Литература: ***1.*** *Воронцов Ю. В., Гайдамакин Н. А. Модель комплексной оценки защищенности компьютерных систем в идеологии ущерба от угроз безопасности. "Вопросы защиты информации", №1, 2003 г.* ***2.*** *Вихорев С. В., Кобцев Р. Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации. Журнал "Защита информации. Конфидент", №2, 2003.*

УДК 681.3

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ВЕРОЯТНОСТНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ РЕШЕНИЯ ЗАДАЧИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ КОМПЬЮТЕРНЫХ СИСТЕМ

Елена Высоцкая, Анатолий Давиденко*
Национальный авиационный университет
**Институт проблем моделирования в энергетике им. Г. Е. Пухова НАН Украины*

Аннотация: **Исследуется возможность и эффективность применения вероятностных нейронных сетей для аутентификации пользователя компьютерных систем. Определяются ограничения, которые связанны с областью применения данного подхода. Выделяются наиболее критичные параметры, за счет настройки которых можно повышать эффективность данного метода. Проводится количественный и качественный анализ этих параметров.**

Summary: **In this article the opportunity and efficiency of application of probabilistic neural networks for authentification of the user of computer systems is researched. The limitations are defined, which one are connected with area of applicability of this approach. The most critical parameters are selected, at the owing to of regulation which one are possible are to raise efficiency of this method. The quantitative and qualitative analysis of these parameters will be carried out.**

Ключевые слова: **Вероятностные нейронные сети, аутентификация пользователя, классификация, распознавание образов, защита информации.**

Одной из наиболее часто встречающихся угроз является угроза несанкционированного доступа к компьютерной системе пользователей, которые являются сотрудниками организации или имеют временный доступ к системе. Одним из способов решения этой проблемы является аутентификация пользователя компьютерной системы. Поэтому можно сказать, что одной из главных задач защиты информации [1 – 3] является задача аутентификации пользователей компьютерных систем. В результате рассмотрения основных способов аутентификации был выбран механизм, который использует особенности работы пользователя на клавиатуре, т. е. “почерк” пользователя. При этом задачу аутентификации можно свести к задаче классификации или распознавания образов. Одним из наиболее эффективных механизмов для решения этих задач являются механизмы на базе нейронных сетей [4 – 11]. В результате анализа особенностей основных видов нейронных сетей [4 – 6], были выбраны вероятностные нейронные сети (сеть PNN – Probabilistic Neural Network) [4].

Цель данной работы:

1. исследовать возможность применения вероятностных нейронных сетей для аутентификации пользователя компьютерных систем;
2. определить эффективность использования вероятностных нейронных сетей для решения выбранной задачи;
3. определить ограничения, которые связанны с областью применения данного подхода;
4. выделить наиболее критичные параметры, за счет настройки которых можно повышать эффективность данного метода;
5. провести количественный и качественный анализ наиболее критичных параметров.

Для достижения поставленной задачи была создана на языке Borland C++ Builder программа на базе вероятностной нейронной сети для определения эффективности применения данного вида нейронных сетей для решения задачи аутентификации пользователей компьютерной системы. Для обработки и хранения информации использовалась программа для работы с базами данных Database Desktop 7.0 и SQL-запросы. Затем, с помощью созданной программы была накоплена информация о “почерке” работы на клавиатуре некоторого количества пользователей, после чего, на основе этих данных было проведено ряд экспериментов.

При накоплении информации пользователям необходимо было набрать некоторое количество раз набор из 10 слов, каждое из которых повторялось по 10 раз. У всех этих слов последние 6 букв были одинаковыми. При наборе система замеряла время необходимое для набора каждого символа. Далее эта информация использовалась для аутентификации пользователя компьютерной системы.

Архитектура вероятностной нейронной сети имеет вид, представленный на рис. 1.

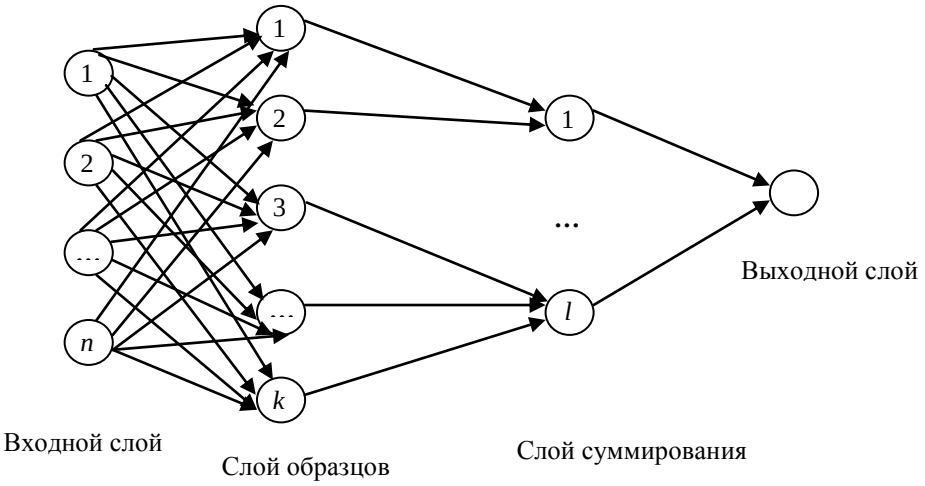

Рисунок 1 – Архитектура вероятностной нейронной сети для решения задачи аутентификации пользователя компьютерной системы

Количественно определим архитектуру сети, исходя из структуры учебных данных, в соответствии с предлагаемой постановкой задачи:

- число входных элементов равно числу признаков; в качестве признаков используем время набора соответствующего символа слова; таким образом, если мы анализируем время набора шести символов, то входной слой будет состоять из шести элементов;
- число элементов слоя образцов равно числу учебных образцов; в нашем случае, учебным образцом будут данные о времени набора одним пользователем символов одного слова при одной попытке; следовательно, количество элементов в слое образцов равняется количеству пользователей, для которых строится сеть, умноженному на количество слов, введенных каждым пользователем;
- число элементов слоя суммирования равно числу классов; при решении задачи аутентификации необходимо определить конкретного пользователя системы; поэтому классом является пользователь системы; следовательно, количество пользователей в системе определяет количество классов;
- выходной слой имеет всегда один элемент.

Входной слой распределяет данные входного образца для слоя образцов, т. е. входной слой имеет столько элементов, сколько признаков. Слой образцов имеет по одному элементу для каждого образца из набора учебных данных. Первый слой весовых значений определяется учебными образцами, т. е. для входящих в элемент слоя образцов связей весовые значения устанавливаются равными элементам соответствующего вектора-образца.

В зависимости от выбора функции активации изменяется эффективность работы сети при решении конкретной задачи. Для определения активности элемента слоя образцов используем квадрат евклидового расстояния от неизвестного экземпляра до элемента слоя образцов.

Будем определять активность элемента слоя образцов по формуле [12]:

$$O_j = \exp\left(\frac{\sum x_i w_{ij} - 1}{\sigma^2}\right).$$

где x – неизвестный входной образец, σ – ширина функции активности, w – вес связи, входящей в элемент слоя образцов.

В этом случае вектор входных данных должен быть нормализован по формуле:

$$xn_i = \frac{x_i}{\sqrt{\sum_{i=1}^{k} x_i^2}},$$

где xn_i – нормализованный признак, x_i – ненормализованный признак.

Слой суммирования имеет по одному элементу для каждого класса из учебного множества данных. К любому элементу слоя суммирования идут связи только от элементов слоя образцов, принадлежащих соответствующему классу. Весовые значения связей, идущих от элементов слоя образцов к элементам слоя суммирования, устанавливаются равными 1. Элемент слоя суммирования складывает выходные значения элементов слоя образцов. Полученная сумма дает оценку значения функции плотности распределения вероятностей для всего набора экземпляров соответствующего класса. Выходной элемент представляет собой дискриминатор пороговой величины, указывающий элемент слоя суммирования с максимальным значением, т. е. указывает, к какому классу принадлежит неизвестный экземпляр.

Для сети PNN не требуется обучение в привычном понимании, потому что все параметры сети PNN, такие как число элементов и значение весов, определяются непосредственно учебными данными.

Когда сеть построена, неизвестный экземпляр подается на вход сети, и в результате прямого прохода через сеть выходной слой укажет класс, к которому, вероятнее всего, принадлежит образец.

Сети PNN очень удобно использовать для классификации. Они быстро обучаются, допускают наличие ошибочных данных и обеспечивают хорошие результаты даже на малых наборах учебных данных, поэтому этот вид нейронных сетей и был выбран для решения поставленной задачи.

На основе описанной архитектуры вероятностной нейронной сети, как уже было сказано, была создана программа для определения эффективности применения вероятностной нейронной сети для решения задачи аутентификации пользователей компьютерной системы.

Созданная версия программы включает в себя функции четырех групп:

- накопление информации;
- анализ накопленной информации;
- настройки;
- выход из программы.

Накопление информации заключается в сборе данных о характере работы пользователя на клавиатуре. Тестируемому пользователю предлагается сначала ввести фамилию, имя, отчество и выбрать текущую дату. Потом начинается тест. Тест заключается в вводе набора слов. Набор состоит из десяти слов. Минимальное количество повторений каждого слова в тесте – одно, а максимальное – десять. Чем больше количество повторений каждого слова и количество выполненных тестов, тем результативнее будет работать вероятностная нейронная сеть, но минимальное количество введенных слов – тысяча. Эта тысяча слов используется как учебные данные для нейронной сети, а остальные образцы служат для определения эффективности работы сети. При вводе слов замеряется время, необходимое для ввода каждого символа. Время измеряется в миллисекундах. Полученные данные хранятся в базе данных. Кроме того в базе сохранялось количество ошибок при наборе каждого слова. После выявления того, что ошибки при наборе текста имеют большое влияние на правильность аутентификации, программа была модифицирована и теперь если при наборе слова допускается ошибка, то время набора символов этого слова удаляется и данное слово необходимо набрать снова. Тоже самое происходит и в случае, если при наборе одного из символов слова происходит большая временная задержка.

Анализ накопленной информации состоит из трех частей:

- анализ, который не использует вероятностную нейронную сеть;
- анализ с использованием вероятностной нейронной сети;
- определение характеристик работы пользователей на клавиатуре.

Анализ, который не использует вероятностную нейронную сеть, состоит из просмотра имеющейся базы данных и графического представления имеющейся информации.

При просмотре имеющейся базы данных возможен отбор по фамилии пользователя и по анализируемому слову. При этом показывается количество найденных записей.

Графическое представление заключается в построении графиков зависимостей времени набора каждого символа слова от самого символа. На каждой странице можно построить не больше десяти графиков и эти графики должны быть для одного и того же слова. Для построения графиков предоставлено две “книжки” по десять страниц каждая. Если на одной странице строить несколько графиков, то очень удобна функция построения графика средних значений. Также предусмотрена возможность распечатки построенных графиков.

Анализ с использованием вероятностной нейронной сети заключается в построении вероятностной

нейронной сети для указанных пользователей. При этом, для построения сети показывается количество записей в базе и для скольких пользователей есть данные. После этого необходимо указать, для каких пользователей построить сеть (минимальное количество пользователей – 2). Для указанных пользователей производится разделение данных на учебные и неизвестные образцы. Тысяча записей используются как учебные образцы, а для остальных образцов определяется, к какому пользователю они принадлежат. После проверки всех "неизвестных" экземпляров вычисляется, для скольких проверенных образцов принадлежность определена правильно, после чего эти результаты переводятся в процентное соотношение. Для построения сети необходимо также указать ширину функции и необходимость отбора по словам (сравнивать "неизвестные" экземпляры со всеми учебными данными или только с такими же словами).

Также, предусмотрена возможность тестирования построенной сети с изменением ширины функции, количества признаков, самих признаков, количества учебных данных, количества пользователей компьютерной системы и при условии, что усреднение учебных данных (по 10) проводится или не проводится. Сеть рассматривается при условии, что отбор по словам проводится и не проводится. Значение ширины функции можно указывать, а можно протестировать сеть в режиме выбора оптимального значения ширины функции активности. При этом с помощью перебора выбирается значение данного параметра, при котором вероятность правильного ответа для каждой рассматриваемой комбинации пользователей наибольшая и при этом значении считается результирующая эффективность. Диапазон рассматриваемых значений – от 0.1 до 1.0 с шагом 0.01.

По результатам анализа и тестирования сети создаются отчеты, которые можно сохранить на диске для дальнейшего просмотра, а также распечатать.

Кроме того, на этой экранной форме предусмотрена возможность просмотреть созданные ранее отчеты.

При определении характеристик работы пользователей на клавиатуре вычисляются такие параметры как скорость набора текста, процент ошибок при наборе и неравномерность набора текста.

В разделе настроек есть три пункта:

- изменить настройки;
- добавить новый набор;
- переписать таблицу;
- доступ.

При изменении настроек можно изменить:

- номер просматриваемого набора слов;
- номер набора, который будет предлагаться при прохождении теста для сбора информации;
- количество повторений каждого слова при прохождении теста;
- количество предлагаемых слов при прохождении теста.

При добавлении нового набора необходимо ввести десять слов, после чего новый набор можно сохранить в специальной таблице базы данных.

Учитывая, что сбор данных может происходить на разных компьютерах, не связанных между собой, очень полезной является функция дополнения таблицы с данными информацией из другой таблицы с такой же структурой. При этом, необходимо указать из какой таблицы в какую переписывать информацию. С помощью этой функции можно объединить данные, собранные на разных компьютерах.

В системе организовано разграничение доступа. При запуске программы пользователю доступны только несколько необходимых ему функций: тест; анализ, который не использует вероятностную нейронную сеть; доступ; выход. А для изменения настроек и проведения экспериментов необходим пароль администратора, который надо ввести в экранной форме "доступ". И только после этого открывается доступ к остальным функциям программы.

Для того, что бы обеспечить гарантию сохранения измененных настроек при случайном выходе, организована дополнительная защита – выход из программы можно осуществить только тогда, когда все измененные настройки сохранены.

С помощью этой программы, как уже было сказано, была накоплена информация о "почерке" работы на клавиатуре некоторого количества пользователей, после чего на основе этих данных было проведено ряд экспериментов.

При проведении экспериментов определялось влияние следующих параметров на эффективность применения вероятностной нейронной сети для решения поставленной задачи.

- Количество ошибок при наборе текста, или другими словами, внимательность пользователей при работе за клавиатурой.

- Наличие усреднения учебных данных, при котором увеличивается точность данных, но уменьшается их количество.

- Наличие отбора по словам, т. е. возможность сравнивать “неизвестные” экземпляры со всеми учебными данными или только с такими же словами. Если отбор не проводить, тогда не точным будет только первый признак, а при проведении отбора этих неточностей не будет, но количество учебных данных уменьшится в 10 раз.
- Количество признаков.
- Количество учебных данных.
- Ширина функции активности.

Сначала пользователи были разделены на три группы в зависимости от количества ошибок при наборе текста. Первая группа – 1 – 6%, вторая группа – 7.5 – 9.6%, третья группа – 10 – 16.4%. После чего сеть была протестирована для каждой из этих групп. В первой и второй группе эффективность отличается на 1 – 7%, причем, чем больше учебных данных, тем разница больше, особенно при относительно большом количестве пользователей, а между первой и третьей, и второй и третьей группами эффективность отличается на 15 – 24%. При этом, надо заметить, что амплитуда процента ошибок в первой и второй группах значительно отличается – этим и объясняется относительно не очень большая разница эффективностей для этих двух групп. На рис. 2. показано влияние количества ошибок при наборе текста на эффективность работы вероятностной нейронной сети при решении задачи аутентификации пользователя компьютерной системы, при условии что признаков – 6, учебных данных – 1500, отбора по словам нет, усреднения нет. Из этой группы экспериментов можно сделать следующие выводы:

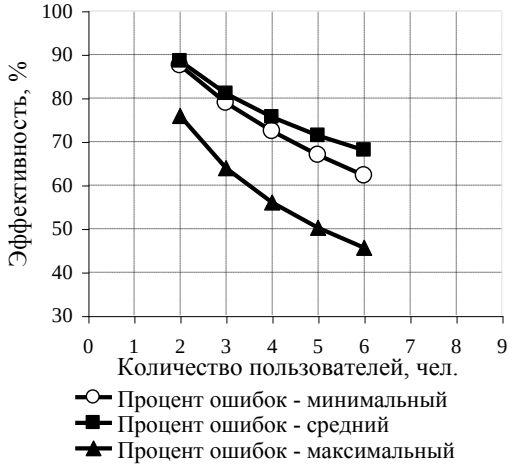

Рисунок 2 – Результаты первой гуппы экспериментов

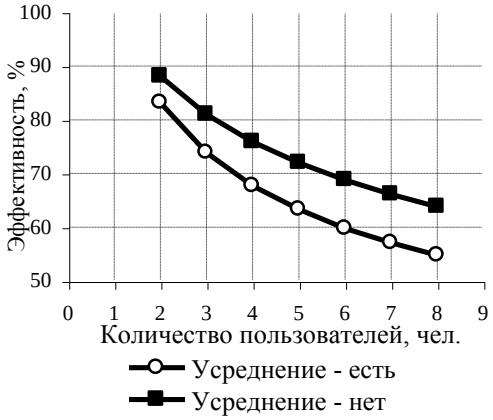

Рисунок 3 – Результаты второй группы экспримето в

- чем меньше процент ошибок при наборе текста, тем больше эффективность применения данного подхода;
- чем меньше амплитуда процента ошибок у пользователей между собой, тем больше эффективность применения данного подхода.

Все следующие эксперименты проводились для группы пользователей со средним количеством ошибок.

Далее исследовалось влияние усреднения учебных данных (по 10) на эффективность применения данной сети для решения задачи аутентификации. В случае, когда усреднение не производилось, эффективность была выше на 4 – 6%. На рис. 3. показано влияние усреднения учебных данных на эффективность работы вероятностной нейронной сети при решении задачи аутентификации пользователя компьютерной системы, при условии что признаков – 6, учеб. данных – 1500, процент ошибок - средний, отбор по словам – есть. Таким образом, можно сделать вывод, что количество учебных данных имеет большее влияние на результат, чем небольшое увеличение точности учебных данных.

Затем исследовалось влияния выполнения отбора по словам на эффективность применения данного подхода. Если отбор по словам не проводится, то почти во всех случаях эффективность выше на 1 – 3%, причем чем больше учебных данных, тем эта разница меньше. На рис. 4. показано влияние отбора по словам в учебных данных на эффективность работы вероятностной нейронной сети при решении задачи аутентификации пользователя компьютерной системы, при условии что признаков – 6, учебных данных – 1500, процент ошибок – средний, усреднение – есть. Поэтому можно сделать вывод, что лучше больше учебных данных, пусть даже с неточностями, чем проведение отбора по словам, т. к. без отбора по словам

“страдает” только первый признак, а количество учебных данных, при этом, в 10 раз больше.

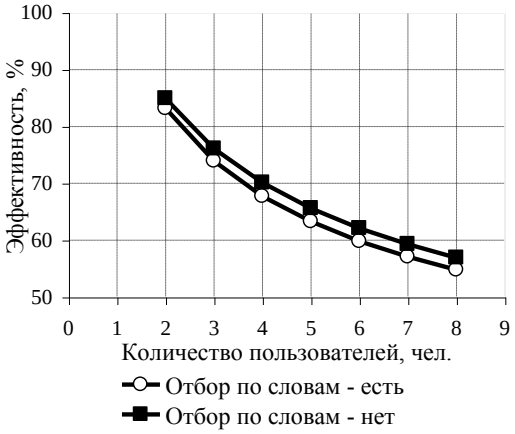

Рисунок 4 – Результаты третьей группы экспериментов

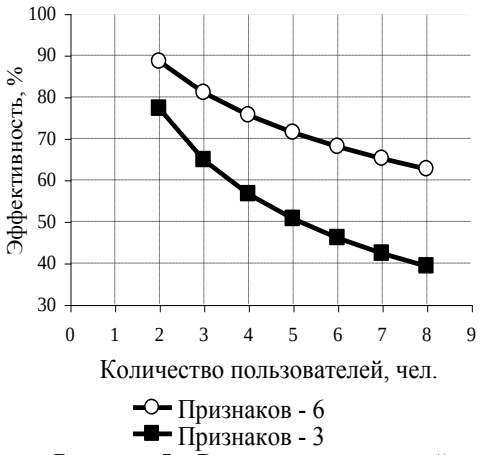

Рисунок 5 – Результаты четвертой группы экспериментов

Далее определялось влияние количества признаков на эффективность работы сети. Изменение количества признаков от 3 до 6 (рассматривалось время набора последних 6 букв либо последних или предпоследних 3 букв) увеличивало вероятность правильного ответа примерно на 10%, причем, чем больше пользователей в системе, тем больше улучшение результата. На рис. 5. показано влияние количества признаков на эффективность работы вероятностной нейронной сети при решении задачи аутентификации пользователя компьютерной системы, при условии что учебных данных – 1500, отбора по словам нет, процент ошибок – средний, усреднения нет. Отсюда можно сделать вывод, что чем больше признаков используется, тем эффективность больше.

В следующих опытах исследовалось влияние количества учебных данных на эффективность использования вероятностных нейронных сетей для решения выбранной задачи. Для этого эффективность считалась при условии, что используется 500, 1000, 1500 учебных данных. При этом между вторым и третьим вариантами эффективность отличатся незначительно, между первым и третьим, и первым и вторым эффективность отличается на 2 – 4%. На рис. 6. показано влияние количества учебных данных на эффективность работы вероятностной нейронной сети при решении задачи аутентификации пользователя компьютерной системы при условии, что признаков – 6, отбора по словам нет, процент ошибок – средний, усреднения нет. Отсюда можно сделать вывод, что чем больше учебных данных, тем эффективность выше. Сейчас проводятся эксперименты для большего количества учебных данных. Рассматриваются варианты, в которых используется от 2000 до 10000 учебных данных для каждого класса, т. е. 2, 3, 4, 5, 6, 7, 8, 9, 10 тысяч.

Кроме того, исследовалось влияние ширины функции активности на эффективность. Удачное изменение ширины функции активности увеличивало вероятность правильного ответа только на 1 – 2%. Можно сделать вывод, что этот параметр мало влияет на эффективность применения данного подхода. Поэтому во всех ранее рассмотренных экспериментах была выбрана ширина функции активности, равная 0.1. Сейчас проводятся эксперименты, в которых выбирается оптимальное значение ширины функции активности, т. е. с помощью перебора выбиралось значение данного параметра, при котором вероятность правильного ответа для каждой рассматриваемой комбинации пользователей наибольшая и при этом значении считалась результирующая эффективность. Диапазон рассматриваемых значений был выбран от 0.1 до 1.0 с шагом 0.01.

При проведении экспериментов возникли трудности, связанные во-первых с временными затратами, а во-вторых с повышенными требованиями к используемой вычислительной технике. Эти трудности объясняются, тем, что вероятностные нейронные сети весьма требовательны в отношении ресурсов.

Для накопления необходимого количества учебных данных требуется большие временные затраты. Так, если считать, что минимальное необходимое количество учебных данных – 1000 и использовать по 1000 экземпляров в качестве неизвестных образцов, то для накопления данных по одному пользователю системы необходимо примерно 4 – 5 часов, а если тестировать сеть при условии что в системе 20 пользователей, то необходимо 80 – 100 часов. Для уменьшения временных затрат администратора, который должен контролировать процесс накопления учебных данных, в программе предусмотрена

возможность накопления учебных данных на разных компьютерах, но при этом не снижаются временные затраты пользователей системы и затраты, связанные с использованием компьютеров.

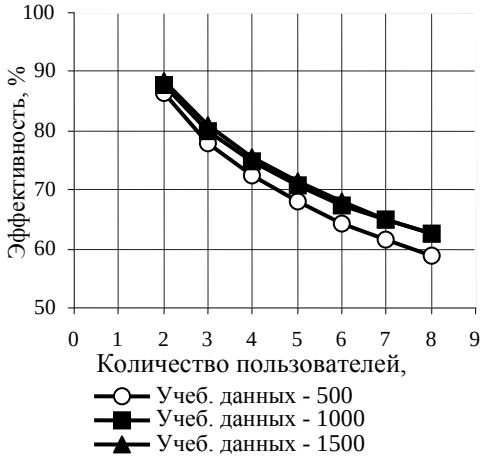

Рисунок 6 – Результаты пятой группы экспериментов

При анализе накопленной информации также возникают проблемы. Как уже было сказано, чем больше количество учебных образцов и количество признаков, тем эффективнее работает построенная сеть, но при этом увеличивается объем обрабатываемой информации, а следовательно увеличивается необходимое количество требуемой памяти и снижается быстродействие. Эти требования касаются оперативной памяти, емкости жесткого диска, частоты процессора. Например, файл свопинга занимал примерно 700 МБ. И это при том, что сама программа занимает относительно мало места. Весь инсталляционный пакет занимает примерно 8 МБ и в него входит сама инсталляционная программа с необходимыми dll-файлами и другими установочными файлами, кроме того, сюда входит необходимая база данных. Для работы программы необходимо наличие на компьютере Borland Database Engine; в случае отсутствия этого пакета его необходимо установить. Поэтому в инсталляционный пакет созданной программы входят файлы, необходимые для установки Borland Database Engine. Для инсталляции необходимо наличие на жестком диске примерно 27 МБ, из них для самой программы требуется 19 МБ, и для Borland Database Engine – 8 МБ. При накоплении большого количества учебных данных и при их анализе потребуется еще примерно 15 МБ на рабочем диске (кроме оговоренных раньше 700 МБ для файла свопинга).

При тестировании сети также возникают временные затраты. Так, например, если тестировать сеть для всех комбинаций по 5 пользователей из 8, при условии, что не проводится усреднение учебных данных и используется по 1000 учебных образцов для каждого класса, то один такой эксперимент занимает примерно 4 часа. А если проводить эксперименты, например, для всех комбинаций по 5 пользователей из 20, то время увеличивается до нескольких суток. Кроме того, при проведении экспериментов, в которых для расчетов выбирается оптимальное значение ширины функции активности, временные затраты увеличиваются как минимум в 20 раз.

Все эти эксперименты проводились на компьютере Pentium III – 500 с оперативной памятью – 192 МБ, на котором была установлена операционная система – Windows 98. Затем эксперименты были повторены на компьютере Athlon XP + 2000 с оперативной памятью 224 МБ, на котором была также была установлена операционная система – Windows 98. При этом время проведения каждого эксперимента уменьшилось примерно в 3–5 раз, благодаря чему удалось провести большее количество экспериментов.

В результате проведенного количественного и качественного анализа наиболее критичных параметров можно сделать вывод, что эффективность работы сети зависит от количества пользователей системы и от настройки наиболее критичных параметров.

По поводу критичных параметров можно сделать следующие выводы.

Для эффективности работы сети количество учебных данных важнее, чем их первичная обработка, т. е. лучше больше учебных данных пусть даже с небольшой погрешностью, чем более точные данные, но в меньшем количестве.

Ширина функции активности слабо влияет на качество аутентификации.

Увеличение количества анализируемых признаков достаточно сильно влияет на достоверность аутентификации.

Наибольшее влияние оказывает количество ошибок при наборе текста и, при этом, чем меньше амплитуда процента ошибок у пользователей между собой, тем больше эффективность применения

данного подхода. Т. е., чем внимательнее пользователи при наборе текста, тем больше эффективность, кроме того, желательно, чтобы уровень внимательности пользователей был примерно одинаковым.

Главными недостатками данного подхода являются временные затраты для накопления учебных данных и их обработки, а также повышенные требования к используемой вычислительной технике.

Эти недостатки являются основными проблемами при применении данного подхода для решения задачи аутентификации пользователей компьютерных систем, поэтому можно сказать, что решение этих проблем – это одна из задач, которую необходимо решать в дальнейшем.

Литература: ***1.*** *Высоцкая Е. А., Давиденко А. Н. Анализ алгоритмов реализации выборочной политики безопасности в автоматизированных системах. Сборник научных трудов Института проблем моделирования в энергетике НАН Украины. Вып. 16, Киев, 2002 г., с. 124-130.* ***2.*** *Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. 452 с., ил.* ***3.*** *Гундарь К. Ю, Гундарь А. Ю., Янишевский Д. А. Защита информации в компьютерных системах. – К.: "Корнейчук", 2000. – 152 с., ил.* ***4.*** *Каллан Р. Основные концепции нейронных сетей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2001. – 290с.* ***5.*** *Байдык Т. Н. Нейронные сети и задачи искусственного интеллекта. – К.: "Наукова думка", 2001. 265с.* ***6.*** *Архангельский В. И. и др. Нейронные сети в системах автоматизации. – К.: "Техника", 1999. – 364 с.* ***7.*** *neurnews.iu4.bmstu.ru/book/it/it898/stat1.htm/ Бондарев П. А. , Астафьев М. С. Распознавание отпечатков пальцев методами, использующими нейросети.* ***8.*** *nnet.chat.ru.nbp.html. Программа распознавания образов и прогноза.* ***9.*** *www.neuroproject.ru/index.htm/ Ward Systems Group, Inc. и компания НейроПроект* ***10.*** *www.neuroproject.ru/ Система определения настроения.* ***11.*** *www.neuroproject.ru/ Распознавание способа печати.* ***12.*** *Курош А. Г. Курс высшей алгебры. – М.: Государственное издательство физико-математической литературы, 1963. – 432с.*

УДК 681.3

МЕТОДИКИ ВИЗНАЧЕННЯ ВИХІДНИХ ДАНИХ ДЛЯ ОЦІНКИ ЗАЛИШКОВИХ РИЗИКІВ У ЛОМ

В'ячеслав Василенко, Микола Будько
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Пропонуються методики оцінки залишкових ризиків при забезпеченні конфіденційності, цілісності та доступності інформаційних об'єктів автоматизованих систем.**
Summary: **It is offered methods for the tasks of estimation of remaining risks at providing of confidentiality, integrity and availability of information's holding object of the automated systems.**
Ключові слова: **Інформація, конфіденційність, доступність, цілісність, вихідні дані.**

Вступ

Методики оцінки основних показників захищеності інформації в локальних обчислювальних мережах (ЛОМ) з достатньою глибиною розглянуті в [1, 2]. Але порядок визначення значень змінних (вихідних даних) у формульних виразах для оцінки величин відповідних залишкових ризиків в [1, 2] не наведено. У даній статті пропонуються підходи до їх визначення. Попередньо відзначимо, що чисельні значення змінних у наведених в [1, 2] виразах показників захищеності інформації [3 – 5] (ймовірностей порушення тієї чи іншої властивості захищеності інформації) можуть бути або розраховані (більшість з них), якщо відомі їх складові, чи закони розподілу відповідних ймовірностей, або визначені методом експертних оцінок. В останньому випадку ці показники потребують уточнення чи корегування службою захисту інформації відповідної організації, виходячи з досвіду експлуатації чи застосування системи захисту інформації ЛОМ, з наступною корекцією "Планів захисту інформації ЛОМ", заходів із захисту, складу та можливостей засобів захисту тощо.

У даній статті в більшості випадків розподіл імовірностей подій, пов'язаних зі спробами несанкціонованого доступу до інформаційних ресурсів, уважається рівномірним. Це пов'язано з тим, що, по–перше, такий закон розподілу є найскладнішим для функціонування систем захисту, а по друге, з відсутністю підстав для використання математичних апаратів інших законів розподілу. У разі можливості визначення параметрів потоків випадкових величин потрібні значення ймовірностей визначені з використанням відповідного математичного апарату.

Нижче, з урахуванням попередніх зауважень, викладені методики для практичного визначення вихідних даних для розрахунку показників захищеності інформації ЛОМ.