УДК 004.056.53(045)

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ВЫЯВЛЕНИЯ АНОМАЛИЙ ПОРОЖДЕННЫХ КИБЕРАТАКАМИ

Анна Корченко, Владимир Щербина, Наталия Вишневская

Развитие информационных технологий трансформируется настолько быстро, что классические механизмы защиты не могут оставаться эффективными, а вредоносное программное обеспечение и другие киберугрозы становятся все более распространенными. Поэтому необходимы системы обнаружения вторжений, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности (особенно ранее неизвестных кибератак), характеризующихся нечетко определенными критериями. Известны кортежная модель формирования набора базовых компонент и ряд методов, применяемых для решения задач выявления вторжений. Их использование позволит усовершенствовать функциональные возможности систем обнаружения вторжений. С этой целью предлагается методология ориентированная на решение задач выявления кибератак, базовый механизм которой основывается на семи этапах: формирование идентификаторов кибератак; построение подмножеств параметров; формирование подмножеств нечетких эталонов; построение подмножеств текущих значений нечетких параметров; α-уровневая номинализация нечетких чисел; определение идентифицирующих термов; формирование подмножеств базовых детекционных правил. Такая методология позволяет строить средства расширяющие функциональные возможности современных систем обнаружения вторжений, используемых для определения уровня аномального состояния, характерного воздействию определенного типа кибератак в слабоформализованной нечеткой среде окружения.

Ключевые слова: *атаки, кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, методология построения систем выявления аномалий.*

Актуальность

На сегодняшний день интенсивное развитие, а также огромные масштабы и темпы внедрения информационных технологий в современный бизнес стали естественным процессом для развитых корпораций. Уровень информатизации компании является одним из главных факторов ее успешного развития, а в условиях большой динамичности рынка и усложнения его инфраструктуры, информация становится стратегическим ресурсом. Развитие информационных технологий трансформируется настолько быстро, что классические механизмы защиты, не могут оставаться эффективными и обеспечивать соответствующую безопасность ресурсам информационных систем, а вредоносное программное обеспечение и другие киберугрозы становятся все более распространенными. В связи с этим необходимы специальные средства, позволяющие оперативно обнаруживать и предотвращать нарушения безопасности. Для этого применяются системы обнаружение вторжений, которые являются неотъемлемой частью любой серьезной системы безопасности, а мировая тенденция идет к тому, что обнаружение вторжений, станет обязательной функцией любой операционной системы и уже применятся в различном программном обеспечении. Расширение функциональных возможностей таких систем за счет выявления ранее неизвестных кибератак, характеризующихся неустановленными или нечетко определенными критериями, позволит им фактически оставаться функциональными в слабоформализованной нечеткой среде окружения. Применение необходимых методов, моделей и методологий информационной безопасности, основанных на нечетких множествах для построения соответствующих средств обнаружения вторжений, является основой для успешного противодействия указанным кибератакам. Исходя из этого, актуальной научной задачей является создание методологии построения систем выявления аномалий, позволяющих в нечетких условиях выявить кибератаки ориентированные на различные ресурсы информационных систем.

Анализ существующих исследований

Достаточно эффективными средствами безопасности, применяемыми для решения задач выявления кибератак, являются, например: нечеткие подходы к обнаружению вторжений [1, 2] и детектированию аномалий [3]; соответствующие нечеткие модели [4-6], методы [7-12] и системы обнаружения вторжений [13-15]; наборы нечетких правил [1-2, 7, 16-18], а также другие разработки, используемые для решения задач защиты в нечетких условиях [19-23]. Эти исследования показали эффективность

применения математического аппарата нечетких множеств, а его использование для формализации подхода к выявлению кибератак позволит усовершенствовать процесс создания соответствующих систем обнаружения вторжений. В работах [9-12, 24-26] предложена кортежная модель формирования набора базовых компонент [24-25], а также следующие методы: формирования лингвистических эталонов [9], фаззификации параметров на лингвистических эталонах [10], α-уровневой номинализации нечетких чисел [11], определения идентифицирующих термов [12] и формирования базовых детекционных правил [26]. Указанные разработки можно положить в основу соответствующей методологии, которая позволит строить системы определяющие уровень аномального состояния, порожденного воздействием соответствующего типа кибератак.

Основная цель исследования

Исходя из анализа существующих исследований и актуальности поставленной задачи целью данной работы является разработка методологии построения систем выявления аномалий порожденных кибератаками (МПСВА) для расширения возможностей систем обнаружения вторжений, функционирующих в слабоформализованной нечеткой среде окружения. С помощью такой методологии (при решении задач выявления кибератак) можно эффективно строить системы, детектирующие уровень аномального состояния, характерного определенному типу кибератак относительно конкретной гетерогенной параметрической среды окружения в заданный временной промежуток.

Основная часть исследования

Для достижения поставленной цели предлагается МПСВА (см. рис. 1), ориентированная на решение задач выявления кибератак в компьютерных системах, базовый механизм которой основывается на семи этапах: формирование идентификаторов кибератак; построение подмножеств параметров; формирование подмножеств нечетких (лингвистических) эталонов; построение подмножеств текущих значений нечетких параметров; α-уровневая номинализация нечетких чисел; определение идентифицирующих термов; формирование подмножеств базовых детекционных правил. Опишем каждый из них.

Этап 1 – формирование идентификаторов кибератак.

Идентификаторы кибератак используются для однозначного определения конкретной атаки (из всего возможного множества) посредством присвоения ее имени конкретному идентификатору. Каждый идентификатор CA_i $(i=\overline{1,n})$ определяется на основе того, что каждый элемент множества $\mathbf{CA}^{\tau_f}$ связан с определенной кибератакой, которую идентифицируют по соответствующему ей имени. Первый этап используется для формирования множеств $\mathbf{CA}^{\tau_f}=\{\bigcup_{i=1}^{n}\mathbf{CA}_i^{\tau_f}\}$ [24] за временной промежуток τ_f, каждое из которых отображается обобщенным кортежем $\mathbf{CA}_i^{\tau_f}=<CA_i, \mathbf{P}_i, \mathbf{T}_i^e, \mathbf{P}_i^{\tau_f}, \mathbf{DR}_i>$ [24].

Этап 2 – построение подмножеств параметров.

Подмножества параметров $\mathbf{P}_i$ [24] необходимы для построения нечетких (лингвистических) эталонов. Здесь для построения подмножества $\mathbf{P}_i$ на основе множества всех возможных параметров $\mathbf{P}$ [24], характеризующих состояние среды окружения, по значениям которых можно выявить аномальное состояние, порождаемое воздействием кибератаки с идентификатором CA_i (см. этап 1). Таким образом, формируется $\{\bigcup_{i=1}^{n}\mathbf{P}_i\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}P_{ij}\}\}$ $(j=\overline{1,m_i})$, где конкретные значения членов подмножества $\mathbf{P}_i$ определяют m_i-мерную параметрическую подсреду, используемую для выявления CA_i-атаки.

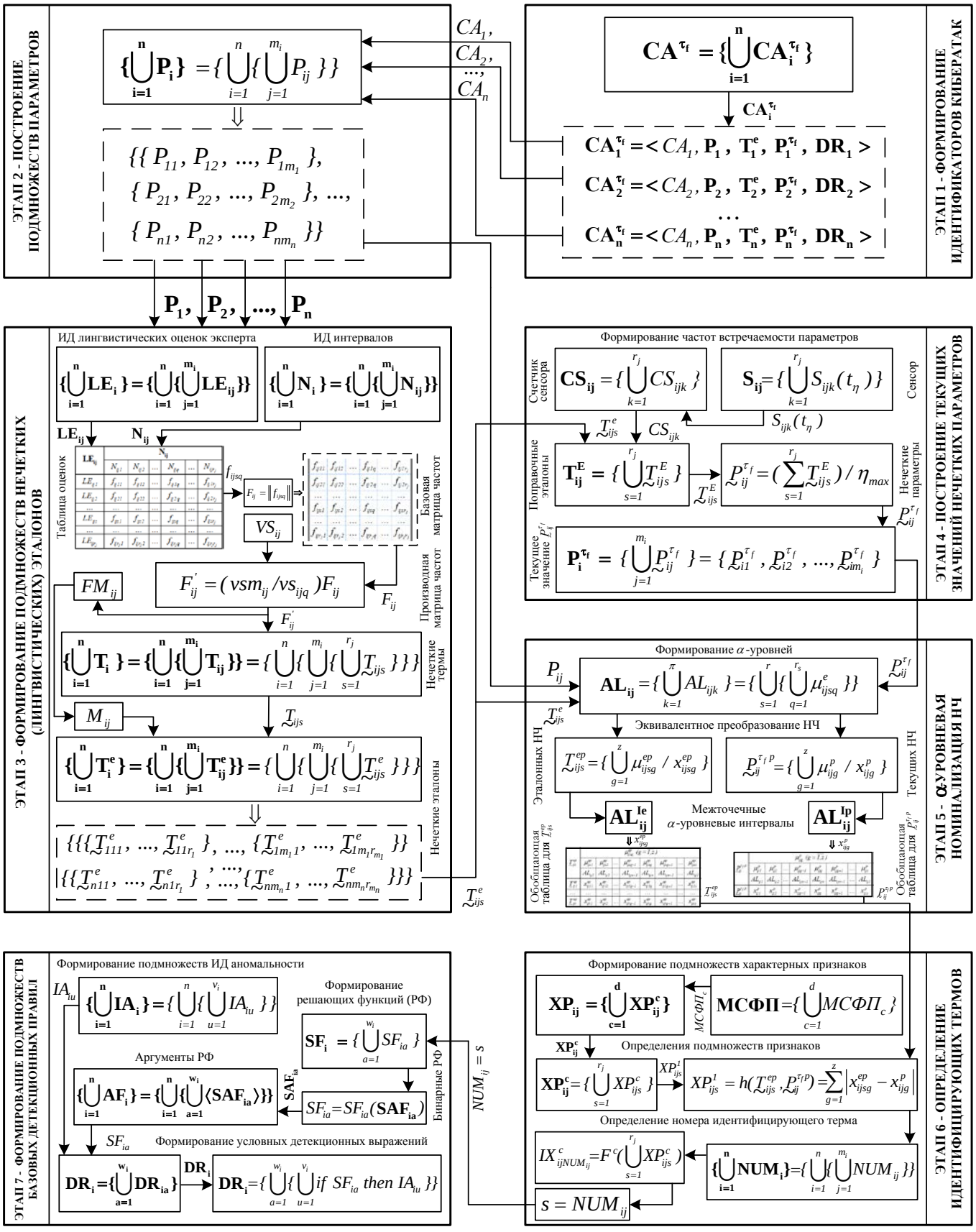

Рис. 1. Схема отображения методологии построения систем выявления аномалий порожденных кибератаками

Этап 3 – формирование подмножеств нечетких (лингвистических) эталонов.

Подмножества нечетких (лингвистических) эталонов $\mathbf{T_i^e}$ [24] необходимы для отображения определенных (фиксированных) состояний соответствующих параметров из подмножества $\mathbf{P_i}$ в определенной среде окружения. На этом этапе осуществляется формирование подмножеств возможных нечетких (лингвистических) эталонов $\mathbf{T_i^e}$, отображающих характерные суждения эксперта относительно аномальности состояния соответствующих параметров P_{ij} из подмножества $\mathbf{P_i}$ (см. этап 2) в заданной среде окружения. Для этого, формируем подмножества идентификаторов лингвистических оценок (суждений) эксперта $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{LE_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{LE_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}LE_{ijk}\}\}\}$ $(k=\overline{1,r_j})$ (см. выражение 7 в [9]) и подмножества идентификаторов интервалов $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{N_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{N_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{k=1}^{r_j}N_{ijk}\}\}\}$ (см. выражение 12 в [9]), которые соответственно необходимы для построения базовой матрицы частот F_{ij} (см. выражение 13 в [9]). Далее с использованием $\mathbf{LE_{ij}}$, $\mathbf{N_{ij}}$ и F_{ij}, посредством вектора сумм VS_{ij} (см. выражение 15 в [9]) строится производная матрица частот $F_{ij}^{'}=(vsm_{ij}/vs_{ijq})F_{ij}$ (см. выражение 17 в [9]). С учетом матрицы $F_{ij}^{'}$ формируются подмножества нечетких термов $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}\}\}\}$ $(s=\overline{1,r_j})$ (см. выражение 22 в [9]), а также с использованием вектора максимумов FM_{ij} (см. выражение 23 в [9]) и матрицы функций принадлежности M_{ij} (см. выражение 24 в [9]) определяются наборы нечетких термов (чисел) $\underset{\sim}{T}_{ijs}$ (см. выражение 25 в [9]). Согласно $\underset{\sim}{T}_{ijs}$ и наборов промежуточных термов $\underset{\sim}{T}_{ijs}^{'}$ (см. выражение 28 в [9]), получим подмножества возможных нечетких (лингвистических) эталонов $\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{T_i^e}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}^e}\}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^{e}\}\}\}$ (см. выражение 14 в [24]), где совокупность конкретных значений всех членов подмножества $\mathbf{T_i^e}$ определяют эталонную среду, ориентированную на выявления кибератаки с идентификатором CA_i (см. этап 1).

Этап 4 – построение подмножеств текущих значений нечетких параметров.

Подмножества текущих значений нечетких параметров $\mathbf{P_i^{\tau_f}}$ [24] необходимы для формирования текущих значений переменных в нечеткой форме, посредством которых формализуются параметры характерные для конкретной среды окружения при решении задач выявления кибератак. Этап ориентирован на построение подмножеств всех возможных текущих значений нечетких параметров, формируемых посредством $\mathbf{T_i^e}$ (см. этап 3) в заданный момент времени τ_f за определенный промежуток, длительность которого $\tau_h=\tau_f-\tau_{f-1}$, $(f=\overline{1,max_\tau})$. Для этого, с учетом подмножества всех возможных сенсоров $\mathbf{S_{ij}}=\{\bigcup_{k=1}^{r_j}S_{ijk}(t_\eta)\}$ (см. выражение 1 в [10]), используемых для контроля текущего состояния физических параметров, отображаемых посредством $\mathbf{P_i^{\tau_f}}$ в $\mathbf{CA_i^{\tau_f}}$ [24] и подмножества всех возможных счетчиков сенсоров $\mathbf{CS_{ij}}=\{\bigcup_{k=1}^{r_j}CS_{ijk}\}=\{\bigcup_{k=1}^{r_j}\sum_{\eta=1}^{\eta_{max}}S_{ijk}(t_\eta)\}$ (см. выражение 3 в [10]) формируются частоты встречаемости физических параметров (см. этап 1 в [10]). Далее с использованием поправочных эталонов $\mathbf{T_{ij}^E}=\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^{E}\}$ (см. выражение 4 в [10]) и нечетких параметров $\underset{\sim}{P}_{ij}^{\tau_f}=(\sum_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^{E})/\eta_{max}$ (см. выражение 6 в [10]) формируются подмножества текущих значений $\mathbf{P_i^{\tau_f}}=\{\bigcup_{j=1}^{m_i}\underset{\sim}{P}_{ij}^{\tau_f}\}$ [24], а совокупность конкретных значений всех членов подмножества $\mathbf{P_i^{\tau_f}}$

определяет текущую среду, используемую для выявления аномального состояния в общей гетерогенной параметрической среде, порожденной кибератакой с идентификатором CA_i (см. этап 1) в момент времени τ_f.

Этап 5 – α-уровневая номинализация нечетких чисел.

Номинализация нечетких чисел необходима для приведения к одному числу компонент эталонных и текущих нечетких чисел, вычисленных на основе объединенных значениях их α-уровней. Преобразование сформированных подмножеств возможных нечетких (лингвистических) эталонов $\mathbf{T_i^e}$ (см. этап 3) и текущих значений нечетких параметров $\mathbf{P_i^{\tau_f}}$ (см. этап 4) требует четкой формализации процесса формирования α-уровневых интервалов для соответствующего эквивалентного преобразования эталонных и текущих НЧ. Это даст возможность определять идентифицирующие термы, отображающие аномальность текущего состояния среды окружения при решении задач выявления атак в информационных системах. Для этого, с помощью подмножеств всех возможных значений $\mathbf{AL_{ij}} = \{\bigcup_{k=1}^{\pi} AL_{ijk}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{q=1}^{r_s}\mu_{ijsq}^{e}\}\}$ (см. выражения 3 в [11]), используемых для преобразования НЧ отображающих P_{ij} с базовым терм-множеством $\mathbf{T_i}$, формируются α-уровни (см. этап 1 в [11]). Далее с использованием множества всех возможных преобразованных (номинализированных) эталонных НЧ $\mathbf{T_{ij}^{ep}} = \{\bigcup_{s=1}^{r}\underset{\sim}{T}_{ijs}^{ep}\}$ (см. выражение 4 в [11]) и полученного на их основе преобразованного текущего НЧ $\underset{\sim}{P}_{ij}^{\tau_f p}$, (т.е.: $\underset{\sim}{T}_{ijs}^{ep} = \{\bigcup_{g=1}^{z}\mu_{ijsg}^{ep} / x_{ijsg}^{ep}\}$ и $\underset{\sim}{P}_{ij}^{\tau_f p} = \{\bigcup_{g=1}^{z}\mu_{ijg}^{p} / x_{ijg}^{p}\}$) (см. выражение 5 и 6 в [11]), а также подмножества α-уровневых интервалов $\mathbf{AL_{ij}^{Ie}} = \{\bigcup_{s=1}^{r} AL_{ijs}^{Ie}\} = \{\bigcup_{s=1}^{r}\{\bigcup_{b=1}^{r_s-1}\{\bigcup_{c=1}^{k_b} AL_{ijsbc}^{Ie}\}\}\}$ (см. выражение 11 в [11]), осуществляется номинализация эталонных НЧ $\underset{\sim}{T}_{ijs}^{ep}$. Далее, за счет подмножества межточечных α-уровневых интервалов $\mathbf{AL_{ij}^{Ip}} = \{\bigcup_{b=1}^{\rho-1}\{\bigcup_{c=1}^{k_b} AL_{ijbc}^{Ip}\}\}$ (см. выражение 13 в [11]), по аналогии с номинализацией эталонных НЧ $\underset{\sim}{T}_{ijs}^{ep}$, формируются преобразованные (номинализированные) текущие НЧ $\underset{\sim}{P}_{ij}^{\tau_f p}$. Исходя из этого находятся значения x_{ijsg}^{ep} и x_{ijg}^{p} для $\underset{\sim}{T}_{ijs}^{ep}$ и $\underset{\sim}{P}_{ij}^{\tau_f p}$. Таким образом осуществляется эквивалентное преобразование НЧ (см. этап 2 в [11]), которое реализуется за счет приведения всех эталонных и текущих НЧ к номинальному (одному для всех) числу компонент. Далее с учетом всех преобразованных эталонных $\underset{\sim}{T}_{ijs}^{ep}$ и текущих $\underset{\sim}{P}_{ij}^{\tau_f p}$ НЧ строятся обобщающие таблицы, а также выполняется графическая интерпретация соответствующих НЧ (см. этап 3 в [11]).

Этап 6 – определение идентифицирующих термов.

Этап ориентирован на поиск в заданной лингвистической переменной идентифицирующего эталонного терма, по которому с помощью детекционных правил можно определить уровень аномального состояния, характерного для определенного типа атак. Для этого, на базе $\mathbf{МСФП} = \{\bigcup_{c=1}^{d} МСФП_c\}$ (см. выражение 2 в [12]) формируются подмножества всех возможных характерных признаков (ХП) $\mathbf{XP_{ij}} = \{\bigcup_{c=1}^{d}\mathbf{XP_{ij}^{c}}\}$ (см. выражение 1 в [12]). Далее на основании сформированных ХП $\mathbf{XP_{ij}^{c}} = \{\bigcup_{s=1}^{r_j} XP_{ijs}^{c}\}$ (см. выражение 3 в [12]) и по значению c определяется номер метода из множества $\mathbf{МСФП}$, который используется для определения конкретного ХП. Например, при $c = 1$ ХП формируется на основании расстояния Хэмминга $XP_{ijs}^{1} = h(\underset{\sim}{T}_{ijs}^{ep}, \underset{\sim}{P}_{ij}^{\tau_f p}) = \sum_{g=1}^{z}\left|x_{ijsg}^{ep} - x_{ijg}^{p}\right|$ (см. выражение 4 в [12]). Таким образом, можно определить все возможные для использования подмножества признаков (см. этап 2 в [12]). Далее

посредством подмножества всех номеров идентифицирующих термов $\{\bigcup_{i=1}^{n}\mathbf{NUM_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i} NUM_{ij}\}\}$ (см. выражение 8 в [12]), а также с учетом функции поиска идентифицирующего ХП и его номера $IX^{c}_{ijNUM_{ij}} = F^{c}(\bigcup_{s=1}^{r_j} XP^{c}_{ijs})$ (см. выражение 6 в [12]) осуществляется нахождение в подмножестве $\mathbf{T^e_{ij}}$ такого терма, у которого значение $s = NUM_{ij}$, которое и принимается в качестве идентифицирующего. Другими словами, определяется номер идентифицирующего терма (см. этап 3 в [12]).

Этап 7 – формирование подмножеств базовых детекционных правил.

Подмножества базовых детекционных правил $\mathbf{DR_i}$ [24, 26], необходимы для обнаружения i-й кибератаки на основе параметрических подсред различной размерности [24-25]. Для этого, формируются подмножества всех возможных идентификаторов аномальности $\{\bigcup_{i=1}^{n}\mathbf{IA_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{u=1}^{v_i} IA_{iu}\}\}$ (см. выражение 5 в [26]) посредством которых (в лингвистический форме) можно отобразить возможные уровни аномального состояния в среде окружения, порождаемые кибератакой с идентификатором CA_i (см. этап 1) для подмножества правил $\mathbf{DR_i}$. Далее на основании подмножества всех построенных бинарных решающих функций $\mathbf{SF_i} = \{\bigcup_{a=1}^{w_i} SF_{ia}\}$ ($SF_{ia} = SF_{ia}(\mathbf{SAF_{ia}})$) (см. выражение 15 и 16 в [26]), формируются подмножества всех аргументов решающих функций $\{\bigcup_{i=1}^{n}\mathbf{AF_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{a=1}^{w_i}\langle\mathbf{SAF_{ia}}\rangle\}\}$ (см. выражение 13 в [26]). Далее, каждое базовое правило может породить v_i детекционных выражений $\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i}\{\bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\}\}$ (см. выражение 22 в [26]), а также с учетом SF_{ia} и IA_{iu}, формируются подмножества условных детекционных выражений $\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i}\mathbf{DR_{ia}}\}$ (см. выражение 21 в [26], которые отображают формируемые базовые правила для выявления i-й кибератаки или CA_i-атаки.

Таким образом, в работе предложена МПСВА, которая за счет механизмов формирования идентификаторов кибератак, построения подмножеств параметров, формирования подмножеств нечетких (лингвистических) эталонов, построения подмножеств текущих значений нечетких параметров, α-уровневой номинализации нечетких чисел, определения идентифицирующих термов и формирования подмножеств базовых детекционных правил позволяет строить средства, расширяющие функциональные возможности современных систем обнаружения вторжений, используемых для определения уровня аномального состояния, характерного воздействию определенного типа кибератак в слабоформализованной нечеткой среде окружения.

ЛИТЕРАТУРА

[1]. 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.

[2]. 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.

[3]. 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).

[4]. 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. 112-118.

[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]. 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]. Стасюк А.И. Метод выявления аномалий порожденных кибератаками в компьютерных сетях / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – №4 (57). – С. 129-134.

[9]. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.

[10]. Корченко А.А. Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак / А.А. Корченко // Безпека інформації. – 2014. – № 1 (20). – С. 21-28.

[11]. Корченко А.А. Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений / А.А. Корченко // Захист інформації. – Т.16, №4. – 2014. – С. 292-304.

[12]. Корченко А.А. Метод определения идентифицирующих термов для систем обнаружения вторжений / А.А. Корченко // Безпека інформації. – Т.20, № 3. – 2014. – С. 217-223.

[13]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.

[14]. Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – 2013. – Т.15, №3. – С. 240-246.

[15]. Корченко А.А. Система формирования эвристических правил для оценивания сетевой активности / А.А. Корченко // Захист інформації. – 2013. – №4. Т.15. – С. 353-359.

[16]. 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.

[17]. 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.

[18]. 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.

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

[20]. Казмирчук С.В. Анализ и оценивание рисков информационных ресурсов / С.В. Казмирчук // Захист інформації. – 2013. – Том 15 №1 (58). – С. 37-46.

[21]. Казмирчук С.В. Интегрированный метод анализа и оценивания рисков информационной безопасности / С.В. Казмирчук, А.Ю. Гололобов // Захист інформації. – 2014. – Т.16. – №3. – С. 252-263.

[22]. Корченко А.Г. Метод n-кратного инкрементирования числа термовлингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, Б.С. Ахметов, С.В. Казмирчук, М.Н. Жекамбаева // Безпека інформації. – 2015. – Т.21. –№2. – С. 191-200.

[23]. Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, А.Ю. Гололобов // Захист інформації. – 2014. – Т.16. – №4. – С. 284-291.

[24]. Корченко А.А. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.

[25]. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.

[26]. Карпинский Н. Метод формирования базовых детекционных правил для систем обнаружения вторжений / Н. Карпинский, А. Корченко, С. Ахметова // Захист інформації. – 2015. – №4. Т.17. – С. 312-324.

REFERENCES

[1]. 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.

[2]. 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.

[3]. 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).

[4]. Korchenko A.A. The model of heuristic rules on the set of logical-linguistic tangles for abnormality detection in computer systems, Zahist ìnformacìï, 2012, №4 (57), pp. 112-118.

[5]. Stasiuk A.I., Korchenko A.A. The basic model of parameters in attack detection (Identification) systems construction, Zahist ìnformacìï, 2012, №2 (55), pp. 47-51.

[6]. Lutskiy M.G., Korchenko A.A., Gavrylenko A.V., Okhrimenko A.A. The models of linguistic variables for attack detection systems, Zahist ìnformacìï, 2012, №2 (55), pp. 71-78.

[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]. Stasiuk A.I., Korchenko A.A. A method of abnormality detection caused by cyber attacks in computer networks, Zahist ìnformacìï, 2012, №4 (57), pp. 129-134.

[9]. Korchenko A.A. The formation method of linguistic standards created for the intrusion detection systems, Zahist ìnformacìï, T.16, №1, 2014, pp. 5-12.

[10]. Korchenko A.A. The method of parameter fuzzification based on linguistic standards for cyber attacks detection, Bezpeka ìnformacìï, T.20, №1, 2014, pp. 21-28.

[11]. Korchenko A.A. The method of α-level of nominalization for intrusion detection systems, Zahist ìnformacìï, T.16, №4, 2014, pp. 292-304.

[12]. Korchenko A.A. The detection method of identification terms for intrusion detection system, Bezpeka ìnformacìï, T.20, №3, 2014, pp. 217-223.

[13]. Korchenko A.A. Anomaly-based detection system in computer networks, Bezpeka ìnformacìï, 2012, №2 (18), pp. 80-84.

[14]. Korchenko A.A. The system development of fuzzy standards of network parameters, Zahist ìnformacìï, T.15, №3, 2013, pp. 240-246.

[15]. Korchenko A.A. The system of heuristic rules formation for network activity assessment, Zahist ìnformacìï, T.15, №4, 2013, pp. 353-359.

[16]. 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.

[17]. 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.

[18]. 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.

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

[20]. Kazmirchuk S.V. Risk analysis and assessment of information resources, Zahist ìnformacìï,2013, VOL. 15 №1, pp. 37-46.

[21]. Kazmirchuk S.V., Gololobov A.Yu. The integrated risk analysis and risk assessment method of information security, Zahist ìnformacìï, 2014, VOL. 16 №3, pp. 252-263.

[22]. Korchenko A.G., Akhmetov B.S., Kazmirchuk S.V., Zhekambaeva M.N. Method of n-fold incrementation the number of terms the linguistic variables in the tasks of analysis and risk assessment, Bezpeka Informácie, 2015, VOL. 21 №2, pp. 191-200.

[23]. Korchenko A.G., Akhmetov B.S., Kazmirchuk S.V., Gololobov A.Yu., Seilova N.A. "The n-fold decrease method of terms number of linguistic variables in risk assessment and task analysis", Zahist ìnformacìï, 2014, VOL. 15 № 4, pp. 284-291.

[24]. Korchenko A.A. The tupel model of basic components' set formation for cyberattacks, Legal, regulatory and metrological support information security system in Ukraine, 2014, V.2 (28), pp. 29-36.

[25]. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.

[26]. Karpinski M., Korchenko A., Akhmetova S. The method of developmentof basic detection rules for intrusion detection systems, Zahist ìnformacìï, T.17, №4, 2015, pp. 312-324.

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ АНОМАЛІЙ ПОРОДЖЕНИХ КІБЕРАТАКАМИ

Розвиток інформаційних технологій трансформується настільки швидко, що класичні механізми захисту не можуть залишатися ефективними, а шкідливе програмне забезпечення та інші кіберзагрози стають все більш поширеними. Тому необхідні системи виявлення вторгнень, що дозволяють оперативно виявляти і запобігати порушенням безпеки (особливо раніше невідомих кібератак), які характеризуються нечітко визначеними критеріями. Відомі кортежна модель формування набору базових компонент і низка методів, що застосовуються для вирішення завдань виявлення вторгнень. Їх використання дозволить удосконалити функціональні можливості систем виявлення вторгнень. З цією метою пропонується методологія, орієнтована на вирішення завдань виявлення кібератак, базовий механізм якої ґрунтується на семи етапах: формування ідентифікаторів кібератак; побудова підмножин параметрів; формування підмножин нечітких еталонів; побудова підмножин поточних значень нечітких параметрів; α-рівнева номіналізація нечітких чисел; визначення ідентифікуючих термів; формування підмножин базових детекційних правил. Така методологія дозволяє будувати засоби, які розширюють функціональні можливості сучасних систем виявлення вторгнень, що використовуються для визначення рівня аномального стану, характерного впливу певного типу кібератак в слабоформалізованому нечіткому середовищі оточення.

Ключові слова: атаки, кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, методологія побудови систем виявлення аномалій.

A METHODOLOGY FOR BUILDING CYBERATTACK-GENERATED ANOMALY DETECTION SYSTEMS

The IT development is transforming so fast that the classical defense mechanisms cannot remain effective, malicious software and other cyber threats getting more and more widespread. For this reason, there appears a necessity in intrusion detection systems that could allow prompt detection and prevention of security incidents (especially cyber attacks unknown before) characterized by fuzzy criteria. There is a tuple model for basic component set formation and a number of methods used for intrusion detection, the use of which would expand the functionality of intrusion detection systems. For this purpose, we suggest a cyber attack detection methodology whose basic mechanism relies on the following seven stages: formation of cyber attack identifiers; building of parameter subsets; formation of fuzzy standard subsets; building of subsets of fuzzy parameters current values; α-level nominalization of fuzzy numbers; determination of identifying terms; formation of basic detection rule subsets. This methodology allows creating tools that would expand the functionalities of modern intrusion detection systems used to determine the level of the abnormal condition characteristic of a certain cyber attack type in a poorly formalized fuzzy environment.

Keywords: attacks, cyber attacks, anomalies, intrusion detection systems, anomaly detection systems, intrusion detection systems, methodology for building anomaly detection systems.

Корченко Анна Александровна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: annakor@ukr.net

Корченко Анна Олександрівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Anna, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Щербина Владимир Порфирьевич, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: smya@nau.edu.ua

Щербина Володимир Порфирійович, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Shcherbyna Volodymyr, Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Вишневская Наталия Сергеевна, старший преподаватель кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: viserj@ukr.net

Вишневська Наталія Сергіївна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.

Vyshnevska Natalia, senior lector of IT-Security Academic Department, National Aviation University (Kyiv, Ukraine)