УДК 004.7.056.5:004.93(045)



**Федорик С. И.**

# ОБНАРУЖЕНИЕ СЕТЕВЫХ ВТОРЖЕНИЙ МЕТОДАМИ ТЕОРИИ РАСПОЗНАВАНИЯ ОБРАЗОВ (ТЕОРИИ ПАТТЕРНОВ)

Национальный авиационный университет

*Проанализирована проблема защиты от сетевых вторжений. Предложен метод классификации подписей и обнаружения вторжения. Разработан алгоритм сравнительной оценки эффективности различных систем распознавания для компьютерной сети.*

## *Введение*

В настоящее время разработкам в области обеспечения информационной безопасности уделяется повышенное внимание. Действующие специализированные департаменты в корпоративном секторе имеют одни из наибольших бюджетов по сравнению с другими структурными подразделениями. В то же время наблюдаются закономерные тенденции оптимизации времени реагирования и комплексов контрмер к соответствующим угрозам, а также по повышению эффективности управления и контроля комплексных систем безопасности. При этом увеличение количества разновидностей потенциальных угроз, а также интенсивность их возникновения приводят к необходимости разработок новых методов и планов реагирования, а также улучшения существующих [1]. Разработаны общие и специальные рекомендации, методики ранжирования типов угроз информационной безопасности.

Для обеспечения оперативного контроля и прогнозирования состояния информационных ресурсов необходимо создание новых технологий обнаружения признаков кибернетического нападения с использованием активных и пассивных методов и датчиков слежения, выходящих за рамки рутинного аудита операционных систем и журналов сетевых протоколов.

## *Анализ последних исследований и публикаций*

Для создания эффективной методики защиты необходима разработка системы профилирования массива данных, несущих информацию об угрозе. Существующие системы обнаружения сетевых атак [2] достаточно эффективно выполняют детализированные расследования и поиск злоумышленников на основании полученных во время атаки данных, однако, они не в состоянии прогнозировать цели, намерения, дальнейшие действия злоумышленников. В частности, одна из наиболее распространенных систем обнаружения вторжений *BlackICE Defender*, которая используется для обеспечения безопасности систем, обрабатывающих данные открытого характера, функционирует посредством сравнения элементов потока *IP*-данных с имеющейся базой сигнатур. На основании сравнительного анализа система принимает решение блокировать тот или иной пакет, либо пропускать для взаимодействия непосредственно с операционной системой. Сигнатурные системы обнаружения вторжений, в том числе и *BlackICE Defender*, обладают высокой производительностью, эффективностью обнаружения при сравнительно невысоких требованиях к аппаратному обеспечению [3]. Однако они имеют ряд недостатков:

- невозможность ввода новых сигнатур;
- отсутствие системы блокирования неизвестных сигнатур;
- отсутствие возможностей прогнозирования действий злоумышленника;
- отсутствие подсистемы мониторинга аппаратных ресурсов.

### Нерешенные проблемы

Учитывая большое количество данных, разнящихся как по качественным, так и по количественным характеристикам, целесообразно рассматривать некоторые последовательности событий в виде регулярных конфигураций, что, в свою очередь открывает следующие возможности:

- обнаружение сходства элементов, образующих конфигурации;
- обнаружение сходства конфигураций;
- обнаружение условий, при которых непроизводные элементы могут взаимодействовать между собой;
- изучение внутренней топологии регулярных структур.

Сетевые вторжения, локализуемые при помощи анализа соответствующих сигнатур в потоке данных, представляют собой массив несвязанных между собой конфигураций. Однако они включают элементы, которые можно объединить по определенным признакам. В рамках категорий сетевых вторжений (сбор информации, попытка несанкционированного доступа, отказ в обслуживании, подозрительная активность, системные атаки), существуют подвиды атак, которые могут быть реализованы с большей или меньшей вероятностью в зависимости от операционной системы, коммутационного оборудования, системы обнаружения вторжений, типа искомых данных, организационной инфраструктуры и т.д. Однако такое группирование не позволят делать выводы, необходимые для всестороннего изучения и принятия адекватных контрмер.

### Постановка задачи

Существующие сигнатурные системы обнаружения вторжений [4] не могут профилировать перехваченный поток данных распределенных атак для их классификации и отработки сигнала о вторжении.

Второй тип систем обнаружения атак – системы, реагирующие на аномалии в сети как на протокольном, так и на программном уровнях, – не могут адекватно реагировать на разнообразные атаки. Кроме того, из-за сравнительно высоких вероятностей ошибок первого и второго рода их работа в режиме реального времени на объектах инфраструктуры, критичной к атакам, оказывается малоэффективной.

Учитывая вышеизложенное, можно сделать вывод, что для вынесения предположения о цели и последствиях атаки необходима разработка системы обнаружения вторжений, профилирующей комбинации сигнатур и сетевых аномалий на основании задаваемых признаков. Инструментом для эффективного группирования и обработки может стать методика упорядочивания данных, которые не могут быть классифицированы по непосредственным признакам. Наиболее перспективным направлением решения данной задачи является теория распознавания образов (теория паттернов) [5-7].

### Основной материал исследования

Паттерновые сети состоят из модульных логических элементов, называемых образующими. Любая образующая обладает неотделимыми от нее связями, которые могут быть ориентированными (вход → выход) или неориентированными. Образующая, имеющая только входные и/или выходные связи, называется ориентированной, а образующая со связями произвольного направления – неориентированной.

Образующая представляется набором символов, который называется вектором признаков образующей.

Паттерновые сети строятся из связки двух или большего числа образующих. Каждая связка паттерновой сети, в зависимости от данных, присвоенных паре ее связей, может находиться в одном из двух состояний - истинном (замкнутом) или ложном (разомкнутом). Путем замыкания и размыкания связок в паттерновых сетях, составленных из ориентированных образующих, моделируют соединения и разъ-

единения выходов и входов модулей, из которых состоят реальные системы.

Логические и физические модули с входами и выходами можно представить векторами ориентированных образующих:

$$a(gi) = a(i, \gamma_{il}, \beta_{im}^{il}, \beta_{ir}^{out}). \qquad (1)$$

Компоненты $\gamma_{il}, \beta_{im}^{il}, \beta_{ir}^{out}$ параметрической образующей *gi* делятся на две группы. Компоненты первой группы, представленные символами с нижними индексами, называются атрибутами образующей. Если $l$=1, то образующая *gi* имеет только один атрибут $\gamma_{il}$. Компоненты второй группы, представленные в векторе (1) символами β, называются в общей теории паттернов показателями связей образующей. В дискретной теории паттернов [8] показатели связей β и атрибуты γ вектора (1) трактуются как переменные, имеющие соответствующие области значений.

Параметры *l, m, r,* фигурирующие в нижних индексах переменных и образующей *gi*, могут принимать различные числовые значения:

$l$=1,2,...; $m$=0,1,2,...; $r$=0,1,2,.... В результате изменения значений параметров *m, r* из вектора (1) получаются векторы компонент образующих с разными числами входных и выходных связей.

Образующими, которые определяются вектором (1), представляют структуры реальных модулей в обобщенной форме. Поставим в соответствие переменным $\gamma_{il}, \beta_{im}^{il}, \beta_{ir}^{out}$ множества

$$D_{il}, D_{im}^{in}, D_{ir}^{out}, \qquad (2)$$

называемые доменами. В доменах помещаются данные, присваиваемые переменным γ и β векторов компонент образующих.

Для получения образующих с разными числами входных и выходных связей параметры *m, r* в векторе (1) заменяются конкретными числами. Одновременно эти параметры заменяются в доменах (2) такими же числами. Вектор (1) и его домены (2) представляют собой образы структур и содержаний многих образующих, имеющих различные числа входных и выходных связей.

Особыми являются случаи, когда параметры *m* и *r* принимают значения, равные нулю. В случае, когда $m$=0, переменная $\beta_{im1}^{in}$ и домен $D_{im}^{in}$ исключаются из соотношений (1-2). В случае, когда $r$=0, из соотношений (1-2) исключаются переменная $\beta_{ir}^{out}$ и домен $D_{ir}^{out}$. Таким способом строятся модели образующих, которые не имеют входных и выходных связей.

В дискретной теории паттернов применяются три вида образующих - абстрактные, конкретные и ассоциированные.

Абстрактная образующая определяется следующим образом. Во все домены образующей помещается неопределенное значение данных, обозначаемое символом $\lambda_0$. Образующая называется абстрактной, если во всех ее доменах содержится только символ $\lambda_0$ и ни в одном из них нет конкретных данных, характеризующих реальные модульные объекты. Следовательно, абстрактная образующая не определена на какой-либо конкретной информационной среде.

Образующая, в доменах которой, помимо символа $\lambda_0$, помещены данные об одном или нескольких реальных модулях, называется конкретной. Абстрактная образующая превращается в конкретную после размещения в ее доменах данных о реальных модулях. Конкретные образующие занимают промежуточное положение между абстрактными и ассоциированными образующими. Домены конкретных образующих определяются в общем случае как конечные или счетные множества значений переменных $\gamma$ и $\beta$. В этом они аналогичны доменам атрибутов реляционных отношений, которые определяются в теории реляционных баз данных как конечные или счетные множества значений атрибутов.

Если переменным $\gamma$ и $\beta$ конкретной образующей присваиваются взятые из доменов данные о реальном модуле, то образующая становится ассоциированной с данными и служит паттерновой моделью этого модуля.

При анализе событий, которые могут классифицироваться как сетевые вторжения, образующими, согласно теории паттернов, являются дейтаграммы сетевого трафика, сигнатуры как комбинации направленных дейтаграмм – регулярными конфигурациями, комбинации сигнатур и сетевых аномалий – изображениями, а профиль атаки в терминах теории паттернов – образом.

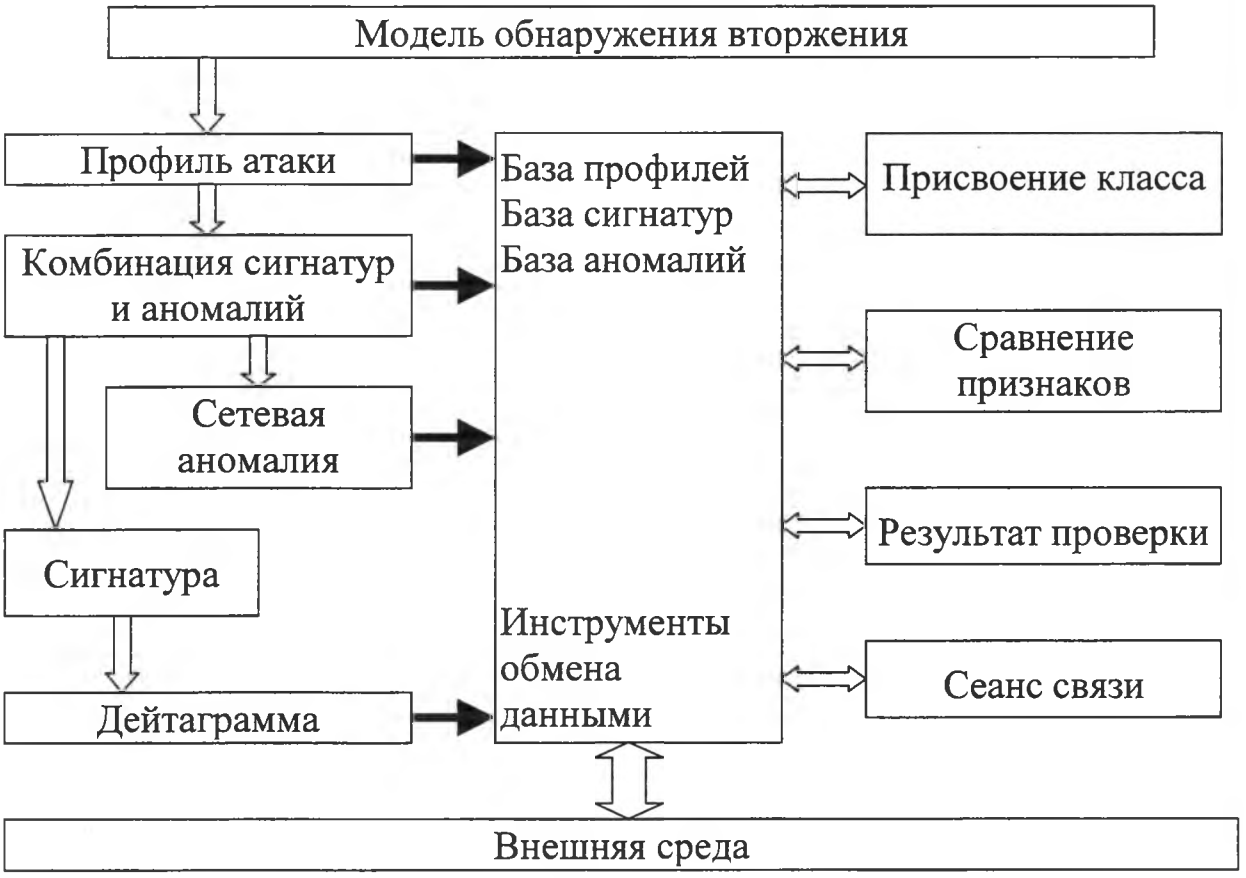


Рис. 1. Иерархическая структура модели обнаружения вторжения.

Известно, что система сетевой безопасности имеет иерархическую структуру, представленную на различных уровнях (см. рис.1). Каждый уровень такой системы имеет свои собственные элементарные единицы, которые могут сочетаться определенным образом. Особую сложность представляет собой согласование переходов с уровня на уровень.

Для перехода от одного уровня к другому недостаточно просто определить правила выделения образующих каждого уровня. Необходимо, кроме того, определить правила соединения образующих в регулярные конфигурации [5]. Ясно, что если имеется конфигурация

$$K_i = \left\{O_1^i, O_2^i, ..., O_n^i\right\}, \qquad (3)$$

которая получена, например, при использовании правила $L_i$ при объединении образующих $O_{ij}$ в регулярную конфигурацию, то она может быть описана в виде

$$K_i = \left\langle N_{k_i}, n, L_i \right\rangle, \qquad (4)$$

где $N_{k_i}$ – наименование конфигурации;

$n$ – количество образующих в конфигурации;

которыми выражаются признаки классифицируемых объектов [K-J, связанных соотношениями вида $5(\in AX,7 \equiv 1,2,\ldots,л$, устанавливаются по результатам предварительно собранных экспериментальных данных или непосредственно в процессе функционирования системы. Эти значения, как правило, устанавливаются не достоверно («да» – «нет»), а с известной неопределенностью, нечеткостью. Причинами этого могут быть следующие факторы.

1. Нечеткие высказывания типа «истинное значение $8$ лежит в пределах интервала А...», причем результат измерения значения $8$ есть случайная величина.

2. Непреднамеренные помехи и/или противодействие противника, вследствие чего создаются предпосылки для ошибочных заключений.

В рассматриваемой задаче наиболее вероятной причиной нечеткости является вторая.

Предположим, что выбранный способ описания классифицируемых объектов позволяет различать между собой все $N$ классов как при представлении их с помощью логических функций $\phi(1(\cdot)) \equiv$ так и через предварительно измеренные или наблюдаемые в ходе опыта признаки $=5; +\delta s_i;\ г \equiv 1,M,\ \delta s_i$- ошибки измерения (наблюдения). Для количественного описания искажений информации о классифицируемых объектах и вытекающих из этого ошибочных решениях, рассмотрим следующие вероятности:

$$\eta_{1,M}(1|1) = P\left(\tilde{5}_i = 1 \mid \quad = 1\right) \qquad (5)$$

– вероятность того, что событие $5_i$ действительно имело место, и будет принято решение $5_i = 1$;

$$\left(\tilde{5}_i \equiv X|5_i = 1\right) \qquad (6)$$

– вероятность того, что событие $S_i$ имело место, а значение истинности элемента $5_i$ не будет установлено;

$$\eta_7((0|1)) = P\left(\tilde{L}_i = 0 \mid s_i = 1\right) \qquad (7)$$

– **вероятность того, что событие $5_i$ имело место, а будет принято решение** $5_i = 0$.

Аналогичные по смыслу вероятности $\eta((0|0)), \eta((x|0)), \eta(1|0)$ можно записать и для случая, когда событие не имело места.

Очевидно, события, описываемые вероятностями (7-9), составляют полную группу.

Поэтому $\eta(1|1) + \eta(x|1) + \eta(0|1) = 1$.

Обозначим через $CУ, i, j = 1,2,\ldots,N$ выигрыш (при $i = j$ - отнесение $i$– го объекта к $i$–му классу) или штраф (при $i \neq j$ - отнесение $i$– го объекта к $j$–му классу), а через $C_{ix}$ – штраф, который накладывается, если для объекта из $j$– го класса не удается получить определенного решения.

Пусть $p$ – условная вероятность принятия того или иного решения (5-7) о принадлежности обнаруженного объекта к $i$– му классу при условии, что в действительности объект принадлежит к $j$–му классу. Тогда условный средний выигрыш $Яу$ от принятия решения при условии, что классифицируемый объект принадлежит к $j$–му классу, определяется следующим выражением:

$$R_j = \sum_{i=1}^{N} C_{ij}\, p_{ij} + C_{N\times,j}\left(1 - \sum_{i=1}^{N} p_{ij}\right) = \\ = C_{N\times,j} + \sum_{i=1}^{N} p_{ij}\left(C_{ij} - C_{N\times,j}\right). \quad (8)$$

Положим априорную вероятность появления объекта, принадлежащего к $j-$ му классу, равной $F_j$. Тогда безусловный средний выигрыш $R$ от принятия решения в системе распознавания определяется выражением

$$R_j = \sum_{i=1}^{N} F_j R_j = \sum_{i=1}^{N} F_j C_{N\times,j} + \\ + \sum_{j=1}^{N}\sum_{i=1}^{N} F_j\, p_{ij}\left(C_{ij} - C_{N\times,j}\right). \quad (9)$$

Таким образом, разрабатывая различные алгоритмы определения истинности признаков $s_i$, и, соответственно, способы задания вероятностей (5-7), можно сравнивать эффективность этих алгоритмов по показателю (9). Выигрыши (или штрафы) $C_{ij}$, $C_{N\times,j}$, и априорные вероятности $F_j$ первоначально задаются одинаковыми (из условия нормировки), а затем корректируются по мере накопления апостериорных данных в процессе функционирования системы распознавания.

### Выводы

Аппарат теории распознавания образов (теории паттернов) целесообразно применять для построения систем профилирования сетевых вторжений.

Для выбора и обоснования адекватных моделей сетевого вторжения необходимо модифицировать известные методы обработки данных с адаптацией к конкретной задаче. Такой подход позволит создать основу для разработки системы профилирования данных, несущих информацию об атаке или угрозе вторжения.

### Список литературы

1. *Cannady, J. and J. Harrell.* «A Comparative Analysis of Current Intrusion Detection Technologies». 4 th Technology for Information Security Conference (TISC'96), May 1996.

2. *Anita K. Jones and Robert S. Sielken.* «Computer System Intrusion Detection». Survey Department of Computer Science, University of Virginia, September, 2000.

3. *Teresa F. Lunt.* «A Survey of Intrusion Detection Techniques». Computers &Security. 12(4), June 1993.

4. *Lunt, T.F.* «Detecting Intruders in Computer Systems». 1993 Conference on Auditing and Computer Technology, 1993.

5. *Гренандер У.* Лекции по теории образов. Синтез образов. / под. ред. Ю. Журавлева; пер. с англ. – М.: Мир, 1979. – 383 с.

6. *Вопросы* статистической теории распознавания. / Барабаш Ю.Л., Варский Б. В., Зиновьев В. Т., Кириченко В. С., Сапегин В. Ф. – М.: Сов. радио, 1967. – 400 с.

7. *Дуда Р., Харт П.* Распознавание образов и анализ сцен. – М.: Мир, 1976. – 511 с.

8. *Шуткин Л. В.* Применение теории паттернов к гипермедиа системам // НТИ, Сер.2. – 1995. – № 7. – С. 19-23.

9. *Маркус С.* Теоретико-множественные модели языков. – М.: Наука, 1970. – 332 с.

10. *Мещеряков Р. В., Бондаренко В. П.* Формирование переходов в иерархии шкал речевых систем. //Диалог-2003. Материалы международной конференции – Протвино, 2003. – М.: ГЕОС, 2003. – С. 50-55