (\boldsymbol{MP_2}),\ (\boldsymbol{MP_3}),\ ...,\ (\boldsymbol{MP_n})\}=$$

$$\{(MP_{11}, MP_{12}, MP_{13}, \ldots, MP_{1c_1}), (MP_{21}, MP_{22}, MP_{23}, \ldots, MP_{2c_2}),$$
$$(MP_{31}, MP_{32}, MP_{33}, \ldots, MP_{3c_3}), \ldots,$$
$$(MP_{n1}, MP_{n2}, MP_{n3}, \ldots, MP_{nc_n})\}, \ (i=\overline{1,n}, \ j=\overline{1,c_n}), \quad (12)$$

где c_n – количество сопряженных пар в множестве, необходимых для составления правил направленных на выявление n-го вторжения. Элементы ***I*** в совокупности ***MP*** могут формировать множества пар – «вторжение **:** множество сопряженных пар»:

$$\boldsymbol{I:MP}=(\bigcup_{i=1}^{n} I_i : \bigcup_{j=1}^{c_i} MP_{ij}) = \{(I_1:\boldsymbol{MP_1}), (I_2:\boldsymbol{MP_2}), (I_3:\boldsymbol{MP_3}), \ldots, (I_n:\boldsymbol{MP_n})\} =$$
$$\{(I_1:\{MP_{11}, MP_{12}, MP_{13}, \ldots, MP_{1c_1}\}), (I_2:\{MP_{21}, MP_{22}, MP_{23}, \ldots, MP_{2c_2}\}),$$
$$(I_3:\{MP_{31}, MP_{32}, MP_{33}, \ldots, MP_{3c_3}\}), \ldots, (I_n:\{MP_{n1}, MP_{n2}, MP_{n3}, \ldots, MP_{nc_n}\})\}. \quad (13)$$

Например, при $c_1=c_2=c_3=5$ выражение (13) примет следующий вид:

$$\boldsymbol{I:MP}=(I_1:\{MP_{11}, MP_{12}, MP_{13}, MP_{14}, MP_{15}\}), \ldots, (I_5:\{MP_{51}, MP_{52}, MP_{53}, MP_{54}, MP_{55}\}) =$$
$$\{(SCANNING:\{\text{«NVC } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{VS}^e\text{»}, \text{«NVC } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{S}^e\text{»},$$
$$\text{«NVC } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{A}^e\text{»}, \text{«NVC } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{B}^e\text{»},$$
$$\text{«NVC } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{VB}^e\text{»}\}),$$
$$(DOS:\{\text{«SPR } \underset{\sim}{L} \text{ соизмеримо с } \underset{\sim}{VS}^e\text{»}, \text{«SPR } \underset{\sim}{L} \text{ соизмеримо с } \underset{\sim}{S}^e\text{»},$$
$$\text{«SPR } \underset{\sim}{L} \text{ соизмеримо с } \underset{\sim}{A}^e\text{»}, \text{«SPR } \underset{\sim}{L} \text{ соизмеримо с } \underset{\sim}{B}^e\text{»},$$
$$\text{«SPR } \underset{\sim}{L} \text{ соизмеримо с } \underset{\sim}{VB}^e\text{»}\}),$$
$$(DOS:\{\text{«DBR } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{VS}^e\text{»}, \text{«DBR } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{S}^e\text{»},$$
$$\text{«DBR } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{A}^e\text{»}, \text{«DBR } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{B}^e\text{»},$$
$$\text{«DBR } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{VB}^e\text{»}\}),$$
$$(SPOOFING:\{\text{«NPSA } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{VS}^e\text{»}, \text{«NPSA } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{S}^e\text{»},$$
$$\text{«NPSA } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{A}^e\text{»}, \text{«NPSA } \underset{\sim}{S} \text{ соизмеримо с } \underset{\sim}{B}^e\text{»},$$
$$\text{«NPSA } \underset{\sim}{S} \text{ со измеримо с } \underset{\sim}{VB}^e\text{»}\}) \quad (14)$$

На основе множества ***MP*** строятся логические правила типа – «Если MP_{ij} то …» и например, для выражения (14) они будут иметь следующий вид:

1. Если MP_{11},то возможность сканирования LOW (Н);
2. Если MP_{12}, то возможность сканирования LTH (БНВ);

3. Если MP_{13}, то возможность сканирования HTTL (БВН);

4. Если MP_{14}, то возможность сканирования H (В);

5. Если MP_{15},то возможность сканирования LIM (П),

где L – LOW (низкая), LTH – LOWER THAN HIGH (больше низкая чем высокая), HTTL – HIGHER THAN THE LOWEST (больше высокая чем низкая), H – HIGH (высокая), LIM – LIMITS (предельная), а понятие «соизмеримо», используемое в сопряженных парах, может отображать минимальное расстояние Хемминга [4] между значениями используемых величин.

Обсуждение результатов

Для проведения дальнейших исследований необходимо построить базовые модели эталонных величин, которые ориентированы на построение систем обнаружения вторжений, основанных на идентификации аномального состояния в информационной системе.

Выводы. На основе предложенной модели величин, базирующейся на множествах возможных вторжений и возможных величин, а также на множествах пар «вторжение : величины» и «вторжение : множество сопряженных пар» можно строить модели систем обнаружения вторжений, позволяющих повысить эффективность соответствующих средств, основанных на идентификации аномального состояния величин в информационной системе.

ЛИТЕРАТУРА

[1] Казахстанский правительственный сайт взломан в отместку за торренты [Электронный ресурс] / TENGRINEWS.KZ // ТОО «EML» : [TENGRINEWS.KZ]. – Электрон. дан. – 2012. – 8 февраля. – Режим доступа: WorldWideWeb. –URL: http://tengrinews.kz/internet/kazahstanskiy-pravitelstvennyiy-sayt-vzloman-otmestku-207728/. – Загл. с титул. экрана.

[2] Корченко О.Г. Построение систем защиты информации на нечетких множествах [Текст]: Теория и практические решения / О.Г. Корченко. – К. : МК-Пресс, **2006**. – 320 с.

[3] Волянська В.В. Система виявлення аномалій на основі нечітких моделей [Текст] / В.В. Волянська, А.О. Корченко, Є.В. Паціра // Зб. наук. пр. Інституту проблем моделювання в енергетиці НАН України ім. Г.Є Пухова. – Львів: ПП «Системи, технології, інформаційніпослуги», 2007.– [Спец. випуск].– Т.2.– С. 56-60.

[4] Корченко О.Г. Системи захисту інформації [Текст] : Монографія / О.Г. Корченко.– К.: НАУ, 2004.– 264 с.

[5] Аксен Б.А. Электронные системы расчетов в Internet: от реальной витрины к виртуальной / Б.А. Аксен // Конфидент. - 1996. - № 6 - С. 43 -48 .

[6] Андерсон Р. UEPS - электронный бумажник второго поколения /Р. Адерсон// Конфидент. - 1996. -№ 1 - С. 49-53.

[7] Галатенко В.А. Основы информационной безопасности: учебное пособие /В.А. Галатенко; под ред . академика РАН В.Б. Бетелина, 4-е изд.-М.:Интернет -Университет .информационных технологий; БИНОМ . Лаборатория знаний, 2008.-205с.

[8] Герасименко, В.А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы /В.А Герасименко // Зарубежная радиоэлектроника . - 1993. - № 3. - С.3-21.

[9] Оценка безопасности информационных технологий / А.П. Трубачев, И.А. Семичев, В. Н . Шакунов и др. - М.: СИП РИА , 2001 . -388 с.:ил.

[10] Ященко В.В. Введение в криптографию / Под общей ред. В.В. Ященко.-СПб.: Питер, 2001. -288с.: ил

[11] Гришина Н. В. Модель потенциального нарушителя объекта информатизации // Материалы V Международной научно-практической конференции «Информационная безопасность». — Таганрог, 2003.

[12] Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / Киев: ООО «ТИД» «ДС», 2002.

[13] Алексенцев А.И. Определение состава конфиденциальной информации // Справочник секретаря и офис-менеджера. - № 2, 3. - 2003.

[14] *Степанов Е. А., Корнеев И. К.* Информационная безопасность и защита информации. - М., 2001.

[15] *Лепехин А. Н.* Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. - 176 с.

[16] *Лепехин А. Н.* Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты. М.: Тесей, 2008. - 176 с.

[17] Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2002. – 816 с.

[18] Введение в криптографию / Под. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.

[19] Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Иващко. – М.: Горячая линия - Телеком, 2000. – 452 с.

[20] Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д. транспорта / В.В. Яковлев, А.А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.

[21] Винокуров, А.Ю. Традиционные криптографические алгоритмы. http://www.enlight.ru/crypto/algorithms/algs.htm.

[22] Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазинин, Н.С. Погожин. – М.: Горячая линия - Телеком, 2001. – 148 с.

REFERENCES

[1] The Kazakh government site hacked in retaliation for torrents [electronic resource] / TENGRINEWS.KZ // TOO «EML»: [TENGRINEWS.KZ]. Elektron. Dan. 2012. February 8. Access: WorldWideWeb. URL: http://tengrinews.kz/internet/kazahstanskiy-pravitelstvennyiy-sayt-vzloman-otmestku-207728/. Zagl. with the title. screen.

[2] Korchenko O.G. Construction of information security systems on fuzzy sets [Text]: theory and practical solutions / OG Korchenko. K. : MC Press, 2006. 320 p. (in Russ.).

[3] Volyanska V.V. System viyavlennya anomaliy on osnovi nechitkih models [Text] / V.V. Volyanska, A.O. Korchenko, E.V. Patsira // ST. Sciences. pr. Institutu problems modelyuvannya in energetitsi IM NAS of Ukraine. G.Є Pukhov. Lviv: PP "system tehnologiї, informatsiyniposlugi», 2007. [Spec. Key infrastructure] .T.2. p. 56-60. (in Ukr.).

[4] Korchenko O.G. Sistemi Zahist Informácie [Text]: Monografiya / OG Korchenko. K .: the NAU, 2004. 264. (in Ukr.).

[5] Axen B.A. Electronic payment system on the Internet: from the real to the virtual showcase / B.A. Axen // Confident, - 1996. - № 6 - p. 43-48. (in Russ.).

[6] Anderson R. UEPS - the second generation of an electronic wallet / P. Aderson // Confident. - 1996. -№ 1 - P. 49-53. (in Russ.).

[7] Galatenko V.A. Fundamentals of Information Security: A Training Manual /V.A. Galatenko; ed. Academician VB Betelin, 4th izd.-M. internet -Universitet .informatsionnyh technologies; BINOMIAL . Knowledge Laboratory, 2008.-205p. (in Russ.).

[8] Gerasimenko V.A. Information protection in automated data processing systems: development, results, prospects / V.A. Gerasimenko // Foreign radioelectronics. -1993.№3.-p.3-21. (in Russ.).

[9] Information Technology Security Evaluation / A.P. Trubachov, I.A. Semichev, V.N. Shakunov, et al. - M .: CIP RIA, 2001. -388 P.: Il. (in Russ.).

[10] Yaschenko V.V. Introduction to cryptography / Under the general editorship. VV Yaschenko.-SPb .: Peter, 2001. - 288p .: silt (in Russ.).

[11] Grishin N.V. Model potential intruder object informatization // Proceedings of the V International Scientific and Practical Conference "Information Security". - Taganrog, 2003. (in Russ.).

[12] Domarev V. Security of information technologies. Methodology of protection systems / Kiev OOO "TID" "DS", 2002. (in Russ.).

[13] Aleksentsev A.I. Determination of confidential information // Reference secretary and office manager. - Number 2, 3 - 2003. (in Russ.).

[14] Stepanov E.A., Korneev I.K. Information security and data protection. - M., 2001. (in Russ.).

[15] Lepekhin A.N. Investigation of crimes against information security. Theoretical and legal and practical aspects. M.: Theseus, 2008. - 176 p. (in Russ.).

[16] Lepekhin A.N. Investigation of crimes against information security. Theoretical and legal and practical aspects. M.: Theseus, 2008. - 176 p. (in Russ.).

[17] Schneier B. Applied Cryptography. Protocols, algorithms, source code in C / B. Schneier - M .: TRIUMPH, 2002. - 816 p. (in Russ.).

[18] Introduction to Cryptography / Under. Ed. V.V. Yaschenko. - SPb .: Peter, 2001. - 288 p. (in Russ.).

[19] Zegzhda D.P. Fundamentals of Information Systems Security / DP Zegzhda, AM Ivaschko. - M.: Hotline - Telecom, 2000. - 452 p. (in Russ.).

[20] Yakovlev V.V. Information security and protection of data in corporate networks of rail transport: Textbook for universities railway Transport / V.V. Yakovlev, A.A. Kornienko. - M .: Russian Ministry of CMD, 2002. - 328 p. (in Russ.).

[21] Vinokourov A.Y. Traditional cryptographic algorithms. http://www.enlight.ru/crypto/algorithms/algs.htm.

[22] Maluk A.A. Introduction to the protection of information in automated systems / AA Maluk, SV Pazinin, NS Pogozhin. - M .: Hotline - Telecom, 2001. - 148 p. (in Russ.).

ҚОРШАҒАН ОРТАНЫҢ АНОМАЛИЯЛЫҚ ЖАҒДАЙЫН БАҚЫЛАУҒА АРНАЛҒАН БАЗАЛЫҚ ШАМАНЫҢ МОДЕЛЬДЕРІ

Б. С. Ахметов[1], А. А. Корченко[2], Н. К. Жұманғалиева[1]

[1]Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университет, Ақпарттық және телекоммуникациялық технологиялар институты, Алматы, Қазақстан,

[2]Ұлттық авиациалық университет, кафедра Ақпараттық технологиялар қауіпсіздігі, Украина, Киев

Тірек сөздер: шабуыл, аномалия, шабуылдар, аномалиялық жағдай, айқын емес орта, басып кірулерді анықтау жүйесі, ақпаратты қорғау.

Аннотация. Ақпараттық жүйедегі аномалиялық жағдайды анықтауға негізделген басып кірулерді анықтау жүйесін құруға негізделген базалық шаманың жалпылама моделі ұсынылды. Модель үш жиынтыққа - ықтимал шабуылдар, ықтималды шама және коньюгат жұптарға негізделеді. Сәйкес жүйелерді құру үшін жиынтық жұптар қалыптасады: «шабуылдар: шама» және «шабуылдар: коньюгат жұптар жиынтығы» негізінде лингвистикалық айнымалылар, шама эталондары және логикалық ережелер ақпараттық жүйеге басып кірулерді анықтауға негізделген. Белгілік тәсілге негізделген жүйелер әдетте тек шабуылдың белгілі түрлерін анықтауға мүмкіндік береді, ал белгісіздерді айқындау көбінесе аномальды жағдайды анықтауға негізделген шабуылдарын анықтау жүйесі арқылы жүзеге асады. Олар әдетте ақпараттық жүйеде аномалия тудырған шабуылдарды анықтауға қажет параметрлерді айқындау қажет болатын әлсіз формальды айқын емес ортада қызмет етуге бағытталған.

Поступила 13.01.2016 г.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

http://www.physics-mathematics.kz

Редактор *М. С. Ахметова*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 16.01.2016.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
10,7 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19