в порівнянні з відомим методом розподілу ключів Діффі-Хеллмана, запропонований метод забезпечує для кожного користувача майже вдвічі меншу складність обчислень. Крім того, запропонований метод має простішу процедуру завдання параметрів.

ЛІТЕРАТУРА

1. Menezes A.J., van Oorschot P.C., Vanstone S.A. Handbook of Applied Cryptography. - CRC Press, 2001. 816 p.
2. W. Diffie, M.E. Hellman. New directions in cryptography // IEEE Transactions on Information Theory. – №22, 1976. – Pp. 644–654.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. - 816 с.
4. W. Diffie, P.C. van Oorschot, M.J. Wiener. Authentication and authenticated key exchanges // Designs, Codes and cryptography. – №2, 1992. – Pp. 107–125.
5. A.M. Odlyzko. Discrete logarithms: the past and the future // Designs, Codes and Cryptography. – №19, 2000. – Pp. 129–154.
6. Smith P. and Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms // In Advances in Cryptology Asiacrypt ’94, Springer-Verlag. – 1995. – Pp. 357–364.
7. Bleichenbacher D., Bosma W., and Lenstra A. Some remarks on Lucas-based cryptosystems // In Advances in Cryptology Crypto ’95, Springer-Verlag. – 1995. – Pp.386–396.
8. Маркушевич А.И. Возвратные последовательности. - М.: Наука, 1975. - 48 с.
9. Кнут Д. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. - М.: Вильямс, 2004.- 832 с.

Надійшла: 18.10.2012 р.

Рецензент: д.т.н., професор Хорошко В.О.

УДК 004.056.53(045)

Стасюк А.И., Корченко А.А.

МЕТОД ВЫЯВЛЕНИЯ АНОМАЛИЙ ПОРОЖДЕННЫХ КИБЕРАТАКАМИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Одним из решений обеспечения безопасности, являются системы обнаружения вторжений, построенные по аномальному принципу. Такие системы обычно основываются на математических методах, требующих много времени на подготовку статистических данных. Поэтому необходимы более эффективные методы, основанные на экспертных подходах. Для решения этой задачи предлагается метод, базирующийся на математических моделях и методах нечеткой логики, и содержащий восемь базовых этапов (выбор метода обработки нечетких данных, выбор метода определения коэффициента важности, формирование множеств атак и параметров, формирование эталонов параметров, фаззификация параметров, формирование множества эвристических правил, определение матриц инициализации, формирование результата), раскрывающие процесс выявления аномального состояния, порождаемого определенным типом кибератак в ИС. Этот метод можно использовать для создания или усовершенствования существующих систем выявления кибератак в компьютерных сетях.

Ключевые слова: кибератака, системы обнаружения вторжений, атаки в компьютерных системах, обнаружение аномалий в компьютерных системах, эвристические правила, базовая модель параметров, универсальная модель эталонов, модель эвристических правил, построение решающих правил, метод обнаружения аномалий, метод обнаружения атак.

Интенсивное развитие информационных технологий оказало положительное влияние на все сферы человеческой деятельности. Вместе с этим наблюдаются и побочные эффекты, в первую очередь в связи с тем, что ресурсы информационных систем (РИС) все больше подвергаются воздействиям кибератак, под которыми понимаются меры, предпринимаемые для подрыва безопасности информационной системы (ИС) или реализация угроз характеристикам безопасности РИС посредством использования их уязвимостей. Современный спектр атак на РИС достаточно широкий и только основываясь на базовые признаки их можно классифицировать по: автоматизации; взаимодействию с политикой безопасности; дистанционности; действию, порожденному несанкционированным доступом; внешнему проявлению; инициализационному условию; инструментальным средствам; наличию обратной связи; нарушению базовых характеристик безопасности; природе

взаимодействия; реляционным признакам; специфике реализации; направленности результата; степени сложности; типу базового ресурса; семиуровневой эталонной модели [1]. В стремительно развивающейся информационной среде появляются новые виды угроз, порождающие новые виды кибератак на ее ресурсы. В этой связи существует потребность в системах безопасности построенных на основе методов, позволяющих анализировать, контролировать, прогнозировать и блокировать такие атаки. Одним из решений защиты РИС от указанных кибератак, являются системы обнаружения вторжений (СОВ), построенные по аномальному принципу. Такие системы обычно основываются на математических методах, требующих много времени на подготовку статистических данных. Поэтому необходимы более эффективные методы основанные на экспертных подходах.

Отметим, что несанкционированные воздействия на ресурсы ИС оказывают влияние на среду их окружения и порождают в ней определенные аномалии. Такая среда обычно слабоформализованная, нечетко определенная и для выявления атак, породивших аномалии в этой среде необходимы соответствующие методы. В работах [1-3] показана эффективность применения математического аппарата нечетких множеств для решения такого рода задач, а его использование для формализации подхода к выявлению атак, позволит повысить эффективность разрабатываемых СОВ. В этой связи, целью данной работы является разработка метода выявления аномалий, использование которого позволит синтезировать эффективно функционирующие системы, осуществляющие обнаружение вторжений по аномальному состоянию параметров (например, сетевого трафика), характеризующих среду окружения. Под такой средой 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 ИС с целью выявления ее аномального состояния. В работах [5-7] предложена базовая модель параметров (БМП), универсальная модель эталонов (УМЭ) и модель эвристических правил (МЭП), которые возьмем за основу разработки соответствующего метода. Реализация метода осуществляется за восемь базовых этапов: 1) выбор метода обработки нечетких данных, 2) выбор метода определения КВ, 3) формирование множеств атак и параметров, 4) формирование эталонов параметров, 5) фаззификация параметров, 6) формирование множества ЭП, 7) определение матриц инициализации, 8) формирование результата, которые представлены на рис. 1. Опишем каждый из них.

Этап 1 – выбор метода обработки нечетких данных. На этом этапе осуществляется выбор методов обработки нечетких данных относительно заданных критериев. В работе [1] рассмотрены три базовые группы соответствующих методов – формирования функций принадлежности (четырнадцать методов – $МФФП_1$, $МФФП_2$, …, $МФФП_{14}$, например, метод корректировки параметров (КП), метод интервальных оценок (МИО), метод лингвистических термов с использованием статистических данных (МЛТС) и др.), сравнения функций принадлежности (восемь методов – $МСФП_1$, $МСФП_2$, …, $МСФП_8$, например, α-уровневое расстояние (АУР), функция упорядочения нечетких подмножеств (ФУ), метод поиска “центра тяжести” (ЦТ) и др.) и нечеткой арифметики (четырнадцать методов – $МНА_1$, $МНА_2$, …, $МНА_{14}$, например, максминная композиция (ММК), α-уровневый принцип обобщения (АУПО), метод линейной аппроксимации по локальным максимумам (ЛАЛМ) и др.), из которых посредством процедур выбора МНА, МСФП и МФФП отбирается один из представителей. Процесс выбора осуществляется на основе заданных критериев. Так для всех групп методов базовыми критериями являются – используемый класс ФП и экспертная информация, для МФФП –использование ранговых оценок и число привлекаемых экспертов, а для МСФП – применение α-уровневого подхода. Если несколько методов будут отвечать установленным критериям, то окончательное решение о выборе будет основываться на предпочтении эксперта. Например, согласно принятых критериев для каждой группы возможных методов $МФФП_i$ ($i = \overline{1,14}$), $МСФП_j$ ($j = \overline{1,8}$) и $МНА_k$ ($k = \overline{1,14}$), после реализации процедуры выбора определяется

соответственно метод ЛАЛМ, АУР и МЛТС, которые совместно будут использоваться для обработки нечетких данных при решении задачи выявления аномального состояния в компьютерных системах.

Этап 2 – выбор метода определения коэффициента важности (МОКВ). Этап ориентирован на выбор (согласно установленным критериям) метода формирования коэффициента важности (КВ) из заданного множества. В работе [4] рассмотрено двадцать пять МОКВ ($МОКВ_1$, $МОКВ_2$, …, $МОКВ_{25}$, например, метод средних рангов (СР), мультипликативная свертка Кини (МСК), метод случайных векторов (СЛВ) и др.), среди которых в процессе реализации процедуры выбора определяется рабочий метод. Если несколько методов будут отвечать установленным критериям, то в данном случае окончательным решением о выборе будет принимать эксперт. Приоритет метода определяется посредством процедуры выбора МОКВ согласно таких критериев как: форма выражения входных (ВхД) и выходных (ВыхД) данных; трудоемкости и рекомендуемой шкалы [4]. Например, согласно установленных критериев и приоритетов эксперта из множества $МОКВ_i$ ($i = \overline{1,25}$) выбирается метод средних рангов (СР).

Этап 3 – формирование множеств атак и параметров. Этап предназначен для формирования множества атак и соответствующего им множества параметров для выявления аномального состояния. На основании входных параметров среды окружения с использованием БМП [5] формируются множество возможных атак $\boldsymbol{AT}=\bigcup_{i=1}^{n} AT_i$ и соответствующее им множество возможных параметров $\boldsymbol{P}=\bigcup_{i=1}^{m} P_i$, согласно значений которых (например, P_1=*КВК*, P_2=*ВВК*, P_3=*КОП*, P_4=*СОЗ*, P_5=*ЗМЗ*, P_6=*КПОА*, …, P_m) с учетом решений экспертов можно выявить аномальное состояние, порождаемое определенным элементом из множества $\boldsymbol{AT}$, например, (AT_1=*SN*, AT_2=*DS*, AT_3=*SP*, …, AT_n) [5]. Для выявления аномального состояния каждому типу атаки множества $\boldsymbol{AT}$ ставится в соответствие подмножество набора параметров $\boldsymbol{P_n}$ из множества $\boldsymbol{P}$, по которым можно обнаружить подозрительную активность в системе. Таким образом, формируется множество пар – “атака→параметры” $\boldsymbol{AT \rightarrow P_n}=\bigcup_{i=1}^{n}(AT_i \rightarrow \bigcup_{j=1}^{k_i} P_{ij})$, в котором каждой атаке будет соответствовать набор параметров ($AT_1 \rightarrow \{P_1, P_2\}$), ($AT_2 \rightarrow \{P_3, P_4, P_5\}$), ($AT_3 \rightarrow \{P_3, P_6\}$), …, например, (*SN*→{*КВК*, *ВВК*}), (*DS*→{*КОП*, *СОЗ*, *ЗМЗ*}), и (*SP*→{*КОП*, *КПОА*}).

Этап 4 – формирование эталонов параметров. Этот этап направлен на получение эталонных величин, которые необходимы для измерения текущих значений параметров характеризующих среду окружения. На основании входных данных (см. этап 3) $\boldsymbol{P}=\bigcup_{i=1}^{m} P_i$, выбранного на первом этапе МФФП и с помощью процедуры формирования эталонных параметров получаем соответствующие значения эталонов ЛП для всех $T_{ij}^{e} = \bigcup_{f=1}^{r} T_{ij}^{ef}$, например, $\{T_{КВК}^{ef}, T_{ВВК}^{ef}, T_{КОП}^{ef}, T_{СОЗ}^{ef}, T_{ЗМЗ}^{ef}, T_{КПОА}^{ef}, ...\}$. Так, например, для КПОА [5] с использованием $МФФП_6$ = МЛТС [1] можем получить эталонные значения $T_{КПОА}^{e}=\bigcup_{i=1}^{3} T_{КПОА}^{ei}$ и осуществить визуализацию лингвистических термов для **КПОА** – $\{T_{КПОА}^{e1}, T_{КПОА}^{e2}, T_{КПОА}^{e3}\}=\{\underset{\sim}{М}^{e}, \underset{\sim}{С}^{e}, \underset{\sim}{Б}^{e}\}$. Далее с помощью процедуры визуализации формируется графическое представление эталонов лингвистических термов $\{\underset{\sim}{М}^{e}, \underset{\sim}{С}^{e}, \underset{\sim}{Б}^{e}\}$.

Этап 5 – фаззификация параметров. На этом этапе осуществляется преобразование набора подмножеств параметров, характеризующих текущее состояние системы, в соответствующие им текущие значения нечетких переменных. На основании БМП [5], выбранного (на первом этапе) метода получения ФП и с помощью процедуры фаззификации, реализующей один из МФФП формируется набор ЛП, каждая из которых представляется кортежем $<P_{ij}, T_{ij}, U_{ij}>$. Далее на основе процедуры, связывающей с каждой атакой из множества ***A*** конкретный набор параметров из множества ***P***, получаем множества связок [5] $\boldsymbol{AT \rightarrow P_n} = \bigcup_{i=1}^{n} (AT_i \rightarrow \bigcup_{j=1}^{k_i} P_{ij})$. Так, например, с использованием множества пар "атака→параметры", $МФФП_6$=МЛТС (см. этап 1) и набора кортежей, отображающих соответствующие значения ЛП для атак SN (при $P_{11}, P_{12} – <КВК, T_{КВК}, U_{КВК}>, <ВВК, T_{ВВК}, U_{ВВК}>$), DS (при $P_{21}, P_{22}, P_{23} – <КОП, T_{КОП}, U_{КОП}>, <СОЗ, T_{СОЗ}, U_{СОЗ}>, <ЗМЗ, T_{ЗМЗ}, U_{ЗМЗ}>$) и SP (при $P_{31}, P_{32} – <КОП, T_{КОП}, U_{КОП}>, <КПОА, T_{КПОА}, U_{КПОА}>$) формируются текущие значения нечетких переменных среды окружения $\underset{\sim}{t}_{КОП}$, $\underset{\sim}{t}_{СОЗ}$, $\underset{\sim}{t}_{ЗЗМ}$, $\underset{\sim}{t}_{КПОА}$, $\underset{\sim}{t}_{ВВК}$ и $\underset{\sim}{t}_{КВК}$, которые соответственно отражают величины КОП, СОЗ, ЗМЗ, КПОА, ВВК и КВК.

Этап 6 – формирование множества эвристических правил (ЭП). Этап ориентирован на формирование ЭП необходимых для измерения текущего состояния системы относительно эталонных параметров. На основании множеств лингвистических идентификаторов $\boldsymbol{LI} = \bigcup_{i=1}^{d} LI_i$ [5] и наборов логико-лингвистических связок $\boldsymbol{LC} = \bigcup_{i=1}^{n} (\bigcup_{j=1}^{c_n} LC_{ij})$ [5] (использующих конкретные значения лингвистических термов, определенных на четвертом этапе) формируется множество альтернатив ER_{ij}^{k} $(i = \overline{1,n};\ k = \overline{1,d};\ j = \overline{1,r_n}$, где n – количество атак, r_n – количество правил для выявления i-й атаки, а d – количество альтернативных вариантов для формирования одного правила). Например, для первой атаки и первого правила это будет $\bigcup_{k=1}^{d} ER_{11}^{k} = \{ ER_{11}^{1},\ ER_{11}^{2},\ ...,\ ER_{11}^{5} \}$. Для построения ЭП, отображаемых выражением $\bigcup_{i=1}^{n} \{ \bigcup_{j=1}^{r_i} ER_{ir_j} = (LC_{ir_j} \rightarrow LI_{ir_j}) \}$ [7]. Формирование правил осуществляется на основе множества альтернатив с помощью процедуры их выбора, которая базируются на одном из методов формирования КВ (см. этап 2). Далее, отобранные LI_{ir_j} на этапе 7 используются в качестве данных для матриц инициализации, которые посредством процедуры инициализации передают конкретные значения в LC_{ir_j} и LI_{ir_j}, формируя таким образом непосредственные наборы эвристических правил, например, $\boldsymbol{ER_2} = \{$ $ER_{21} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОМ}^{e}) \rightarrow Н$, $ER_{22} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{М}^{e}) \rightarrow БНВ$, $ER_{23} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{С}^{e}) \rightarrow БВН$, $ER_{24} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{Б}^{e}) \rightarrow В$, $ER_{25} = (\underset{\sim}{t}_{КПОА} \cong \underset{\sim}{Б}^{e} \wedge \underset{\sim}{t}_{КОП} \cong \underset{\sim}{ОБ}^{e}) \rightarrow П$ } [7].

Этап 7 – определение матриц инициализации. Этап предназначен для формирования исходных данных (в виде набора матриц) для процедуры инициализации ЭП. На основе полученных конкретных значений всех LI_{ir_j}, с помощью процедуры выбора альтернатив для ЭП и данных по конкретным связкам LI_{ij} (см. этап 6) соответственно определяем матрицы инициализации для лингвистических идентификаторов $LI(n, r_n)$ и лингвистических связок $LC(n, r_n)$, где n – количество атак, а r_n – количество правил для выявления i-й атаки. Например, такие матрицы для использования на этапе 6 при построении ЭП имеют вид – LI(3, 5) и LC(3, 5), а их конкретные элементы отображены в [7].

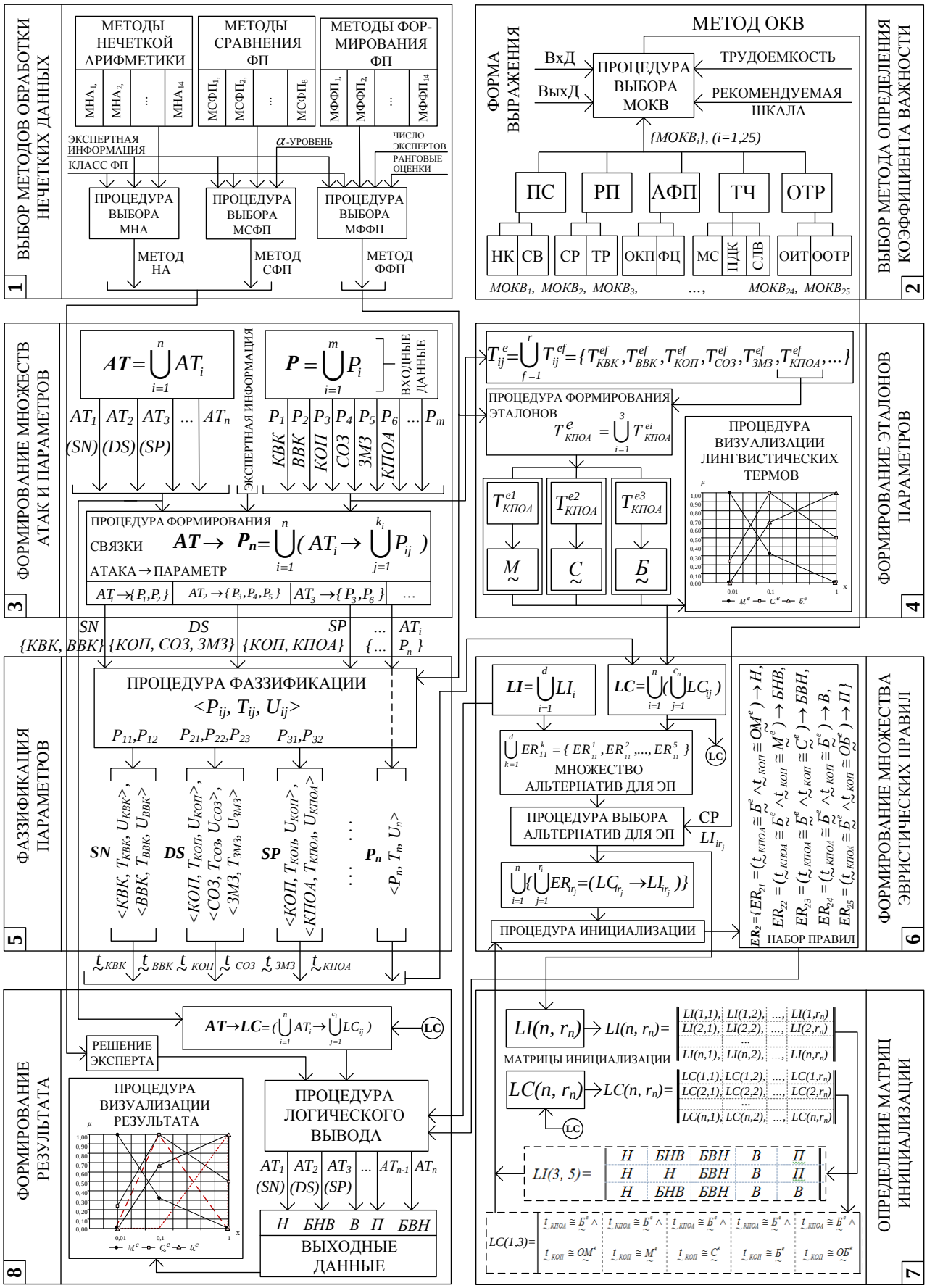

Рис. 1. Схема отображения метода идентификации аномалий

Этап 8 – формирование результата. Этот этап направлен на получение выходных данных, характеризующих аномальное состояние. На основе сформированных множеств возможных атак (см. этап 3) и наборов логико-лингвистических связок (см. этап 6), формируется множество пар – "атака→набор логико-лингвистических связок" $\boldsymbol{AT \rightarrow LC = (} \bigcup_{i=1}^{n} AT_i \rightarrow \bigcup_{j=1}^{c_i} LC_{ij} \boldsymbol{)}$ [5]. Посредством этого множества, сформированных ЭП и множества ***LI*** (см. этап 6), с помощью процедуры логического вывода (функционирующей на основе выбранных по решению эксперта МНА и МСФП) определяются конкретные значения лингвистических идентификаторов, характеризующих уровень аномального состояния, который может быть порожден конкретной кибератакой. Другими словами каждому AT_i присваивается один из LI_i. Так, например, атакам $AT_1=SN$, $AT_2=DS$ и $AT_3=SP$ соответственно будет определен уровень Н, БНВ и В. После определения этих результатов осуществляется их визуализация в виде эталонных лингвистических термов, на фоне которых идентифицируется значение переменной, характеризующей текущее состояние системы относительно аномалий.

Предложенный в работе метод базируется на математических моделях и методах нечеткой логики, и содержит восемь базовых этапов, раскрывающих процесс выявления аномального состояния, порождаемого определенным типом кибератак в ИС. На основе этого метода можно создавать или усовершенствовать реальные системы выявления аномалий, порожденных атакующими действиями в компьютерных сетях.

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. 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, інформаційні послуги», 2007. — [Спец. випуск]. — Т.2. — С. 56–60.
3. Корченко О. Г. Системи захисту інформації [Текст] : Монографія / О. Г. Корченко. — К. : НАУ, 2004. — 264 с.
4. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська, А.О. Корченко // Захист інформації. — 2012. — №1 (54) . — С. 108-121.
5. Стасюк А.И. Базовая модель параметров для построения систем выявления атак / А.И. Стасюк, А.А. Корченко // Захист інформації. — 2012. — №2 (55). — С. 47-51.
6. Модели эталонов лингвистических переменных для систем выявления атак / М.Г. Луцкий, А.А. Корченко, А.В. Гавриленко, А.А Охрименко // Захист інформації. — 2012. — №2 (55). — С. 71-78
7. Корченко А.А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А.А. Корченко // Захист інформації. — 2012. — №4 (57). — С. 109 -115 .

Надійшла: 24.10.2012 р.

Рецензент: д.т.н., професор Дудикевич В.Б.

УДК 003.26:004.056.55

Кінзерявий В.М., Гнатюк С.О., Кінзерявий О.М.

НОВІ ЕФЕКТИВНІ АЛГОРИТМИ ШИФРУВАННЯ ІНФОРМАЦІЇ

Для підвищення ефективності захисту електронних інформаційних ресурсів були розроблені два алгоритми шифрування на основі фіксованої таблиці підстановок з розширеною розрядністю і динамічних ключезалежних таблиць підстановок. Розроблені алгоритми мінімум у два рази швидші за вітчизняний стандарт шифрування ДСТУ ГОСТ 28147-2009 та практично стійкі до лінійного та диференційного криптоаналізу. Властивості псевдовипадкових послідовностей утворених за допомогою запропонованих алгоритмів шифрування (у режимі лічильника) були досліджені у середовищі статистичних тестів NIST STS, згідно яких вони пройшли комплексний контроль за методикою NIST STS і мають кращі результати за інші генератори.

Ключові слова: криптографія, алгоритми шифрування інформації, криптостійкість, лінійний та диференційний криптоаналіз.