N E W S
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 3, Number 307 (2016), 91 – 100

UDC 004.056.53 (045)

MODEL OF DECISION RULES TO DETECT ANOMALIES IN INFORMATION SYSTEMS

B.S. Akhmetov* A.A. Korchenko N.K. Zhumangalieva*****

*– Institute of Information and Telecommunication Technologies, Kazakh National Technical University named after K.I. Satpayev, Almaty, Kazakhstan;
**– Department of Information Technology Security, PhD, Associate Professor, National Aviation University, Kyiv, Ukraine;
***– Institute of Information and Telecommunication Technologies Institute of Postgraduate Education, Kazakh National Technical University after K.I. Satpayev, Almaty, Kazakhstan
nazym_k.81@mail.ru

Key words cyber attack, intrusion detection systems, network traffic anomaly, anomaly detection in computer systems, the set of conjugate pairs , decision rules, expert evaluation.

Abstract. The disadvantage of modern intrusion detection systems, built on the principle of identifying the abnormal condition is that they are mainly focused on the use of mathematical models that require a lot of time to prepare statistics. Mathematical models based on expert approaches in this regard are more effective, but for the performance of its functions it is required the use of appropriate decision rules. For solving this problem, we propose a model of decision rules on fuzzy logic, which through the use of a plurality of pairs of "invasion: the value" and "Invasion: the set of conjugate pairs", as well as models of reference values allows you to display an abnormal condition, generates a certain type of cyber attack in computer network. Based on this model there have been developed examples of rules to detect such intrusions as scanning, spoofing and Dos-attacks that can practically be used to improve real systems intrusion detection mechanism is used to identify anomalies generated by the actions of attacking computer systems.

УДК 004.056.53 (045)

МОДЕЛЬ РЕШАЮЩИХ ПРАВИЛ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Б.С. Ахметов* А.А. Корченко Н.К. Жумангалиева*****

*– КазНТУ имени К.И.Сатпаева, Институт информационных и телекомминикационных технологии, д.т.н., профессор, Алматы, Казахстан
**– Национальный авиационный университет, кафедра Безопасности информационных технологий, к.т.н., доцент, Киев, Украина
***– КазНТУ имени К.И.Сатпаева, Институт информационных и телекомминикационных технологии, докторант, Алматы, Казахстан

Ключевые слова: кибератака, системы обнаружения вторжений, аномалия в сетевом трафике, обнаружение аномалий в компьютерных системах, сопряженная пара, решающие правила, экспертная оценка.

Аннотация. Недостатком современных систем обнаружения вторжений, построенных на принципе идентификации аномального состояния, является то, что они в основном ориентированы на использование

таких математических моделей, которые требуют много времени на подготовку статистических данных. Математические модели, основанные на экспертных подходах, в этом отношении являются более эффективными, но для выполнения своих функций необходимо использование соответствующих решающих правил. Для решения этой задачи в работе предложена модель решающих правил на нечеткой логике, которая за счет использования множества пар «вторжение : величины» и «вторжение : множество сопряженных пар», а также модели эталонных величин позволяет отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. На основе этой модели были разработаны примеры правил для обнаружения таких вторжений, как сканирование, спуфинг и Dos-атака, которые могут практически использоваться для усовершенствования реальных систем выявления вторжений применяющих механизмы выявления аномалий, порожденных атакующими действиями в компьютерных системах.

Введение. Стремительное развитие информационных технологий (ИТ) в свою очередь породило большое количество угроз ресурсам информационных систем (РИС). Одним из решений обеспечения безопасности РИС, являются системы обнаружения вторжений (СОВ), представляющие собой программные или аппаратные средства, ориентированные, прежде всего, на выявление фактов неавторизованного доступа. Следует отметить, что современные СОВ основываются на сигнатурном (шаблонном) и аномальном принципах.

Первый базируется на представлении каждого вторжения в виде определенного шаблона (модели, сценария, правила, сигнатуры) отражающего характеристики и сценарии возможных несанкционированных воздействий. Поэтому такие системы с достаточно высокой точностью выявляют тип кибератак и практически функционируют без ложных срабатываний. Анализ сетевого трафика с использованием сигнатурного принципа характерен тем, что распознавание возможно только при известных кибератаках, а для этого необходимо постоянно обновлять и расширять наборы шаблонов. Кроме неустойчивости к новейшим типам вторжений, такие системы сильно зависят от скорости разработки и обновления сигнатур. Также известно, что например, для таких вторжений как сложные распределенные атаки проверка известных шаблонов является достаточно сложной задачей.

Второй принцип основан на выявлении аномального состояния системы порожденного кибератакой и ориентирован на контроль активности в среде окружения, например, наблюдение за значениями величин сетевого трафика. Преимущества систем, реализирующих этот принцип, в первую очередь связано с тем, что они могут обнаруживать не только новые виды кибератак, но и те, которые характеризуются большой продолжительностью во времени.

Методы исследование. Существующие СОВ аномального принципа в основном ориентированы на использование таких математических моделей, которые требуют много времени на подготовку статистических данных, что не требуют более эффективные в этом отношении экспертные подходы, преимущества которых показаны в [1]. В связи с этим актуальной задачей при разработке СОВ является создание моделей обнаружения аномалий на основе экспертных оценок. В работе [2] предложена модель базовых величин (МБВ), которая за счет множества пар «вторжение: величины» и «вторжение: множество сопряженных пар» позволяют отображать аномальное состояние, порождаемое определенным типом вторжения в компьютерной сети. Также, известна модель эталонных величин (МЭВ) [3], которая за счет данных экспертных оценок и МБВ позволяет формировать множества эталонных величин характерных для определенного типа вторжения.

Применение этих моделей при построении СОВ, базирующихся на втором принципе, связано с необходимостью формирования правил, направленных на выявления аномального состояния порожденного атакующими действиями. В связи с этим, целью данной работы является разработка математической модели используемой при формировании соответствующих решающих правил для идентификации аномального состояния в среде окружения. Под средой окружения будем подразумевать совокупность значений сформированных переменных (например, время обработки запроса, загруженность процессора, количество обращений к ресурсу, число подключений и др.), которые можно использовать для оценивания протекающих процессов в информационной системе (ИС) с целью выявления ее аномального состояния. Отображением среды окружения в данном случае могут быть величины входящие в множество V [2]. Для решения поставленной задачи

необходимо построить решающие правила, представляющие собой некоторые утверждения, основанные на результате обобщения определенных теоретических и экспериментальных знаний (данных) и отражающие интуитивное суждение лица, принимающего решение, для обеспечения поиска рационального смыслового решения слабо формализованных задач.

Результаты исследования. Построение решающих правил можно осуществить с помощью соответствующей модели, для создания которой введем множество нечетких идентификаторов (fuzzy identifiers)

$$\boldsymbol{FI}=\bigcup_{i=1}^{d} FI_i = \{FI_1, FI_2, FI_3, \dots, FI_d\},\ (i=\overline{1,d}), \tag{1}$$

где d – количество элементов множества, необходимое для отображения аномального состояния, а FI_i $(i=\overline{1,d})$ – элементы $\boldsymbol{FI}$, каждый из которых принимает одно из текстовых значений, характеризующих в нечеткой форме уровень аномального состояния системы, которое может быть порождено определенными вторжениями. Например, при $d=5$ выражение (1) можно определить как:

$$\boldsymbol{FI}=\bigcup_{i=1}^{5} FI_i = \{FI_1, FI_2, FI_3, FI_4, FI_5\}=\{L, LTH, HTTL, H, LIM\}, \tag{2}$$

где $FI_1=L$, $FI_2=LTH$, $FI_3=HTTL$, $FI_4=H$ и $FI_5=LIM$ соответственно отображаются текстовыми значениями

- «Low (L)» – «Низкий»,
- «Lower than high (LTH)» – «Больше низкий чем высокий»,
- «Higher than the lowest ($HTTL$)» – «Больше высокий чем низкий»,
- «High (H)» – «Высокий»,
- «Limits (LIM)» – «Предельный».

Далее на основе множеств нечетких идентификаторов $\boldsymbol{FI}$ и сопряженных пар $\boldsymbol{MP}$ [2] построим множество решающих правил (solution rule)

$$\boldsymbol{SR}=\{\bigcup_{i=1}^{n} \boldsymbol{SR}_i\}=\{\boldsymbol{SR}_1, \boldsymbol{SR}_2, \boldsymbol{SR}_3, \dots, \boldsymbol{SR}_n\},\ (i=\overline{1,n}), \tag{3}$$

где $\boldsymbol{SR}_i$ – подмножество возможных правил для выявления i-го аномального состояния, порожденного i-м вторжением, при этом

$$\bigcup_{i=1}^{n} \boldsymbol{SR}_i=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ij}\}=\{SR_{11}, SR_{12}, SR_{13}, \dots, SR_{1r_1}\},$$
$$\{SR_{21}, SR_{22}, SR_{23}, \dots, SR_{2r_2}\}, \{SR_{31}, SR_{32}, SR_{33}, \dots, SR_{3r_3}\}, \dots,$$
$$\{SR_{n1}, SR_{n2}, SR_{n3}, \dots, SR_{nr_i}\}, (i=\overline{1,n},\ j=\overline{1,r_i}), \tag{4}$$

где SR_{ij} – j-е правило i-го подмножества возможных правил, а r_i $(i=\overline{1,n})$ – общее количество возможных правил, направленных на обнаружение i-й аномалии.

Отметим, что каждому SR_{ij} соответствует решающее выражение (правило) т.е.:

$$\{SR_{11}=(MP_{11}\in FI_{11}),\ SR_{12}=(MP_{12}\in FI_{12}),\ SR_{13}=(MP_{13}\in FI_{13}), \dots, SR_{1r_1}=(MP_{1r_1}\in FI_{1r_1})\},$$
$$\{SR_{21}=(MP_{21}\in FI_{21}),\ SR_{22}=(MP_{22}\in FI_{22}),\ SR_{23}=(MP_{23}\in FI_{23}), \dots, SR_{2r_2}=(MP_{2r_2}\in FI_{2r_2})\},$$
$$\{SR_{31}=(MP_{31}\in FI_{31}),\ SR_{32}=(MP_{32}\in FI_{32}),\ SR_{33}=(MP_{33}\in FI_{33}), \dots, SR_{3r_3}=(MP_{3r_3}\in FI_{3r_3})\},$$
$$\dots,$$
$$\{SR_{n1}=(MP_{n1}\in FI_{n1}),\ SR_{n2}=(MP_{n2}\in FI_{n2}),\ SR_{n3}=(MP_{n3}\in FI_{n3}),\ \dots,\ SR_{nr_n}=(MP_{nr_n}\in FI_{nr_n})\}. \tag{5}$$

Обобщая выражение (5) с учетом (3) и (4) получим

$$\boldsymbol{SR}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ir_j}\}=\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i}(MP_{ir_j}\in FI_{ir_j})\}=$$

$$\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{r_i} SR_{ir_j}=(MP_{ir_j}\in FI_{ir_j})\}\},\ (i=\overline{1,n},\ j=\overline{1,r_i}), \qquad (6)$$

где SR_{ir_j} есть r_j-е правило выявления аномалии порожденной i-м вторжением, которое буквально интерпретируется как: «Если MP_{ir_j} истинно, то уровень аномального состояния, который может быть порожден i-м вторжением, будет FI_{ir_j} ».

Построение правил обычно осуществляется на основе экспертного подхода, особенно это важно в тех случаях, когда необходимо дать предпочтение одной из альтернатив, например, при каком MP_{ir_j} (6) исход, связанный с FI_{ir_j} будет наиболее объективно отображать состояние системы. Рассмотрим процесс формирования предпочтения для набора альтернатив на конкретном примере.

Пусть для построения подмножества правил $\boldsymbol{SR_1}$ используется r_1 сопряженных пар и d (1) нечетких идентификаторов, один из которых наиболее объективно может отразить состояние среды окружения относительно наличия аномалии. Итак, общее количество возможных альтернативных решений – $d\times r_1$, т.е. на составление каждого правила SR_{1j} $(j=\overline{1,r_1})$ необходимо рассмотреть d альтернативных вариантов правил, для выбора одного из которых воспользуемся методами определения коэффициентов важности (КВ) [4]. Воспользуемся методом ранговых преобразований (РП), поскольку он позволяет воспользоваться услугами нескольких экспертов, в качестве входных данных применяются табличные формы, выходная функция линейная, а трудоемкость низкая [4].

Далее, в качестве примера, определим $d=r_1=5$, тогда

$$\boldsymbol{MP_1}=\{\bigcup_{j=1}^{r_1} MP_{1j}\}=\{MP_{11}, MP_{12}, MP_{13}, MP_{14}, MP_{15}\}=$$

$$\{((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^e\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^e)\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VS}^e),((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^e\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^e)\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{S}^e),$$

$$((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^e\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^e)\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{A}^e),((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^e\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^e)\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{B}^e),((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^e$$

$$\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^e)\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VB}^e)\},$$

а в качестве значений FI_{1j} $(j=\overline{1,5})$ воспользуемся данными из формулы (2). Таким образом, для каждого MP_{1j} $(j=\overline{1,5})$ возможны $d=5$ исходов выявления аномалий, связанных с конкретными значениями нечетких идентификаторов в (2). Наиболее объективный из исходов определим с помощью метода средних рангов (СР) [4].

Ранги SR_{1j}^{k} и КВ	Таблица 1							
SR_{1j}^{k}	J	k	Эксперты	x_{1j}^{k}	λ_{1j}^{k}			
			1	**2**	**3**	**4**		
SR_{11}^{1}	1	1	1	3	1	2	1,75	0,18
SR_{11}^{2}		2	2	1	3	2	2	0,2
SR_{11}^{3}		3	3	2	2	2	2,25	0,23
SR_{11}^{4}		4	2	4	3	3	3	0,3
SR_{11}^{5}		5	4	4	3	4	3,75	0,38
SR_{12}^{1}	2	1	2	3	1	2	2	0,2
SR_{12}^{2}		2	1	2	1	2	1,5	0,15
SR_{12}^{3}		3	3	1	2	3	2,25	0,23
SR_{12}^{4}		4	3	4	2	2	2,75	0,28
SR_{12}^{5}		5	3	2	3	4	3	0,3
SR_{13}^{1}	3	1	2	3	2	4	2,75	0,28
SR_{13}^{2}		2	3	2	2	1	2	0,2
SR_{13}^{3}		3	2	3	1	1	1,75	0,18
SR_{13}^{4}		4	3	4	3	4	3,5	0,35
SR_{13}^{5}		5	4	3	2	4	3,25	0,33
SR_{14}^{1}	4	1	4	2	2	4	3	0,3
SR_{14}^{2}		2	2	4	3	2	2,75	0,28
SR_{14}^{3}		3	3	1	2	2	2	0,2
SR_{14}^{4}		4	1	2	3	1	1,75	0,18
SR_{14}^{5}		5	2	4	4	3	3,25	0,33
SR_{15}^{1}	5	1	4	4	3	3	3,5	0,35
SR_{15}^{2}		2	2	4	4	3	3,25	0,33
SR_{15}^{3}		3	2	4	3	3	3	0,3
SR_{15}^{4}		4	4	3	2	3	3	0,3
SR_{15}^{5}		5	2	2	4	3	2,75	0,28

Согласно этого метода, в качестве примера, воспользуемся суждениями 4-х экспертов относительно $d=5$ возможных исходов SR_{1j}^{k} $(k=\overline{1,d},\ \ j=\overline{1,r_1})$ по каждому j-му правилу. Например, для первого правила подмножество альтернативных решений будет

$$\bigcup_{k=1}^{d} SR_{11}^{k} = \{SR_{11}^{1},\ SR_{11}^{2},\ SR_{11}^{3},\ SR_{11}^{4},\ SR_{11}^{5}\} =$$

$$\{((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^e \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^e) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^e) \in L,\ ((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^e \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^e) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{S}^e) \in LTH,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^e \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^e) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{A}^e) \in HTTL,\ ((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^e \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^e) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^e) \in H,$$

$$((\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^e \vee \underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^e) \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^e) \in LIM\}.$$

Далее на основе РП определим КВ, которые отражаются величиной λ. Его минимальное значение свидетельствует о большей предпочтительности альтернативы, т.е. ее КВ более высокий. Для правила SR_{11} произведем расчеты значений x_{1j}^k и λ_{1j}^k по каждому из возможных исходов SR_{11}^k $(k=\overline{1,5})$: x_{11}^1=(1+3+1+2)/4=1,75; x_{11}^2=(2+1+3+2)/4=2; x_{11}^3= (3+2+2+2)/4=2,25; x_{11}^4 =(2+4+3+3)/4=3; x_{11}^5=(4+4+ 3+4)/4=3,75. Значение КВ определяется как $\lambda_{1j}^k = x_{1j}^k / N$, где N – сумма всех рангов ($N=10$). По результатам, занесенным в табл. 1 видно, что лучший исход имеет, SR_{11}^1 поскольку $\bigwedge_{k=1}^{5} \lambda_{11}^k = \lambda_{11}^1 = 0{,}18$.

Аналогично произведем расчеты для SR_{1j}^k $(j=\overline{2,5})$: SR_{12}^k – x_{12}^1=(2+3+1+2)/4=2; x_{12}^2 = (1+2+1+2)/4=1,5; x_{12}^3 =(3+1+2+3)/4=2,25; x_{12}^4 =(3+ 4+2+2)/4=2,75; x_{12}^5 =(3+2+3+4)/4=3; SR_{13}^k – x_{13}^1 = (2+3+2+4)/4=2,75; x_{13}^2 =(3+2+2+1)/4=2; x_{13}^3 =(2+3 +1+1)/4=1,75; x_{13}^4 =(3+4+3+4)/4=3,5; x_{13}^5 =(4+3+2 +4)/4=3,25; SR_{14}^k – x_{14}^1 =(4+2+2+4)/4=3; x_{14}^2 =(2+4 +3+2)/4=2,75; x_{14}^3 =(3+1+2+2)/4=2; x_{14}^4 =(1+2+3+ 1)/4=1,75; x_{14}^5 =(2+4+4+3)/4=3,25; SR_{15}^k – x_{15}^1 =(4+ 4+3+3)/4=3,5; x_{15}^2 =(2+4+4+3)/4=3,25; x_{15}^3 =(2+4+3 +3)/4=3; x_{15}^4 =(4+3+2+3)/4=3; x_{15}^5 =(2+2+4+3)/4= 2,75.

По результатам вычислений (см. табл. 1) видно, что лучший исход для правил SR_{12}, SR_{13}, SR_{14}, SR_{15} имеют соответственно альтернативные варианты SR_{12}^2, SR_{13}^3, SR_{14}^4, SR_{15}^5.

Полученные данные можно использовать в качестве конкретных значений при построении реальных правил в практических СОВ. С этой целью, с учетом (6), осуществим структурирование необходимых данных путем ввода матриц инициализации (МІ) для множеств ***FI*** и ***MP***, которые обозначим соответственно $FI(n, r_n)$ и $MP(n, r_n)$, т.е.

$$FI(n, r_n)= \begin{Vmatrix} FI(1,1), & FI(1,2), & FI(1,3), & \dots, & FI(1,r_n) \\ FI(2,1), & FI(2,2), & FI(2,3), & \dots, & FI(2,r_n) \\ FI(3,1), & FI(3,2), & FI(3,3), & \dots, & FI(3,r_n) \\ & & \dots & & \\ FI(n,1), & FI(n,2), & FI(n,3), & \dots, & FI(n,r_n) \end{Vmatrix} \text{ и}$$

$$MP(n, r_n)= \begin{Vmatrix} MP(1,1), & MP(1,2), & MP(1,3), & \dots, & MP(1,r_n) \\ MP(2,1), & MP(2,2), & MP(2,3), & \dots, & MP(2,r_n) \\ MP(3,1), & MP(3,2), & MP(3,3), & \dots, & MP(3,r_n) \\ & & \dots & & \\ MP(n,1), & MP(n,2), & MP(n,3), & \dots, & MP(n,r_n) \end{Vmatrix}. \quad (7)$$

Например, при n=3 и r_n=5 на основе экспертных оценок [4] были определены следующие МІ $FI(3, 5)$ и $MP(3, 5)$, т.е.

$$FI(3, 5)= \begin{Vmatrix} LOW & LTH & HTTL & H & LIM \\ LOW & LOW & HTTL & H & LIM \\ LOW & LTH & HTTL & H & H \end{Vmatrix} \text{ И}$$

$$MP(3,5)=\left\|\begin{array}{ccccc}
\begin{array}{l}(\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\\ \underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{VS}^{e}\end{array} &
\begin{array}{l}(\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\\ \underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{S}^{e}\end{array} &
\begin{array}{l}(\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\\ \underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{A}^{e}\end{array} &
\begin{array}{l}(\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\\ \underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{B}^{e}\end{array} &
\begin{array}{l}(\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\\ \underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{VB}^{e}\end{array}\\
\hline
\begin{array}{l}\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{VS}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{S}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{A}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{B}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{NPSA}\cong\underset{\sim}{B}^{e}\wedge\\ \underset{\sim}{t}_{NCC}\cong\underset{\sim}{VB}^{e}\end{array}\\
\hline
\begin{array}{l}\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\\ \underset{\sim}{t}_{NVC}\cong\underset{\sim}{VS}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\\ \underset{\sim}{t}_{NVC}\cong\underset{\sim}{S}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\\ \underset{\sim}{t}_{NVC}\cong\underset{\sim}{A}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\\ \underset{\sim}{t}_{NVC}\cong\underset{\sim}{B}^{e}\end{array} &
\begin{array}{l}\underset{\sim}{t}_{VCA}\cong\underset{\sim}{S}^{e}\wedge\\ \underset{\sim}{t}_{NVC}\cong\underset{\sim}{VB}^{e}\end{array}
\end{array}\right\|, \quad (8)$$

где $\underset{\sim}{t}_{NCC}$, $\underset{\sim}{t}_{SPR}$, $\underset{\sim}{t}_{DBR}$, $\underset{\sim}{t}_{NPSA}$, $\underset{\sim}{t}_{VCA}$, $\underset{\sim}{t}_{NVC}$ – текущие значения величин «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», «Virtual Channel Age (*VCA*)» – «Возраст виртуального канала», «Numbers of Virtual channels (*NVC*)» – «Количество виртуальных каналов» и являются идентификаторами величин [2] в среде окружения. Используемый в (8) знак «$\cong$» – интерпретируется как «Нечеткое равно» и указывает на то, что текущее значение величины (например, $\underset{\sim}{t}_{SPR}$) находящегося слева от «$\cong$» наиболее близко к одному из элементов (например, $\underset{\sim}{L}^{e}$) из заданного множества (например, $T^{e}_{SPR}=\{\underset{\sim}{L}^{e}, \underset{\sim}{A}^{e}, \underset{\sim}{H}^{e}\}$), который указывается справа от «$\cong$», т.е. запись $\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}$ можно интерпретировать как: «$\underset{\sim}{t}_{SPR}$ наиболее близко расположен к $\underset{\sim}{L}^{e}$ входящего в T^{e}_{SPR}».

Обсуждение результатов. Далее с учетом MI (при $i=1$, $j=\overline{1,5}$) для $FI(n, r_n)$ и $MP(n, r_n)$ на основе (7) и (8) построим подмножество правил $\boldsymbol{SR_1}$ для выявления аномального состояния, которое может быть порождено таким вторжением, как Dos (DDos) атака.

$$\boldsymbol{SR_1}=\left\{\begin{array}{l}
SR_{11}=((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VS}^{e})\in L,\\
SR_{12}=((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{S}^{e})\in LTH,\\
SR_{13}=((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{A}^{e})\in HTTL,\\
SR_{14}=((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{B}^{e})\in H,\\
SR_{15}=((\underset{\sim}{t}_{SPR}\cong\underset{\sim}{L}^{e}\vee\underset{\sim}{t}_{DBR}\cong\underset{\sim}{S}^{e})\wedge\underset{\sim}{t}_{NCC}\cong\underset{\sim}{VB}^{e})\in LIM.
\end{array}\right\} \quad (9)$$

Отметим, что правило SR_{15} в (9) буквально можно интерпретировать как: «Если $\underset{\sim}{t}_{SPR} \cong \underset{\sim}{L}^{e}$ или $\underset{\sim}{t}_{DBR} \cong \underset{\sim}{S}^{e}$ и при этом $\underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e}$, то уровень аномального состояния, который может быть порожден Dos-атакой, будет LIM (Предельный)».

Из подмножества правил (9) видно, что для каждой сопряженной пары из SR_{1j} $(j=\overline{1,5})$ определены конкретные значения из ***FI*** согласно расчетов КВ с помощью метода РП. Используя эти данные по аналогии можно составить правила для выявления аномалий порожденных спуфингом и сканированием [2, 3]. Так с учетом (7) и (8) при $i=\overline{2,3}$ и $j=\overline{1,5}$ наборы правил $\boldsymbol{SR_2}$ (10) и $\boldsymbol{SR_3}$ (11) будут иметь следующий вид:

$$\boldsymbol{SR_2}=\{SR_{21}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VS}^{e}) \in L,\ SR_{22}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{S}^{e}) \in LTH,$$

$$SR_{23}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{A}^{e}) \in HTTL,\ SR_{24}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{B}^{e}) \in H,$$

$$SR_{25}=(\underset{\sim}{t}_{NPSA} \cong \underset{\sim}{B}^{e} \wedge \underset{\sim}{t}_{NCC} \cong \underset{\sim}{VB}^{e}) \in LIM\} \text{ и} \qquad (10)$$

$$\boldsymbol{SR_3}=\{SR_{31}=(\underset{\sim}{t}_{VCA} \cong \underset{\sim}{S}^{e} \wedge \underset{\sim}{t}_{NVC} \cong \underset{\sim}{VS}^{e}) \in L,\ SR_{32}=(\underset{\sim}{t}_{VCA} \cong \underset{\sim}{S}^{e} \wedge \underset{\sim}{t}_{NVC} \cong \underset{\sim}{S}^{e}) \in LTH,$$

$$SR_{33}=(\underset{\sim}{t}_{VCA} \cong \underset{\sim}{S}^{e} \wedge \underset{\sim}{t}_{NVC} \cong \underset{\sim}{A}^{e}) \in HTTL,\ SR_{34}=(\underset{\sim}{t}_{VCA} \cong \underset{\sim}{S}^{e} \wedge \underset{\sim}{t}_{NVC} \cong \underset{\sim}{B}^{e}) \in H,$$

$$SR_{35}=(\underset{\sim}{t}_{VCA} \cong \underset{\sim}{S}^{e} \wedge \underset{\sim}{t}_{NVC} \cong \underset{\sim}{VB}^{e}) \in LIM\}. \qquad (11)$$

Выводы. Предложенная в работе модель решающих правил на нечеткой логике, позволяет за счет использования множества пар «вторжение : величины», «вторжение : множество сопряженных пар» и МЭВ отображать аномальное состояние, порождаемое определенным типом кибератак в компьютерной сети. На основе этой модели были разработаны примеры правил для обнаружения таких вторжений как сканирование, спуфинг и Dos-атака, которые могут практически быть использованы для усовершенствования реальных систем обнаружения вторжений применяющих механизмы выявления аномалий, порожденных атакующими действиями в компьютерных системах.

ЛИТЕРАТУРА

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

[2] Ахметов Б.С., Корченко А.А., Жумангалиева Н.К. Модель базовых величин для контроля аномальности состояния среды окружения / Вестник НАН РК. – 2016.– №1.

[3] Ахметов Б.С., Корченко А.А., Жумангалиева Н.К. Базовые модели эталонных величин для систем обнаружения вторжений / Вестник МКТУ Х.А.Ясави . – 2015. – №4.

[4] Использование методов экспертного оценивания в системах обнаружения вторжений / Б.С. Ахметов, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // Інформаційна безпека. – 2014. – №3 (15); №4 (16). – С. 34-43.

[5] 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.

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

[7] 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.

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

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

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

[11] 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.

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

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

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

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

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

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

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

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

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

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

REFERENCES

[1] Korchenko O. G. Creation of systems of information security on indistinct sets [Text]: Theory and practical decisions / O. G. Korchenko. – To.: MK-Press, 2006. 320 pages

[2] Akhmetov B. S., Korchenko A.A., Zhumangaliyeva N. K. Model of basic sizes for control of anomaly of a condition of the environment the Environment / Messenger NAN RK. 2016. No. 1.

[3] Akhmetov B. S., Korchenko A.A., Zhumangaliyeva N. K. Basic models of reference sizes for systems of detection the MKTU Invasions / Bulletin of H.A.Yasavi. 2015. No. 4.

[4] Use of methods of expert estimation in systems of detection of invasions / B. S. Akhmetov, A.A. Korchenko, S. T. Akhmetova, N. K. Zhumangaliyeva//a _nformats_yna of a bezpek. – 2014. – No. 3 (15); No. 4 (16). Page 34-43.

[5] The Kazakhstan government website is cracked in revenge for torrents [An electronic resource] / TENGRINEWS.KZ//TOO "EML": [TENGRINEWS.KZ]. □Электрон. it is given. □ 2012. □ February 8. □ Access mode: WorldWideWeb. □URL: http://tengrinews.kz/internet/kazahstanskiy-pravitelstvennyiy-sayt-vzloman-otmestku-207728/. □Загл. about a title. screen.

[6] Korchenko O. G. Creation of systems of information security on indistinct sets [Text]: Theory and practical decisions / O. G. Korchenko. □K.: MK-Press, 2006. □ 320 pages.

[7] Volyanska V.V.Sistema виявлення аномалій on основі the nech_tkikh of models [Text] / V. V. Volyanska, A.O. Korchenko, Є. V. Pats_ra/ZB. sciences. the ave. to a _nstitut of problems моделювання in енергетиці Ukra§ni's NAN ім. Є Pukhova. □Львів: Software "Sistemi, technologist і ї, _nformats_yn_poslug", 2007.□ [Special випуск]. □ T.2.□ of Page 56-60.

[8] Korchenko of O. G. Sistemi to a zakhist інформац і ї [Text]: Монографія / O.G. Корченко.□ To.: NAU, 2004.□ 264 pages.

[9] Aksen, B. A. Electronic systems of calculations in Internet: from a real show-window to virtual / B. A. Aksen//the Confidant, - 1996. - No. 6 - Page 43 - 48.

[10] Anderson, R. UEPS - an electronic wallet of the second generation / R. Aderson//the Confidant. 1996.№ 1. Page 49-53.

[11] Galatenko, VA. Bases of information security: manual/VA. Galatenko; under the editorship of the academician of the Russian Academy of Sciences V. B. Betelin, 4 prod. - the M.:internt University the .informatsionnykh of technologies; BINOMIAL. Laboratory of knowledge, 2008. - 205 pages.

[12] Gerasimenko, VA. Information security in the automated systems of data processing: development, results, Gerasimenko's prospects/VA//Zarubuzhenaya radio electronics.-1993.№3. - Page 3-21.

[13] Assessment of safety of information technologies / A.P. Trubachev, I.A. Semichev, V. N. Shakunov, etc. M.: VULTURE of RIA, 2001.-388 with I.:it.

[14] Yashchenko, V. V. Introduction to cryptography / Under the general editorship of V. V. Yashchenko. - SPb.: St. Petersburg, 2001. - 288 pages: silt

[15] Grishina N. V. Model of the potential violator of object of informatization//Materials V Mezhdunarod

[16] Domarev V. V. Safety of information technologies. Methodology of creation of systems protection / Kiev: LLC TID of "DS", 2002.

[17] Aleksentsev A. I. Definition of structure of confidential information//Reference book of the secretary and office manager. No. 2, 3. 2003.

[18] Stepanov E. A., Korneev I. K. Information security and information security. — M, 2001.

[19] Lepyokhin A. N. Investigation of crimes against information security. Teoretiko-pravovye and applied aspects. M.: Theseus, 2008. — 176 pages.

[20] Lepyokhin A. N. Investigation of crimes against information security. Teoretiko-pravovye and applied aspects. M.: Theseus, 2008. 176 pages.

[21] Schneier, B. Applied cryptography. Protocols, algorithms, source texts in the Xi language / B. Schneier. M.: TRIUMPH, 2002. 816 pages.

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕГІ АУЫТҚЫМАЛЫҚ ЖАҒДАЙЫН АНЫҚТАУҒА НЕГІЗДЕЛГЕН ШЕШУШІ ЕРЕЖЕЛЕРДІҢ МОДЕЛІ

Б.С. Ахметов*, А.А. Корченко, Н.К. Жумангалиева *****

*-Қ.И. Сәтбаев атындағы Қазақ Ұлттық Техникалық зерттеу Университет, Ақпарттық және телекоммуникациялық технологиялар институты. *Алматы*.bakhytzhan.akhmetov.54@mail.ru,

**- Ұлттық авиациалық университет, кафедра Ақпараттық технологиялар қауіпсіздігі, *Украина, Киев*annakor@ukr.net

***- Қ.И. Сәтбаев атындағы Қазақ Ұлттық Техникалық зерттеу Университет, Ақпарттық және телекоммуникациялық технологиялар институты. *Алматы, Қазақстан*_nazym_k.81@mail.ru

Түйін сөздер: кибершабуыл, шабуылдарды анықтау жүйелері, жүйелік трафиктегі аномалия, компьютерлік жүйедегі ауытқымалы жағдайды анықтау, коньюгат жұптар жиынтығы, шешуші ережелер, сарапшы баға.

Аннотация. Ауытқымалы жағдайларды анықтауға негізделген қазіргі заманғы шабуылдардың кемшілігі – олар статистикалық мәліметтердің дайындығына көп уақыт қажет ететін математикалық модельдердің қолданылуына негізделген. Сарапшы тәсілге негізделген математикалық модельдер бұл жағынан тиімді болып табылады, бірақ олардың өз қызметтерін атқаруы үшін сәйкес шешуші ережелерді қолдану қажет. Жұмыста бұл міндетті шешу үшін шабуылдар жиынтығына: «шама: шабуылдар» және «шабуылдар: коньюгат жұптар жиынтығы» негізінде айқын емес логиканың шешуші ережелерінің моделі ұсынылды. Сонымен қатар шама бірлігі эталондарының модельдері компьютерлік желідегі кибершабуылдың белгілі бір туындатқан аномалиялық жағдайды бейнелейді. Бұл модельдің негізінде сканерлеу, спуфинг және DOS – шабуыл сияқты шабуылдар түрін анықтауға арналған ережелер үлгісі құрастырылды. Бұл ережелер компьютерлік жүйедегі шабуыл әрекеттері туғызған аномалиялық жағдайды анықтауға қолданылатын шабуылдардың шынайы жүйесін жетілдіру үшін қолданылуы мүмкін.

Поступила 17.06.2016 г.