СИСТЕМА ВЫЯВЛЕНИЯ АНОМАЛЬНОГО СОСТОЯНИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

Анна Корченко

Национальный авиационный университет

КОРЧЕНКО Анна Александровна, к.т.н. НАУ
Год и место рождения: 1985 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 2007 год.
Должность: ассистент кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, компьютерная безопасность, экспертные системы.
Публикации: больше 20 научных публикаций, среди которых научные статьи, учебники и учебно- методическое пособие.
E-mail: annakor@ukr.net

***Аннотация**. Эффективное обнаружение новых типов кибератак, например, "нулевого дня", а также атак, которые не имеют сигнатур, связано с широким применением соответствующих средств защиты. Существующие системы обнаружения вторжений используют для решения задач безопасности математические модели, которые требуют много ресурсов и затрат различного характера, например, связанными с выборкой статистических данных, обучении систем, ее адаптацией и др. Более эффективные в этом отношении являются экспертные подходы, основанные на использовании знаний и опыта специалистов соответствующей предметной области. Для решения этой задачи на основании метода идентификации аномалий построенного на нечеткой логике предложено структурное решение системы выявления аномального состояния в компьютерных сетях, порожденного несигнатурными атаками. Система состоит из подсистем первичной обработки, формирования нечетких эталонов и эвристических правил, а также модулей нечеткой арифметики, лингвистического вывода и визуализации, которые позволяют идентифицировать уровень аномального состояния в сетевом трафике, порожденного определенным типом кибератак. Результат работы системы представляется в лингвистической и графических формах.*

***Ключевые слова:** атаки, кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, атаки в компьютерных системах, обнаружение аномалий в компьютерных сетях.*

Актуальность

Проблема защиты компьютерных систем и сетей становится более острой с развитием и распространением информационных технологий во все сферы деятельности человека, общества и государства. Несмотря на существующее разнообразие современных средств сетевой безопасности, информационные системы все больше подвергаются воздействиям угроз, новые виды которых порождают новые кибератаки на их ресурсы. В частности, системы обнаружения вторжений (СОВ), в этом аспекте, ориентированы на решение задач сетевой защиты. Эти СОВ чаще всего основываются на математических моделях, которые требуют от внедренных систем много времени на ввод их в эксплуатацию.

Такой подготовительный этап чаще всего связан, например, с выборкой статистических данных, обучением системы и др. Более эффективные в этом отношении являются экспертные методы, основанные на использовании знаний и опыта специалистов соответствующей предметной области [1].

В связи с этим, актуальной задачей является разработка соответствующих технических решений, основанных на экспертном подходе.

Анализ существующих исследований

Известна базовая модель параметров [2], для нечетко определенной слабоформализованной среды и универсальная модель эталонов лингвистических переменных [3], которые за счет сформированных множеств пар "атака → параметры" и "атака → набор логико-лингвистических связок" позволяют формализовать процесс построения эталонных значений ориентированных на измерение текущих параметров среды окружения в нечетких слабоформализованных условиях. А исходя из результатов измерений текущих величин и их привязки к типу атаки можно идентифицировать соответствующее вторжение.

Также известна модель эвристических правил [4], которая за счет множества эталонных параметров и матриц инициализации, позволяет формализовать процесс формирования множеств решающих правил для выявления аномального

состояния, поро-жденного определенным типом атак в компью-терных сетях.

С учетом этих моделей в [5] предложен метод выявления аномалий порожденных действиями неавторизованной стороны, позволяющий строить средства обнаружения несигнатурных кибератак и атак "нулевого дня" (0-day), которые чаще всего являются скрытыми.

Основная цель исследования

В связи с этим, целью данной работы является разработка нового структурного решения для совершенствования систем сетевой безопасности, посредством реализации предложенного метода обнаружения аномалий [4], ориентированного на контроль активности в среде окружения. Такое решение позволит расширить функциональные возможности современных СОВ за счет эффективной идентификации новых (0-day) и несигнатурных типов кибератак.

Основная часть исследований

Для реализации известного метода [5] разработаем структурное решение соответствующей системы (рис. 1), содержащей: подсистему первичной обработки (ППО), предназначенную для формирования множеств атак, параметров и их фаззификации (см. этап 3 и 5 в [5]); подсистему формирования нечетких эталонов (ПФНЭ), ориентированную на получение всех необходимых термов для каждой лингвистической переменной (см. этап 4 в [5]) с целью измерения текущих значений сетевых параметров; подсистему формирования эвристических правил (ПФЭП), применяемую при создании множества правил для контроля сетевой активности (см. этап 6 и 7 в [5]); модули нечеткой арифметики (МНА), логического вывода (МЛВ) и визуализации (МВ), предназначенные для формирования результата в лингвистическом и графическом представлении (см. этап 8 в [5]); управляющий модуль, служащий для управления коммутацией (УК), а также переводом системы в режим корректировки эталонов (РКЭ) и корректировки правил (РКП).

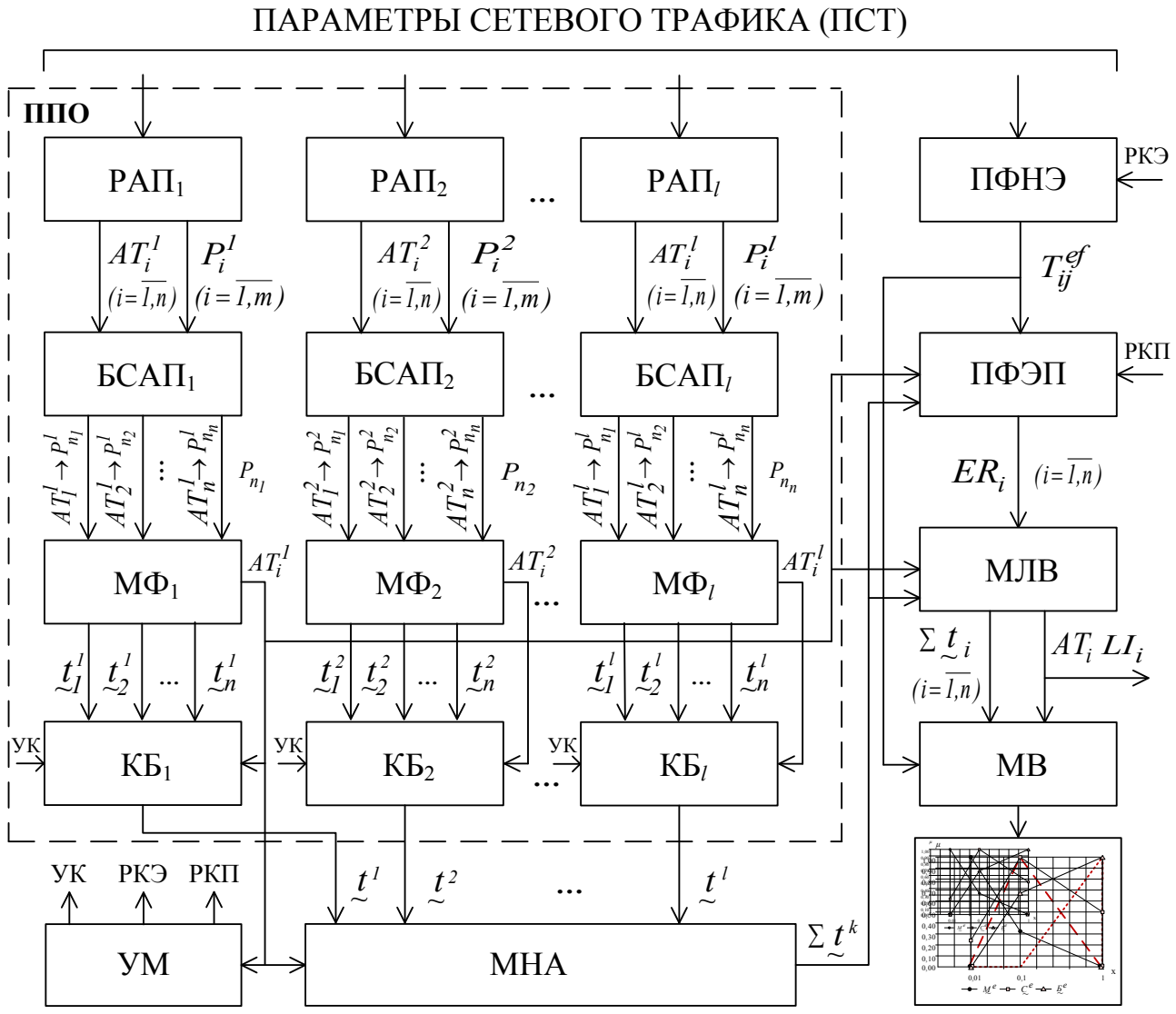

Рис. 1. Структура системы выявления аномального состояния в компьютерных сетях

Система выявления аномального состояния (СВАС) в компьютерных сетях функционирует следующим образом. Перед началом вычислительного процесса, в ПФНЭ на основе параметров сетевого трафика (ПСТ) согласно соответствующей базовой модели [2] формируется множеств атак AT_i, $(i=\overline{1,n})$ и параметров P_i, $(i=\overline{1,m})$, посредством которых, с использованием выбранного (согласно установленным критериям) метода формирования функций принадлежности (МФФП) (см. этап 1 в [5]), генерируются эталоны (см. этап 4 в [5]) для определенных лингвистических переменных (ЛП) по каждому терму T_{ij}^{ef}.

Согласно полученных эталонов параметров в ПФЭП создаются шаблоны наборов эвристических правил ER_i $(i=\overline{1,n})$, (см. этап 6 и 7 в [5]), используемых для контроля сетевой активности относительно возможных проявлений атакующих действий в компьютерной сети. Эти шаблоны и эталоны параметров не изменяются на протяжении всего процесса функционирования СВАС, но при необходимости могут модифицироваться посредством их перевода в РКЭ или РКП.

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

Например при $n=3$ и $m=6$ для k-го узла сети осуществляется формирование AT_i, и P_i (см. этап 3 в [5]) позволяющих идентифицировать аномальное состояние, порожденное тремя видами атак AT_1^k, AT_2^k и AT_3^k $(SN^k, DS^k$ и $SP^k)$ на основе шести параметров P_1^k, P_2^k, P_3^k, P_4^k, P_5^k и P_6^k $(КВК^k, ВВК^k, КОП^k, СОЗ^k, ЗМЗ^k$ и $КПОА^k)$. Следует отметить, что если узлы компьютерной сети разнородны по своим характеристикам, то для определенных типов аномалий порожденных соответствующими атакующими действиями, значения эталонов будут отличаться.

Для формирования связки конкретной атаки с необходимыми для ее выявления параметрами (см. этап 3 в [5]), в ППО используется l блоков связи атаки с параметрами БСАП$_k$ $(k=\overline{1,l})$, представляющие собой специальным образом организованное запоминающее устройство. Например, при тех же $n=3$ и $m=6$ для k-го узла с идентификаторами атак (AT_1^k),(AT_2^k) и (AT_3^k) соответственно образуются связи с параметрами $P_{n_1}^k=(P_1^k, P_2^k)$, $P_{n_2}^k=(P_3^k, P_4^k, P_5^k)$ и $P_{n_3}^k=(P_3^k, P_6^k)$, т.е. $SN^k \to \{КВК^k, ВВК^k\}$, $DS^k \to \{КОП^k, СОЗ^k, ЗМЗ^k\}$ и $SP^k \to \{КОП^k, КПОА^k\}$, $(k=\overline{1,l})$. В этом примере, относительно организации БСАП, можно отметить, что идентификаторы SN^k, DS^k и SP^k будут адресами специально организованного запоминающего устройства, а $\{КВК^k, ВВК^k\}$, $\{КОП^k, СОЗ^k, ЗМЗ^k\}$ и $\{КОП^k, КПОА^k\}$ соответственно содержимым по этим адресам.

По завершению в БСАП$_k$ $(k=\overline{1,l})$ процедуры формирования связок $AT_i^k \to P_{n_i}^k$ с помощью модулей фаззификации МФ$_k$ $(k=\overline{1,l})$ осуществляется преобразование (с использованием МФФП, см. этап 1 в [5]) множества текущих значений параметров (наблюдаемых за определенный промежуток времени) посредством одного нечеткого числа (НЧ) $(i=\overline{1,n})$, (см. этап 5 в [5]) и таким образом на выходе МФ$_k$ получаем n НЧ $\underset{\sim}{t}_i^k$ $(i=\overline{1,n})$ связанных с соответствующими AT_i.

Например, при $n=6$ значение $\underset{\sim}{t}_1^k = \underset{\sim}{t}_{КВК}^k$, $\underset{\sim}{t}_2^k = \underset{\sim}{t}_{ВВК}^k$, $\underset{\sim}{t}_3^k = \underset{\sim}{t}_{КОП}^k$, $\underset{\sim}{t}_4^k = \underset{\sim}{t}_{СОЗ}^k$, $\underset{\sim}{t}_5^k = \underset{\sim}{t}_{ЗМЗ}^k$ и $\underset{\sim}{t}_6^k = \underset{\sim}{t}_{КПОА}^k$.

Далее, поочередно полученные $\underset{\sim}{t}_i^k$ $(i=\overline{1,n}, k=\overline{1,l})$ посредством k-х коммутирующих блоков КБ$_k$ $(k=\overline{1,l})$ по сигналу управления коммутацией (УК) соответственно типу атаки AT_i^k $(i=\overline{1,n}, k=\overline{1,l})$ с ППО в модуль нечеткой арифметики (МНА) поступают текущие параметры $\underset{\sim}{t}^k$ $(k=\overline{1,l})$ со всех КБ$_k$ $(k=\overline{1,l})$ для получения суммарных показателей $\sum \underset{\sim}{t}^k$, характеризующих активность во всех узлах компьютерной сети. Наиболее подходящий метод, который может использоваться для реализации операций нечеткой арифметики (из четырнадцати фиксированных) выбирается согласно заданным критериям и реализуется в МНА (см. этап 1 в [5]).

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

На основе полученных в МНА суммарных показателей $\underset{\sim}{t}^k$, а также с использованием инициированного в ПФЭП множества правил ER_i ($i = \overline{1,n}$) соответствующих определенным AT_i в МЛВ, согласно известного метода (см. этап 8 в [5]) посредством LI_i ($i = \overline{1,d}$), осуществляется определение текущего уровня аномального состояния в ПСТ, которое может быть порождено определенным типом кибератак. Этот уровень может представляться в лингвистической форме, а также посредством МВ быть идентифицирован в графической форме в виде соответствующего НЧ, отображенного на фоне сформированных в ПФЭП эталонных значений лингвистических переменных.

Выводы

В работе предложено новое структурное решение, на основе которого можно разрабатывать алгоритмическое, программное и программно-аппаратное обеспечение, применяемое для обнаружения аномального состояния, порожденного действиями несигнатурных кибератак. Такое обеспечение может использоваться автономно или в качестве расширителя функциональных возможностей современных систем обнаружения вторжений в компьютерных сетях.

Литература

[1] 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] 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.

[3] 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.

[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. 109-115.

[5] 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.

УДК 004.056.53(045)

Корченко А.О. Система виявлення аномального стану в комп'ютерних мережах

Анотація. *Ефективне виявлення нових типів кібератак, наприклад, "нульового дня", а також атак, які не мають сигнатур, пов'язане з широким застосуванням відповідних засобів захисту. Існуючі системи виявлення вторгнень використовують для вирішення завдань безпеки математичні моделі, які вимагають багато ресурсів і витрат різного характеру, наприклад, пов'язаними з вибіркою статистичних даних, навчанні систем, її адаптацією та ін. Більш ефективні в цьому відношенні є експертні підходи, засновані на використанні знань і досвіду фахівців відповідної предметної області. Для вирішення цього завдання на підставі методу ідентифікації аномалій побудованого на нечіткій логіці запропоновано структурне рішення системи виявлення аномального стану в комп'ютерних мережах, породженого несигнатурними атаками. Система складається з підсистем первинної обробки, формування нечітких еталонів і евристичних правил, а також модулів нечіткої арифметики, лінгвістичного виводу і візуалізації, які дозволяють ідентифікувати рівень аномального стану в мережевому трафіку, породженого певним типом кібератак. Результат роботи системи представляється у лінгвістичній і графічних формах.*

Ключові слова: *атаки, кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, атаки в комп'ютерних системах, виявлення аномалій в комп'ютерних мережах.*

Korchenko A.A. Anomaly-based detection system in computer networks

Abstract. *Effective detection of new types of cyber-attacks, such as 'zero-day', as well as attacks which have no signatures associated with the widespread use of appropriate means of protection. The existing intrusion detection systems use the mathematical models for security solution, which require a lot of resources and expenses of different nature, for example, connected with sample of statistical data, training systems, its adaptation, etc. More effective in this regard are peer-based approaches and knowledge of the subject area specialists. To meet this challenge, based on the anomaly detection technique based on fuzzy logic it was suggested the structural solution of anomaly-based detection system in computer networks, created by the unsignature attacks. The system is composed of primary processing subsystems, generation of fuzzy standards and heuristic rules, as well as Fuzzy Modular Arithmetic, linguistic corollary and visualization, that make possible to identify the abnormal condition in the network traffic, generated by a specific type of cyber-attacks. The result of the system is represented in linguistic and graphic forms.*

Keywords: *attacks, cyber-attacks, intrusion detection system, Anomaly-Based Detection Systems, computer networks attacks, anomaly-based detection in computer networks.*

Отримано *8 жовтня 2012 року*, затверджено редколегією *5 листопада 2012 року*
(рецензент д.т.н., професор О.К. Юдін)