Выводы. Результаты проведенных исследований показывают, что разработанные модули защиты интернет-магазина позволяют защититься от таких атак злоумышленника как несанкционированный доступ и кража платежных данных из БД, XSS-атаки, SQL-инъекции, а следовательно могут использоваться при разработке и сопровождения реальных систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. January 2013 WebServerSurvey.[Электронный ресурс] – Официальный сайт компании Netcraft. – Режим доступа:http://news.netcraft.com/ (дата обращения 23.02.2014).
2. Статистика web-уязвимостей за 2013 год. [Электронный ресурс] – Режим доступа: http://netnsk.ru/publica/security/sec_10.php (дата обращения 23.02.2014).
3. *Леонтьев В.С.* Безопасность в сети интернет. – М.: ОЛМА Медиа Групп, 2008. – 256 с.
4. *Рэйнолдс М.* Сделай сам Интернет-магазин. – М.: Изд-во “Лори”, 2009. – 538 с.
5. Защита Web приложений//ООО «СОВИТ». [электронный ресурс]: URL –http://www.sovit.net/services/endpoint_security/web_application_protection (дата обращения 23.02.2014).
6. Статистика национального домена в рунете//Координационный центр национального домена сети интернет: URL - http://www.cctld.ru/ru/statistics (дата обращения 23.02.2014).
7. Статистика и аналитика // Домена России: URL – http://statdom.ru/researchs (дата обращения 23.02.2014).

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Оладько Алексей Юрьевич – Волгоградский государственный университет; e-mail: bop-x@yandex.ru; 400062, г. Волгоград, пр-т Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; старший преподаватель.

Аткина Владлена Сергеевна – e-mail: atkina.vlaldlena@yandex.ru; кафедра информационной безопасности; к.т.н.; старший преподаватель.

Oladko Alexey Yuryevich – Volgograd State University; e-mail: bop-x@yandex.ru; 100, Ave University, Volgograd, 400062, Russia; phone: +78442460368; the department of information security; lecture.

Atkina Vladlena Sergeevna – e-mail: atkina.vlaldlena @ yandex.ru; the department of information security; cand. of eng. sc.; lecture.

УДК 004.056

А.В. Никишова, Р.Ф. Рудиков, Е.А. Калинина

НЕЙРОСЕТЕВОЙ АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Статистика за 2013 год и предсказания на 2014 год относительно атакующих воздействий на информационную систему показывает как рост возникающих атакующих воздействий из числа известных, так и рост новых образцов и направлений реализации атак. В связи с этим актуальной является задача сбора сведений о событиях, происходящих в информационной системе и относящихся к основным объектам информационной системы, и проведение их эффективного анализа. Основными требованиями к средствам анализа являются: скорость и возможность приспособления к новым обстоятельствам – адаптивность. Средствами, удовлетворяющими этим требованиям, являются системы искусственного интеллекта. В частности существует ряд исследований, применяющих нейронные сети в качестве средства анализа. Выделяют различные типы нейронных сетей, различающиеся в зависимости от решаемых задач и более подходящие для различных входных данных. Построена многоагентная система обнаружения атак, осуществляющая сбор и анализ собранных сведений о событиях информационной системы с помощью двух типов нейронных сетей. Для анализа различных журналов

объектов информационной системы применяется многослойный персептрон. Для анализа непосредственно собираемых сведений о событиях объектов информационной системы применяется сеть Джордана. Применение многоагентной системы обнаружения атак позволяет повысить защищенность информационной системы.

Нейронная сеть; многослойный персептрон; события безопасности; атаки; система обнаружения атак; многоагентная система обнаружения атак.

A.V. Nikishova, R.F. Rudikov, E.A. Kalinina

NEURAL NETWORK ANALYSIS OF SECURITY EVENTS IN INFORMATION SYSTEM

Statistics for 2013 and predictions for 2014 relative to the attacking impacts on the information system shows the growth of emerging attacking impacts from a number of known and also the growth of new designs and directions of implementation of attacks. In this regard, the urgent task is to gather information about events occurring in the information system and related to the main objects of the information system and conducting effective analysis. The main requirements to the analysis means are: speed and the ability to adapt to new circumstances - adaptability. The means that can satisfy these requirements are in artificial intelligence systems. In particular there are a number of studies, using neural networks as a tool of analysis. There are different types of neural networks, which differ depending on the task and more suitable for various input data. The multi-agent intrusion detection system engaged in the collection and analysis of the collected information about the events of the information system with two types of neural networks has been built. For analysis of various objects' of the information system logs multilayer perceptron is used. For analysis directly collected information about events of information system's objects the Jordan's network is used. Application of multi-agent intrusion detection system allows increasing the security of the information system.

Neural network; multilayer perceptron; security event; attacks; intrusion detection system; multi-agent intrusion detection system.

В информационной системе ежесекундно происходит огромное количество событий, влияющих на состояние информационной системы и определяющие переходы информационной системы из одного состояния в другое. С точки зрения защищенности информации хранящейся, обрабатывающейся и передающейся внутри информационной системы можно выделить три состояния: нормальное, аномальное, опасное.

В нормальном состоянии информационная система функционирует в повседневном режиме, в соответствии со своими задачами и согласно документам, регламентирующим ее работу, а для защищаемой информации обеспечивается конфиденциальность, доступность и целостность. Отнесем к нормальным событиям такие события S^n, которые переводят информационную систему в нормальное состояние.

В аномальном состоянии функционирование информационной системы отличается от функционирования в нормальном состоянии, однако однозначные признаки проявления атакующих воздействий отсутствуют, т.е. для защищаемой информации также обеспечивается конфиденциальность, доступность и целостность. Отнесем к аномальным событиям такие события S^a, которые переводят информационную систему в аномальное состояние.

В опасном состоянии нормальное функционирование информационной системы нарушается, приводя к нарушению конфиденциальности, доступности или целостности хранящейся, обрабатывающейся или передающейся в информационной системе информации. Отнесем к опасным событиям такие события S^d, которые переводят информационную систему в опасное состояние.

Подобное деление можно представить в виде конечного автомата (рис. 1).

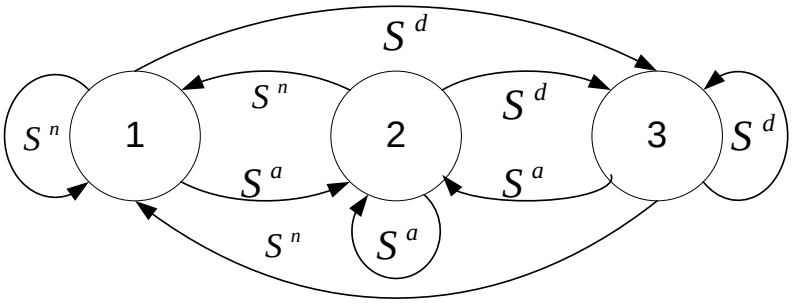

Рис. 1. Конечный автомат перехода информационной системы из одного состояния в другое

Здесь «1» соответствует нормальному состоянию информационной системы, «2» – аномальному состоянию информационной системы, и «3» – опасному состоянию информационной системы.

С учетом большого числа событий, происходящих в информационной системе, требуется проводить автоматический сбор и автоматизированный анализ сведений, описывающих происходящие события.

Выделяют следующие основные источники сведений о событиях, которые следует анализировать для определения состояния, в котором находится информационная система:

- сведения о сетевых пакетах;
- журналы маршрутизаторов;
- журналы операционных систем;
- журналы приложений;
- журналы баз данных;
- сведения о процессах.

Эти источники в первую очередь отличаются между собой характером зависимости появляющихся в них событий. Источники событий, являющиеся журналами, отражают некоторую выборку событий информационной системы наиболее важных с точки зрения разработчика соответствующего объекта информационной системы. Поэтому, хотя некоторые события, принадлежащие этим источникам, и возникают группами, которые можно рассматривать как цепочку взаимосвязанных событий, но в целом эти источники не сохраняют корреляцию исходного потока событий, что дает возможность определять их как множество независимых событий.

С другой стороны если рассматривать сведения о сетевых пакетах или процессах, запущенных в системе, то они являются прямой информацией, об объектах информационной системы, что дает возможность говорить об их взаимной зависимости.

Проводя анализ сведений о событиях из любого из приведенных источников, необходимо решать задачу классификации, относя текущее событие к одному из трех классов событий $\{S^n, S^a, S^d\}$. Кроме этого важными показателями для средств анализа являются скорость анализа и простота процесса приспособления средств к новым видам событий, то есть обучения средств анализа.

Одним из возможных направлений развития средств анализа событий информационной системы, отвечающих данным тенденциям, является использование нейронных сетей. Использование нейронных сетей обусловлено следующими их свой-

ствами: выявление скрытых закономерностей, классификация согласно выявленным закономерностям, высокая устойчивость к зашумлению обрабатываемых данных и отсутствие необходимости жесткой формализации решаемых задач.

Нейронные сети по своей природе являются параллельным средством обработки информации. Такая "врожденная" параллельность обработки позволяет эффективно использовать все ресурсы современных аппаратных решений, что увеличивает скорость проведения анализа.

Для проведения комплексного анализа сведений о событиях информационной системы, относящихся ко всем приведенным источникам, требуется два типа нейронных сетей. Оба они должны осуществлять классификацию. Один из них должна подходить для анализа независимых событий, в то время как другой – для выполнения анализа взаимосвязанных событий.

Были выбраны два типа нейронных сетей, отвечающих данным требованиям: многослойный персептрон и сеть Джордана.

Многослойный персептрон (рис. 2) характеризуется прямым распространением сигналов от входов нейронной сети к ее выходам, что позволяет проводить анализ независимых событий. Так как результат выхода нейронной сети зависит только от значений входного вектора, переданного нейронной сети в данный момент.

На рисунке через x_i обозначены компоненты входного вектора, через v_{ji} – веса синаптических связей между входным и скрытым слоем, через y_i – выходы нейронов скрытого слоя, через w_j – веса синаптических связей между скрытым и выходным слоем, через o – выход нейронной сети.

Нейроны скрытых слоев многослойного персептрона, осуществляющие основную обработку входного сигнала, имеют сигмоидную передаточную функцию. Для приведенной задачи классификации выход нейрона, обладающего данной передаточной функцией, имеет следующую интерпретацию (рис. 3).

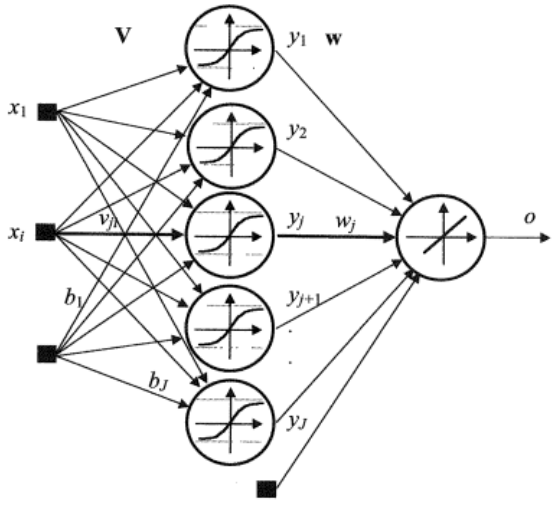

Рис. 2. Пример многослойного персептрона с одним скрытым слоем

Если выход сигмоидной передаточной функции нейрона скрытого слоя оказывается в нижней части графика, т.е. меньше некоторого порогового значения, отмеченного на графике нижней прямой, то событие, анализируемое в данный момент нейронной сетью, относится к классу событий S^d.

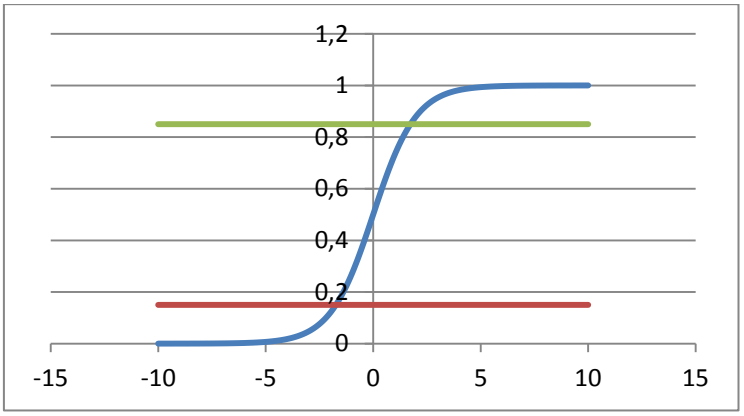

Рис. 3. Интерпретация выхода сигмоидной передаточной функции нейрона

Если выход сигмоидной передаточной функции нейрона скрытого слоя оказывается в верхней части графика, т.е. больше некоторого порогового значения, отмеченного на графике верхней прямой, то событие, анализируемое в данный момент нейронной сетью, относится к классу событий S^n.

Если выход сигмоидной передаточной функции нейрона скрытого слоя оказывается на склоне сигмоидной функции, т.е. между заданными пороговыми значениями, отмеченными прямыми на графике, то событие, анализируемое в данный момент нейронной сетью, относится к классу событий S^a.

Нейронная сеть Джордана (рис. 4) получена на основе многослойного персептрона, путем введения обратных связей, передающих сигнал с нейронов выходного слоя на соответствующие им нейроны во входном слое.

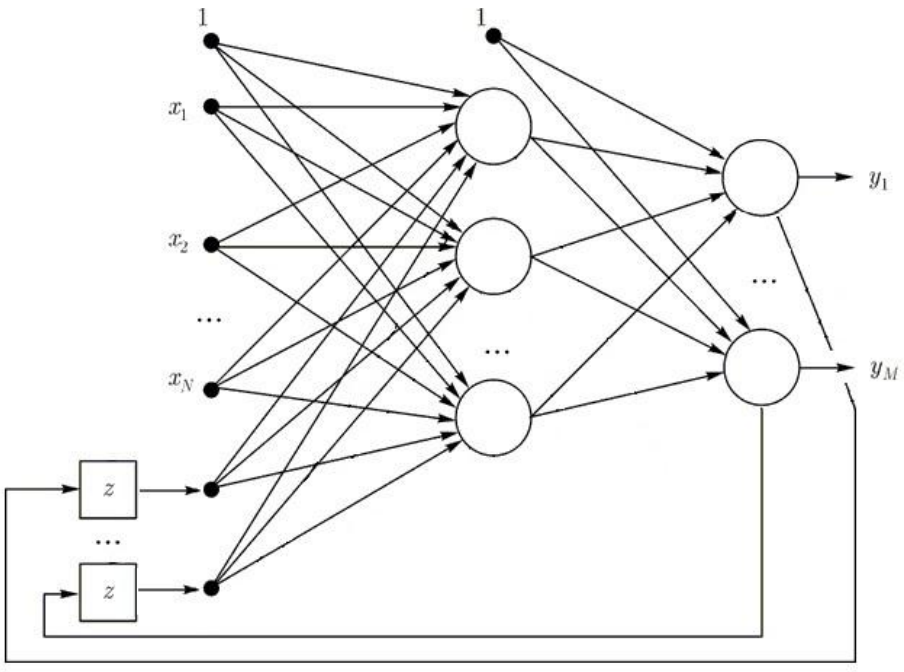

Рис. 4. Нейронная сеть Джордана

На рисунке через x_i обозначены компоненты входного вектора, через y_i – выходы нейронной сети, через z – контекстные нейроны, т.е. нейроны входного слоя, соответствующие нейронам выходного слоя.

В сети Джордана передача сигналов на контекстные нейроны происходит с задержкой в один такт сети. Таким образом, получается зависимость решения нейронной сети от прошлых состояний нейронной сети, а значит и состояний информационной системы. Такая способность позволяет использовать нейронную сеть для анализа связанных совокупностей событий, где анализ событий независимо не является правильным.

Оба типа нейронных сетей обучаются с учителем. Поэтому для их обучения специалист по защите информации должен сформировать обучающую выборку, содержащую образцы событий всех трех классов.

Для реализации предложенных принципов разработана многоагентная система обнаружения атак на информационную систему [1] (рис. 5), осуществляющая сбор сведений о событиях из выделенных источников и анализ этих сведений с помощью нейронной сети. В системе представлены нейронные сети обоих типов, применяемые для различных источников.

Агенты маршрутизаторов и часть агентов рабочих станций и серверов, работающих с журналами событий, осуществляют анализ собранных сведений с помощью многослойного персептрона. Агенты сети и часть агентов рабочих станций и серверов, осуществляющих непосредственный сбор сведений о состоянии объектов информационной системы, используют для проведения анализа нейронную сеть Джордана.

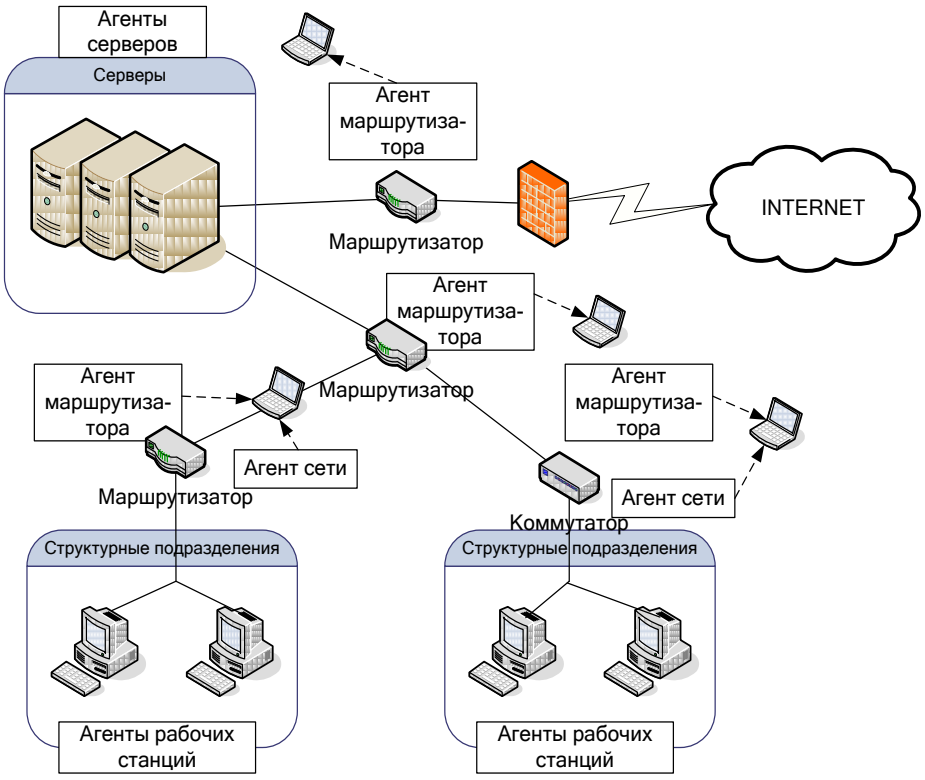

Рис. 5. Состав многоагентной системы обнаружения атак

Выводы. Для разработанной многоагентной системы обнаружения атак, применяющей нейронные сети обоих типов, были проведены экспериментальные исследования, подробно описанные в [2]. По результатам экспериментов количество пропусков атак в среднем уменьшилось в 1,1 раза, количество ложных срабатываний в среднем уменьшилось в 3,8 раза. Это позволяет сделать вывод о повышении защищенности информационной системы при применении разработанной многоагентной системы обнаружения атак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Никишова А.В.* Принципы функционирования многоагентной системы обнаружения атак // Известия ЮФУ. Технические науки. – 2012. – № 12 (137). – С. 28-33.
2. *Никишова А.В., Чурилина А.Е.* Обнаружение распределенных атак на информационную систему предприятия // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 135-143.

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Бабенко.

Никишова Арина Валерьевна – Волгоградский государственный университет; e-mail: arinanv@mail.ru; 400062, г. Волгоград, пр. Университетский, 100; тел.: 88442460368; кафедра информационной безопасности; к.т.н.; старший преподаватель.

Рудиков Роман Федорович – e-mail: rudikovrf@gmail.com; кафедра информационной безопасности; студент.

Калинина Екатерина Александровна – e-mail: kalinina573@gmail.com; кафедра информационной безопасности; студентка.

Nikishova Arina Valerievna – Volgograd State University; e-mail: arinanv@mail.ru; 100, Universitetsky prospect, Volgograd, 400062, Russia; phone: +78442460368; the department of informational security; cand. of eng. sc.; lecturer.

Rudikov Roman Fedorovich – e-mail: rudikovrf@gmail.com; the department of informational security; student.

Kalinina Ekaterina Aleksandrovna – e-mail: kalinina573@gmail.com; the department of informational security; student.

УДК 004.056

И.Ю. Половко, О.Ю. Пескова

АНАЛИЗ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ К СИСТЕМАМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Работа посвящена проблеме оценки качества систем обнаружения вторжений. Проведен сравнительный анализ принятых ФСТЭК требований к системам обнаружения вторжений и перечня функциональных характеристик СОВ. Основной целью данных характеристик является определение функциональных способностей систем обнаружения вторжений (например, обнаружение вторжений в защищаемую сеть, способность сообщать о возникших инцидентах, производить сбор и сохранение информации). Проведенный анализ показал, что принятые требования не позволяют полноценно сравнить функциональные возможности различных систем обнаружения вторжений. Практическое использование принятых требований способствует решению задач классификации СОВ, но не достаточно, чтобы оценить качество реализации функций безопасности в рассматриваемых системами обнаружения вторжений. Для решения вопросов, связанных с оценкой ка-