УДК 621.34

С.Г. Семенов[1], Р.В. Королёв[2], С.А. Енгалычев[3]

[1] *Харьковский национальный технический университет «ХПИ», Харьков*
[2] *Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*
[3] *Харьковский национальный университет радиоэлектроники, Харьков*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ И ИСЛЕДОВАНИЕ СИСТЕМ ОБНАРУЖЕНИЯ АТАК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Проведен сравнительный анализ и исследование систем обнаружения атак несанкционированного доступа, приведены их достоинства и недостатки. Выявлены основные угрозы данного вида атак. Проведена оценка эффективности механизмов обеспечения безопасности информационных систем. Приведена классификация различных систем обнаружения атак.

Ключевые слова: *защита информации, несанкционированный доступ, системы обнаружения атак.*

Введение

Постановка проблемы. Интенсивное развитие глобальной информационной инфраструктуры, а так же необходимость интеграции Украины в мировое информационное сообщество на равноправных условиях с остальными участниками этого процесса усилили зависимость показателей эффективности функционирования общества и государства от состояния развития информационной сферы, прежде всего, системы государственного управления национальными информационными ресурсами.

В соответствии с концепцией государственной информационной политики Украины, законами Украины «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист інформації в автоматизованих системах» и др. одной из основных проблем в процессе разработки, внедрения и эксплуатации информационно-телекоммуникационных ресурсов остается обеспечение безопасности, при этом результаты исследований показывают на приоритетность задач, связанных с защитой информационных систем от несанкционированного доступа.

Анализ литературы [1 – 3] показал, что для решения этой проблемы в разных странах используют различные методы и алгоритмы, аппаратные и программные средства, а так же целый ряд специализированных систем [1]. Проведенные исследования показали, что существенный (до 60%) вклад в разработку новых, эффективных средств защиты вносит частный инвестор (отдельные корпорации), не заинтересованный в несанкционированном доступе к своим информационным ресурсам. Особенно заметен этот процесс в банковской сфере (рис. 1).

Проведенный анализ основных угроз безопасности показал, что в 80% случаев несанкционированного доступа злоумышленниками используются программные средства, при этом результатом такого вторжения могут быть не только удаленный контроль (ограниченный в ряде возможностей), но непосредственный доступ к ресурсам системы.

Как показали исследования, использование стандартных антивирусных средств или средств криптографической (парольной) защиты не всегда обеспечивает требуемый уровень безопасности информационных систем. В этой связи представляется целесообразным наряду с использованием уже готовых программных средств использовать новые разработки, направленные на идентификацию такой угрозы, как несанкционированный доступ.

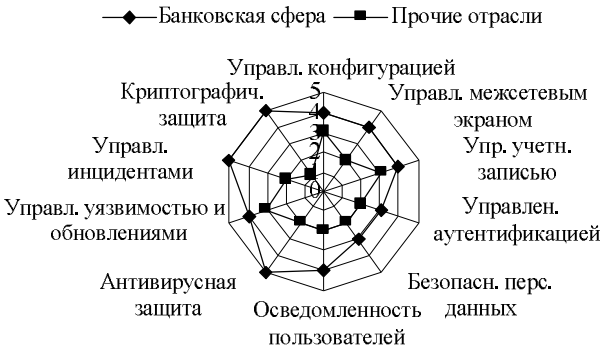

Рис. 1. Оценка эффективности механизмов обеспечения безопасности информационных систем

Целью данной статьи является анализ и сравнительные исследования существующих методов идентификации злоумышленников.

Основная часть

Анализ поведения злоумышленников при попытках осуществления несанкционированного доступа показал, что обнаружение атак является процессом оценки подозрительных действий, которые происходят в исследуемой телекоммуникационной сети.

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа полученной информации. Исследования показали, что на данный момент существует множество различных подходов к обнаружению несанкционированного доступа. Рассмотрим некоторые из них.

Статистический метод. Основным преимуществом статистического подхода является использование известного аппарата математической статистики и адаптация к поведению субъекта. К используемым методам математической статистики можно отнести: теорию измерений; статистику бинарных отношений; статистику случайных множеств; статистику нечетких множеств; статистику интервальных данных и др.

На примере одной из указанных методик (теории измерений) [2, 5] рассмотрим возможности решения поставленной задачи. Как показали исследования, статистические выводы могут быть адекватны реальности только тогда, когда они не зависят единицы измерения выбираемой исследователем, т.е. когда они инвариантны относительно допустимого преобразования шкалы.

Практическую пользу теории измерений обычно демонстрируют на примере задачи сравнения средних значений для совокупностей $x_1, x_2, ..., x_n$ и $y_1, y_2, ..., y_n$. Пусть среднее вычисляется с помощью функции $f : R^n \to R^1$. Если

$$f(x_1, x_2, ..., x_n) < f(y_1, y_2, ..., y_n), \qquad (1)$$

то необходимо, чтобы

$$f(\varphi(x_1), \varphi(x_2), ...\varphi(x_n)) < \\ < f(\varphi(y_1), \varphi(y_2), ...\varphi(y_n)) \qquad (2)$$

для любого допустимого преобразования φ из задающей шкалу группы Ф.

Из [2, 5] известно, что в случае равносильности неравенств (1) и (2), а так же условия регулярности в порядковой шкале в качестве средних можно использовать только члены вариационного ряда, в частности, медиану, но нельзя использовать среднее геометрическое, среднее арифметическое, и т.д.

При идентификации систем теория измерений может использоваться при обработке статистических данных о пользователе легальной системы. В этом случае для всех субъектов анализируемой системы определяются профили. Любое отклонение используемого профиля от эталонного считается несанкционированной деятельностью.

Исследования показали, что статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых уязвимостях.

Экспертные системы. Экспертные системы [4] состоят из набора правил, которые охватывают знания человека-эксперта. Использование экспертных систем представляет собой распространенный метод обнаружения атак, при котором информация об атаках формулируется в виде правил. Эти правила могут быть записаны, например, в виде последовательности действий или в виде сигнатуры. При выполнении любого из этих правил принимается решение о наличии несанкционированной деятельности.

Классификация экспертных систем представлена на рис. 2.

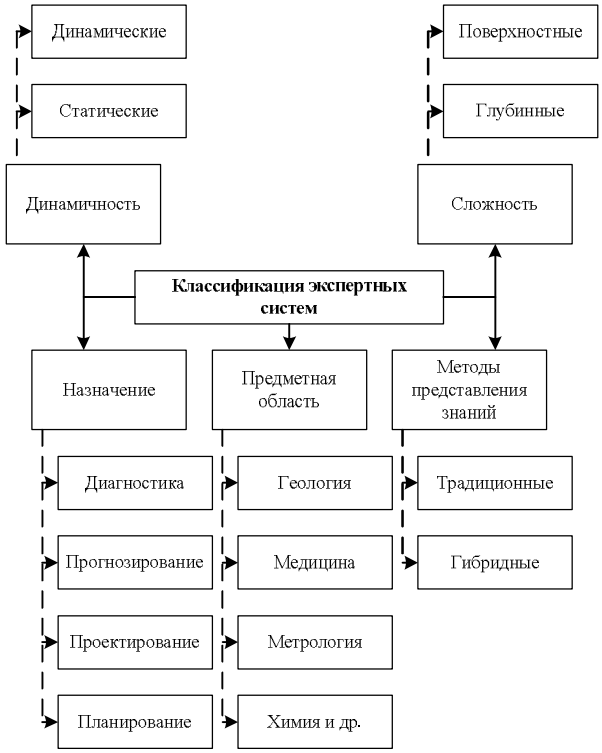

Рис. 2. Классификация экспертных систем

Одним из достоинств использования экспертных систем является практически полное отсутствие ложных тревог.

Однако, как показали исследования отслеживать динамику (прогресс) изменений (развития) в действиях злоумышленника такие системы не в состоянии. Поэтому такие системы более статичны по сравнению с системами, использующими статистический подход или, например, нейронные сети.

Нейронные сети. Иску́сственные нейро́нные се́ти (ИНС) – математические модели, а также их программные или аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма [3].

На рис. 3 представлена классификация нейронных сетей.

В последние десятилетия широкое применение получило моделирование ТКС с помощью нейронных сетей. При этом в качестве показателя качества системы выступает энергетическая функция вида:

$$E = -\frac{1}{2}\sum_i \sum_{j \neq i} w_{ij} x_i x_j , \qquad (3)$$

где w_{ij} – весовой коэффициент между i-м и j-м нейронами; x_i и x_j – компоненты вектора X (входных данных системы).

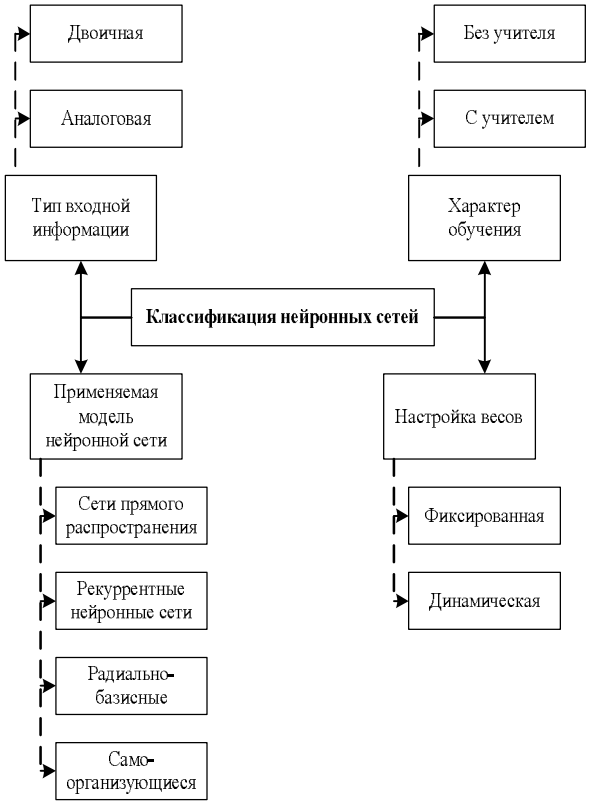

Рис. 3. Классификация нейронных сетей

Нейронные сети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения – одно из главных преимуществ нейронных сетей перед традиционными алгоритмами.

Анализ показал, что в отличие от экспертных систем, которые могут дать пользователю определённый ответ о соответствии рассматриваемых характеристик заложенным в базе данных правилам, нейронная сеть проводит оценку полученных данных и предоставляет возможность выбора решения.

Проведенные исследования моделей телекоммуникационных сетей, представленных в виде нейронных сетей наряду с их достоинствами показали и недостатки связанные с существенными (до 100 наблюдений) временными затратами на процесс обучения при построении модели, и как следствие, «консерватизмом» по отношению к динамическим изменениям поведения злоумышленника.

Однако степень соответствия нейросетевого представления, достоверность выбора полностью зависит от качества системы в анализе примеров поставленной задачи.

Выводы

Проведенный анализ и сравнительные исследования современных подходов выявления несанкционированного доступа позволили сделать вывод о необходимости комплексного использования различных моделей при разработке систем защиты компьютерных и телекоммуникационных систем от несанкционированного доступа.

Список литературы

1. Кузнецов О.О. Протоколи захисту інформації у комп'ютерних системах та мережах: навч. посібник / О.О. Кузнецов, С.Г. Семенов – Х.: ХНУРЕ, 2009. – 186 с.

2. Орлов А.И. Нечисловая статистика / А.И. Орлов. – М.: МЗ-Пресс 2004. – 513 с.

3. Галушкин А.И. Теория нейронных сетей. Уч. пособие для вузов / А.И. Галушкин – М.: ИПРЖР, 2000. – 416 с.

4. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник / С.О. Субботін. – Запоріжжя: ЗНТУ, 2008. – 341 с

5. Orlov A.I. On the Development of the Statistics of Non-numerical Objects. – In: DESIGN OF EXPERIMENTS AND DATA ANALYSIS: NEW TRENDS AND RESULTS. Ed. by prof. E.K.Letzky. – Moscow: ANTAL, 1993. – P. 52-90.

Поступила в редколлегию 21.04.2011

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

ПОРІВНЯЛЬНИЙ АНАЛІЗ І ДОСЛІДЖЕННЯ СИСТЕМ ВИЯВЛЕННЯ АТАК НЕСАНКЦІОНОВАНОГО ДОСТУПУ

С.Г. Семенов, Р.В. Корольов, С.О. Енгаличев

Проведений порівняльний аналіз і дослідження систем виявлення атак несанкціонованого доступу, приведені їх достоїнства і недоліки. Виявлені основні погрози даного виду атак. Проведена оцінка ефективності механізмів забезпечення безпеки інформаційних систем. Приведена класифікація різних систем виявлення атак.

Ключові слова: *захист інформації, несанкціонований доступ, системи виявлення атак.*

COMPARATIVE ANALYSIS AND ИСЛЕДОВАНИЕ OF SYSTEMS OF FINDING OUT ATTACKS OF UNAUTHORIZED DIVISION

S.G. Semenov, R.V. Korolyov, S.A. Engalychev

A comparative analysis and research of the systems of finding out the attacks of unauthorized division is conducted, their dignities and failings are resulted. The basic threats of this type of attacks are exposed. The estimation of efficiency of mechanisms of providing of safety of the informative systems is conducted. Classification of the different systems of finding out attacks is resulted.

Keywords: *defence of information, unauthorized division, systems of finding out attacks.*