УДК 519+681

© 2008 г. **О.С. Амосов**, д-р техн. наук
(Амурский гуманитарно-педагогический государственный университет,
Комсомольск-на-Амуре),
Д.С. Магола
(Комсомольский-на-Амуре государственный технический университет)

МОДЕЛИ И АЛГОРИТМЫ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ И ВЕЙВЛЕТОВ

В статье рассматривается подход, позволяющий использовать искусственные нейронные сети и вейвлеты для идентификации пользователя корпоративной информационной системы.

Введение

Жизнедеятельность современной организации трудно представить без хорошо развитой корпоративной информационной системы (КИС), обеспечивающей постоянный обмен деловой информацией независимо от местонахождения пользователей. Искажение информации, необходимой для принятия ответственных решений, блокирование процесса ее получения от партнеров или сотрудников, внедрение в оборот ложной информации, разрушение имеющихся ресурсов могут нанести непоправимый урон деловой репутации фирмы, способствовать принятию ошибочных решений, приводящих к значительному материальному ущербу [1].

В настоящее время, как показывает обзор литературы [2 – 9] в области информационной безопасности, основное внимание уделяется методам противоборства с сетевыми атаками на КИС, использованию криптографии и обработке биометрических данных. Задача же идентификации пользователя КИС затронута лишь в небольшом перечне работ, – например, в [10, 11]. Один из способов обнаружения несанкционированных действий заключается в мониторинге необычной деятельности пользователя на основе данных его «почерка» при работе в КИС, поэтому задача идентификации пользователя КИС на сегодняшний день является актуальной.

В статье рассматриваются модели и алгоритмы идентификации пользователя КИС с применением нейронных сетей (НС) и вейвлетов.

Модели для идентификации пользователя КИС

Наряду с различными системами паролей, ограничением функций и доступа вашего терминала, которые могут быть преодолены злоумышленником, существует образ пользователя системы, воплощенный в средствах идентификации и аутентификации. Этот образ характеризуется «почерком», психологическими особенностями, общей стратегией работы, т.е. индивидуальными чертами, протестированными системой защиты. Она хранит образ и периодически сверяет с ним характер работы рабочей станции. Сигнал тревоги может возникнуть не только при смене пользователя, но и в случае, когда его поведение имеет серьезные отклонения от запечатленного образа. При этом могут применяться и тайные специфические сигналы, но ряд основных характеристик обязателен. Это частота ввода символов с клавиатуры, продолжительность пауз между словами, частота использования различных клавиш и т.д. [11].

Представим *формальную математическую модель пользователя КИС*, построенную на основе логики предикатов [12]. Пусть $\mathbf{p} = [p_1, p_2, \ldots, p_n]^T$ – вектор зарегистрированных пользователей КИС; $\mathbf{c}^j = [c^j_1, c^j_2, \ldots, c^j_m]^T$ – вектор параметров истинного «почерка» j-го пользователя КИС (эталонный вектор почерка j-го пользователя); $j = 1, 2,\ldots, n_1$; $\mathbf{c}^j = f(\mathbf{b}^j)$, где $\mathbf{b}^j$ – данные работы j-го пользователя в КИС, поступающие от сенсоров; $f(\mathbf{b}^j)$ – функция преобразования $\mathbf{b}^j$ в вектор $\mathbf{c}^j$; $\mathbf{cp}^k = [cp^k_1, cp^k_2, \ldots, cp^k_m]^T$ – вектор параметров «почерка» k-го потенциального пользователя КИС; $k = 1, 2,\ldots, n_2$; $\mathbf{r} = [r_1, r_2,\ldots, r_n]^T$ – вектор паролей (кодов) доступа пользователей $\mathbf{p}$; $\mathbf{a}$ – ложный «почерк»; n_1 – количество зарегистрированных пользователей КИС; n_2 – количество пользователей, желающих использовать КИС; m – количество параметров, определяющих «почерк» пользователя КИС. Тогда модель пользователя может быть выражена следующим образом:

$$\exists \mathbf{p} \wedge \exists \mathbf{c}(\mathbf{r}(\mathbf{c}) \wedge \neg(\mathbf{c} = \mathbf{a})). \qquad (1)$$

Под идентификацией пользователя КИС в данной работе будем понимать процесс сопоставления входного вектора $\mathbf{cp}^k$, полученного от возможного пользователя КИС, с эталонным вектором $\mathbf{c}^j$**.**

Постановка задачи идентификации пользователя КИС

Необходимо по вектору входных параметров потенциального пользователя $\mathbf{cp}^k$ определить его принадлежность данной КИС с использованием следующего критерия:

$$J = \frac{1}{n_1} \sum_{j=1}^{n_1} \left\| \mathbf{c}^j - \mathbf{cp}^k \right\|^2, \; k = 1, 2,\ldots, n_2. \qquad (2)$$

В общем случае (рис. 1) для получения доступа к определенным информационным ресурсам пользователь «предоставляет» системе свой «почерк», на основе которого, с использованием блока идентификации, аутентификации и авторизации, предоставляется или не предоставляется доступ к запрашиваемым ресурсам. Для идентификации пользователя КИС предлагается применять НС и вейвлеты.

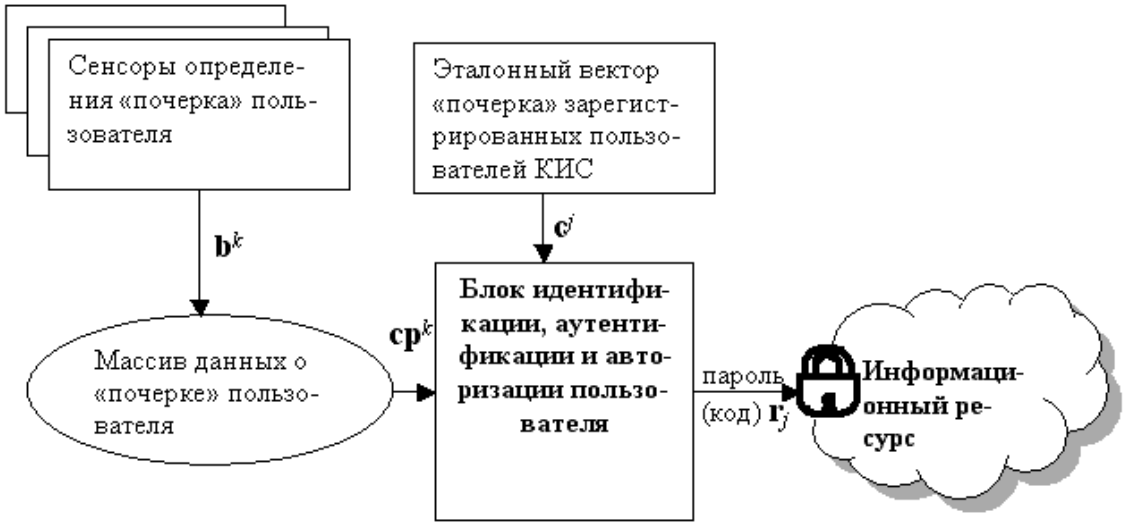

Рис. 1. Схема получения пароля (кода) доступа.

Использование нейронной сети для идентификации пользователя

В качестве блока идентификации, аутентификации и авторизации (см. рис. 1), предлагается использовать НС, обученную на N примерах образа «Друг». Эта НС, исходя из данных о «поведении» пользователя в сети, воспроизводит пароль или код доступа, принадлежащий образу «Друг», предоставляя, таким образом, доступ пользователю. В случае, когда «поведение» пользователя не соответствуют образу «Друг», НС воспроизводит «ложный» пароль, при вводе которого доступ не предоставляется.

В качестве одного из преимуществ предложенного подхода является гибкость, которую предоставляют НС. НС способна анализировать данные, даже если эти данные являются неполными или искаженными, обладает возможностью проводить анализ данных в нелинейном режиме. Поскольку защита вычислительных ресурсов требует своевременной (быстрой) идентификации атак, скорость обработки в НС может быть достаточной для реагирования в реальном времени на проводимые атаки до того, как в системе появятся непоправимые повреждения, что является еще одним преимуществом данного подхода. Это возможно за счет использования двух режимов работы НС: обучение НС (off-line) и работа НС в режиме реального времени (on-line).

Недостаток предложенного подхода связан с требованиями к обучению НС. Поскольку способность НС идентифицировать указания на атаку полностью зависит от точности обучения системы, обучающие данные и используемые методы обучения являются наиболее важными [9].

На основе проведенного анализа литературных источников [11, 13 – 17] и исходя из преимуществ и недостатков различных моделей НС, сделан вывод, что наибольшей эффективности при решения вышеописанной задачи можно достигнуть, используя НС радиально базисных функций (РБФ). НС с РБФ выполняют те же функции, что и сигмоидальные сети, однако реализуют иные методы обработки данных, связанные с локальными отображениями [17].

На рис. 2 представлена структурная схема НС с РБФ. Она содержит в наи-

более простой форме три слоя: обычный входной слой, выполняющий распределение данных образца для первого слоя весов; слой скрытых нейронов с радиально симметричной активационной функцией, каждый *j*-й из которых предназначен для хранения отдельного эталонного вектора в виде вектора весов $w_j^{(h)}$; выходной слой. Для построения сети РБФ необходимо выполнение следующих условий.

Во-первых, наличие эталонов, представленных в виде весовых векторов нейронов скрытого слоя. *Во-вторых*, наличие способа измерения расстояния входного вектора от эталона (стандартное евклидово расстояние). *В-третьих*, специальная функция активации нейронов скрытого слоя, задающая выбранный способ измерения расстояния. Обычно используется функция Гаусса, существенно усиливающая малую разницу между входным и эталонным векторами. Выходной сигнал эталонного нейрона скрытого слоя a_j– это функция (гауссиан) только от расстояния между входным вектором **x** и сохраненным центром $w_j^{(h)}$:

$$\rho_j = \sqrt{\sum_{i=1}^{n}(x_i - w_{ij}^{(h)})^2}\,, \tag{3}$$

$$a_j = g_j(\mathbf{x}) = \varphi\left(\frac{\left\|\mathbf{x} - \mathbf{w}_j^{(h)}\right\|}{\sigma_j}\right); \quad j = 1, ..., m_h, \tag{4}$$

где $c_j = z_j$ – активационный уровень нейрона j скрытого слоя; $\mathbf{x} = [x_1,\ldots, x_n]^T$ – входной вектор; $w_j^{(h)}=(w_{1j}^{(h)}\ldots w_{nj}^{(h)})^T$ – весовой вектор *j*-го эталонного нейрона скрытого слоя; y_j – параметр активационной функции; m_h – число эталонов-нейронов скрытого слоя.

Обучение слоя образцов-нейронов сети подразумевает предварительное проведение кластеризации для нахождения эталонных векторов и определенных эвристик для определения значений y_j.

Нейроны скрытого слоя соединены по полносвязной схеме с нейронами выходного слоя, которые осуществляют взвешенное суммирование:

$$y_i = \sum_{j=1}^{m_h} w_{ji}^{(o)} \varphi\left(\frac{\left\|\mathbf{x} - \mathbf{w}_j^{(h)}\right\|}{\sigma_j}\right),\ i = 1, ..., m_o\,, \tag{5}$$

где $w_j^{(h)}$ – центры; y_j – отклонения радиальных элементов.

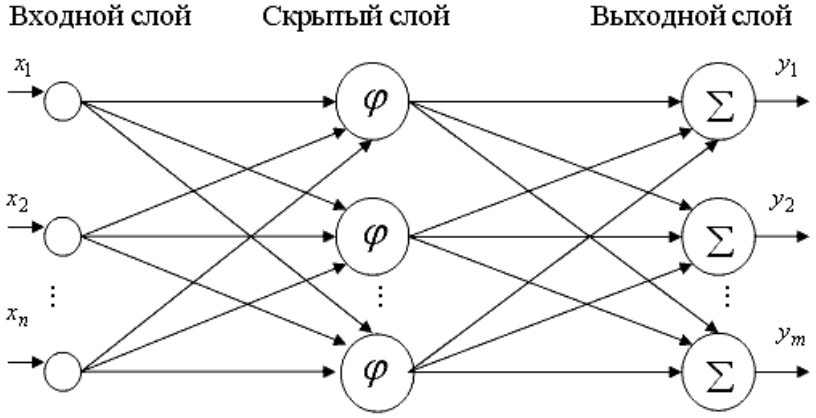

Рис. 2. Сеть с радиальными базисными функциями.

Для нахождения значения весов $w^{(o)}$ от нейронов скрытого к выходному слою используется линейная регрессия.

К недостаткам сетей РБФ можно отнести то, что заранее должно быть известно число эталонов, а также эвристики для построения активационных функций нейронов скрытого слоя [15].

Использование вейвлетов для идентификации пользователя КИС

Другим математическим инструментом, который предлагается использоваться в основе блока идентификации, является вейвлет-анализ.

Одна из основополагающих идей вейвлет-представления сигнала $v(t)$ заключается в разбивке приближения $s_j(t)$ к сигналу на две составляющие – грубую (аппроксимирующую) $s_{j-1}(t)$ и уточненную (детализирующую) $s^d_{j-1}(t)$, с последующим их уточнением итерационным методом:

$$s_j(t_i) = s_{j-1}(t_i) + s^d_{j-1}(t_i) = \sum_{k\in\mathbf{Z}} a_{j-1,k}\varphi_{j-1,k}(t_i) + \sum_{k\in\mathbf{Z}} d_{j-1,k}\psi_{j-1,k}(t_i), \qquad (6)$$

где число j характеризует уровень разрешения; $\varphi_{j-1,k}(t)$, $\psi_{j-1,k}(t)$ – масштабирующая (аппроксимирующая) функция и вейвлет-функция (детализирующая функция) соответственно; $\mathbf{a_1} = \{a_{j-1,k}\}$, $\mathbf{d_1}=\{d_{j-1,k}\}$ – наборы аппроксимирующих и детализирующих коэффициентов разложения (j-1) уровня разрешения; Z – множество целых чисел. Аппроксимирующие функции $\varphi(t)$ присущи далеко не всем вейвлетам, а только тем, которые относятся к ортогональным. Приближению $s_j(t_i)$ соответствует начальный набор коэффициентов $\mathbf{a_0} = \{a_{j,k}\}$. Обычно в качестве $\mathbf{a_0} = \{a_{j,k}\}$ выбирается массив значений сигнала $v(t)$, $a_{ji} = v(t_i)$.

Повторяя процедуру m раз, m=1, 2,.., M, разлагая каждый раз сглаженную функцию $s_{j-m}(t_i)$ на еще более сглаженную $s_{j-m-1}(t_i)$ и детализирующую $s^d_{j-m-1}(t_i)$ части, получаем вейвлет-разложение аппроксимации j-го уровня разрешения $s_j(t)$ для глубины разложения m:

$$s_j(t_i) = s_{j-m}(t_i) + s^d_{j-m}(t_i) + \ldots + s^d_{j-1}(t_i), \qquad (7)$$

$$s_j(t_i) = \sum_{k\in\mathbf{Z}} a_{j-m,k}\varphi_{j-m,k}(t_i) + \sum_{k\in\mathbf{Z}} d_{j-m,k}\psi_{j-m,k}(t_i) + \ldots + \sum_{k\in\mathbf{Z}} d_{j-1,k}\psi_{j-1,k}(t_i). \qquad (8)$$

Вейвлет-разложение можно изобразить в виде следующей схемы нахождения коэффициентов:

$$s_j(t_i) = \mathbf{a}_0 \to \{\mathbf{a}_1, \mathbf{d}_1\} \to \{\mathbf{a}_2, \mathbf{d}_2, \mathbf{d}_1\} \to \ldots \to \{\mathbf{a}_M, \mathbf{d}_M, \mathbf{d}_{M-1}, \ldots, \mathbf{d}_1\}. \qquad (9)$$

Идея использования вейвлет-преобразования для идентификации заключается в следующем: данные «почерка» пользователя представляем в виде сигнала, который, с использованием вейвлетов, раскладываем до заданного уровня разложения. Затем полученный массив аппроксимирующих коэффициентов желаемого уровня разложения преобразовываем в код доступа с использованием специального ключа и специального (например, криптографического) алгоритма (рис. 3).

Кроме того, вейвлет-преобразование предлагается использовать также и на этапе предобработки данных для решения задачи удаления шума. В связи с тем, что человек из-за своих особенностей может допускать отклонения от своего

обычного поведения, это может отразиться на его работе в системе, искажая его образцовый «почерк» пользователя. Другими словами, на «почерк» пользователя может накладываться шум или помехи. Сенсоры, снимающие данные о «почерке» пользователя, могут передавать информацию блоку идентификации пользователей также с шумом или помехами. Вейвлет-анализ является эффективным инструментом при решении задачи удаления шума.

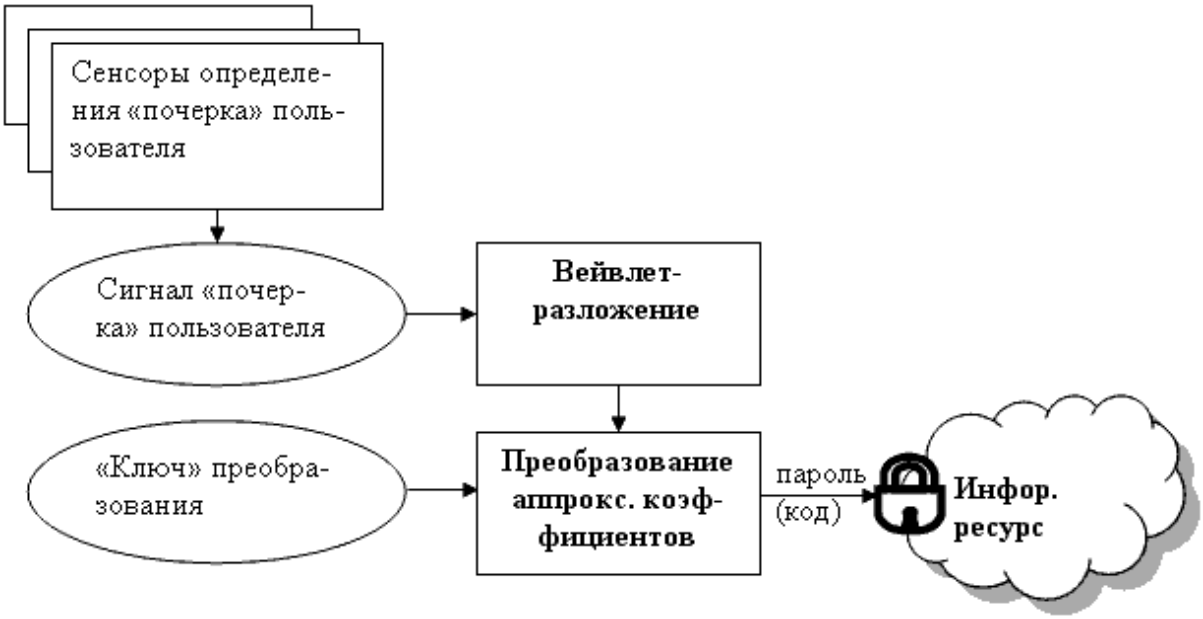

Рис. 3. Схема получения пароля доступа с использованием вейвлетов.

Шумовая компонента в большей степени отражается в детализирующих коэффициентах. Следовательно, при удалении шума необходимо обрабатывать в первую очередь эти коэффициенты. Предполагается, что шумовая компонента представляет собой сигнал, меньший по модулю, чем основной. Поэтому простейший способ удаления шума состоит в том, чтобы сделать нулевыми значения коэффициентов, меньшие некоторого порогового значения. Эта процедура называется пороговой обработкой (трешолдингом) коэффициентов. Широкое распространение получили такие методы пороговой обработки как жесткий трешолдинг и мягкий трешолдинг. В первом случае сохраняются неизменными все коэффициенты, большие или равные по абсолютной величине порога τ, а меньшие коэффициенты обращаются в нуль. При мягкой пороговой обработке, наряду с обращением в нуль коэффициентов, по модулю меньших, чем τ, происходит уменьшение по модулю остальных коэффициентов на величину τ [18 – 20].

В связи с этим изложенную схему получения пароля (кода) доступа (рис. 1) можно дополнить блоком очищения от шума или помех (рис. 4) с использованием вейвлетов.

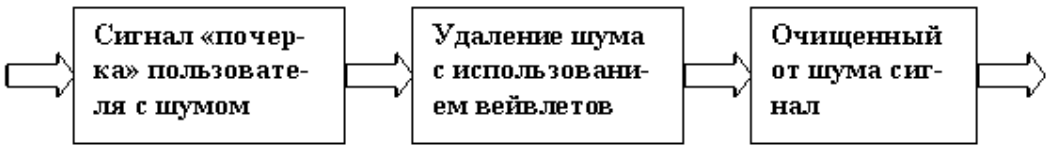

Рис. 4. Очищение сигнала от шума с использованием вейвлетов.

Обработка сигналов с использованием аппарата вейвлетов осложняется первоначальным выбором вида вейвлета. Кроме того, решение задачи шумоподавления осложняется первоначальным выбором типа пороговой обработки. От него зависит качество шумоподавления сигнала, оцениваемое в отношении сигнал/шум. В большинстве случаев определение происходит эмпирически. Для решения задачи определения вида вейвлета и выбора типа пороговой обработки предлагается использовать системы нечеткой логики, на основе знаний экспертов в области вейвлет-преобразования сигналов [19].

Пример использования нейронной сети для идентификации пользователя КИС

Предложенный подход с использованием НС (см. рис. 1) был исследован в среде MATLAB на следующем простом примере. В качестве параметров «почерка» пользователя рассматривались:

c_1 – частота ввода символов с клавиатуры (среднее значение вводимых пользователем символов за промежуток времени T_1);

c_2 – частота работы в заданных компьютерных программах (среднее процентное отношение времени работы пользователя в заданных компьютерных программах от общего времени, проводимого пользователем в корпоративной сети в течение времени T_2);

c_3 – коэффициент допущенных ошибок при вводе текста (процентное отношение введенных неверно слов от общего числа введенных слов за промежуток времени T_3);

c_4 – частота использования клавиши «Esc» (среднее количество нажатий клавиши «Esc» за промежуток времени T_4);

c_5 – частота использования клавиши «delete» (среднее количество нажатий клавиши «delete» за промежуток времени T_5);

c_6 – частота использования клавиши «insert» (среднее количество нажатий клавиши «insert» за промежуток времени T_6);

c_7 – частота отправки документов на печать (среднее количество отправленных на печать документов за время T_7);

c_8 – продолжительность пауз между словами при вводе текста (среднее количество времени, измеряемое в секундах, отсутствия активности пользователя при вводе текста, зафиксированных за промежуток времени T_8).

Обозначим через q количество замеров, произведенных системой, для определения параметров «почерка» пользователя. Тогда данные параметры можно определить следующим образом:

$$c_1 = \frac{1}{q}\sum_{i=1}^{q} S_i, \qquad (10)$$

где S_i – количество введенных символов за время T_1, зафиксированное при замере i;

$$c_2 = \frac{1}{q}\sum_{i=1}^{q} \frac{T_i^{np}}{T_i^{об}} \cdot 100\%, \qquad (11)$$

где $T_i^{пр}$ и $T_i^{об}$ – это время работы пользователя в заданных программах и общее время его работы пользователя в сети соответственно за промежуток времени T_2, зафиксированное при замере i;

$$c_3 = \frac{1}{q}\sum_{i=1}^{q}\frac{Sl_i^{нев}}{Sl_i^{об}}\cdot 100\%, \qquad (12)$$

где $Sl_i^{нев}$ и $Sl_i^{об}$ – количество неверно введенных слов и общее количество введенных слов за промежуток времени T_3, зафиксированное при замере i;

$$c_4 = \frac{1}{q}\sum_{i=1}^{q}Es_i, \qquad (13)$$

где Es_i – количество нажатий клавиши «Esc» за промежуток времени T_4, зафиксированное *i-м* замером;

$$c_5 = \frac{1}{q}\sum_{i=1}^{q}De_i, \qquad (14)$$

где De_i – количество нажатий клавиши «Delete» за промежуток времени T_5, зафиксированное i-м замером;

$$c_6 = \frac{1}{q}\sum_{i=1}^{q}In_i, \qquad (15)$$

где In_i – количество нажатий клавиши «Insert» за промежуток времени T_6, зафиксированное замером i;

$$c_7 = \frac{1}{q}\sum_{i=1}^{q}Ty_i, \qquad (16)$$

где Ty_i – количество отправленных на печать документов за промежуток времени T_7, зафиксированное i-м замером;

$$c_8 = \frac{1}{q}\sum_{i=1}^{q}\frac{T_8 - T_i^p}{Q_i^p}, \qquad (17)$$

где T_i^p –количество времени активных действий пользователя при наборе текста в период времени T_8; $Q_i{}^p$ – количество слов текста, набранных пользователем за время T_8, зафиксированное при замере i.

Таким образом, модель пользователя, идентифицирующую его по указанным параметрам, можно выразить как (1), где $\mathbf{c} = \{c_1, c_2, \ldots, c_8\}$.

Применение указанных восьми параметров объясняется их использованием для простого примера. В реальной системе количество параметров, которые должны идентифицировать пользователя по его работе в сети, может составлять несколько десятков.

Была создана НС с РБФ, на вход которой была подана матрица 8x100 (100 примеров «почерка» по 8 параметрам). В качестве эталонного массива для обучения «с учителем» была задана матрица 8x100, описывающая коды символов для паролей доступа. Рассмотрен случай, когда каждый пароль состоит из 8 символов. Получив на выходе НС коды символов, их легко интерпретировать в символьный пароль для доступа к информационному ресурсу. Некоторые данные матрицы входа и матрицы выхода нейронной сети представлены в табл. 1.

Таблица 1

Значения параметров «почерка» (матрица входов)	Коды символов паролей доступа (целевая матрица)	Символьное представление паролей доступа
43.5 50.5 54 49.5 55.5 54.5 50.5 24	87 101 108 99 111 109 101 48	Welcome0
38 55.5 55 50 55.5 55 25 26.5	76 111 110 100 111 110 50 53	London25
40 57 55.5 51.5 25 26.5 28 26	80 114 111 103 50 53 5 6 52	Prog2584

После обучения НС, в режиме *on-line* на ее вход были поданы значения параметров «почерка» трех пользователей, в результате получены значения кодов символов, которые округлили, используя правило округления. Результаты (входы и выходы нейронной сети) представлены в табл. 2.

Таблица 2

Значения параметров «почерка» (матрица входов)	Символьное представление паролей доступа
43.5 50.5 54 49.5 55.5 54.5 50.5 24	Welcome0
43.3 50.4 54 49.5 55.2 54.5 50 24	Welcomd0
98 50 54 54.5 54 54.5 51.5 24.2	]elmlmg0

Как видно из табл. 2, небольшое отклонение от «стандартного» поведения пользователя в сети закрывает доступ к секретным ресурсам корпоративной сети.

Следует отметить, что при использовании предложенного подхода необходима адаптация в процессе работы КИС, постоянное обучение НС и пополнение статистики в связи с возможным изменением штата пользователей КИС и (или) изменением их «почерка».

Пример использования вейвлетов для идентификации пользователя

Предложенный подход на основе вейвлетов (см. рис. 3) был исследован в среде MATLAB на следующем простом примере.

Рассматривалось 120 параметров «почерка» пользователя, включая и упомянутые в предыдущем пункте. Данные «почерка» пользователя были сведены в один одномерный сигнал. Использовалось разложение до 5-го уровня вейвлетом Добеши3 с использованием стандартных функций MATLAB:

```
v%сигнал
[C,L]=wavedec(v,5,'db3')% раскладываем сигнал v
ca5=appcoef(C,L,'db3',5)
```

В результате получили массив аппроксимирующих коэффициентов 5-го уровня разложения *ca5* = {383.8076, 376.2646, 369.9924, 406.2717, 426.0634, 425.1167, 445.2842}. В качестве ключа в примере рассматривался простейший ключ, который округлял элементы массива аппроксимирующих коэффициентов до целого числа. Далее в каждом числе массива он складывал значения всех разрядов, делил на наименьшее значение разряда, складывал с наибольшим значением разряда, а затем округлял до целого числа:

$$cR_i = round(ca5_i),$$

$$code_i = round\left(\frac{raz_1(cR_i) + raz_2(cR_i) + ... + raz_{\max}(cR_i)}{\min(raz_1(cR_i), raz_2(cR_i), ..., raz_{\max}(cR_i))} + \max(raz_1(cR_i), ..., raz_{\max}(cR_i))\right), \quad (18)$$

где $raz_1(cR_i)$ – значение 1-го разряда числа cR_i; $raz_{max}(cR_i)$ – значение максимального разряда числа cR_i; *round* – операция округления.

Таким образом, получили значение массива code = {13, 12, 10, 09, 12, 11, 08, 10}, который является истинным кодом доступа.

Заключение

Предложена формальная математическая модель пользователя корпоративной информационной системы на основе логики предикатов. Предложены модели и алгоритмы идентификации пользователей с применением нейронных сетей с радиально-базисными функциями и вейвлетов. Эффективность предложенных моделей подтверждена двумя примерами: с использованием нейронной сети с радиально-базисными функциями; с использованием вейвлетов.

ЛИТЕРАТУРА

1. *Кеннеди Дж.* Нейросетевые технологии в диагностике аномальной сетевой активности. / пер. с анг. – НИП «Информзащита», 1999. [www.citforum.ru].
2. *Левин М.* Криптография без секретов. – М.: Новый издательский дом, 2005.
3. *Зегжда П.Д.* Обеспечение безопасности информации в условиях создания единого информационного пространства // Защита информации. – 2007. – № 4. – С.28-33.
4. *Уланов В.А., Котенко И.В.* Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. – 2007. – № 2. – С.70-77.
5. Проверка правил политики безопасности для корпоративных компьютерных сетей /И.В. Котенко, А.В, Тишков, Е.В. Сидельникова, О.В. Черватюк // Защита информации. – 2007. – №6. – С.52-59.
6. *Громыко И.А.* Общая парадигма защиты информации // Защита информации. – 2008. – № 1. – С. 12-18.
7. *Петренко С.А., Беляев А.В.* Проблема обнаружения компьютерных атак в критически важных инфраструктурах // Защита информации. – 2008. – № 2. – С. 32-36.
8. *Иванов А.И.* Нейросетевое преодоление «проклятия» размерности, выход на «благодать» высокой размерности биометрических данных // Защита информации. – 2007. – № 5. – С. 50-56.
9. *Амосов О.С., Олейников Д.А.* Система диагностики и противодействия аномальной активности в компьютерных сетях на основе нечеткой логики и искусственных нейронных сетей // Тр. межрегион. науч.-практ. конф. “Роль науки, новой техники и технологий в экономическом развитии регионов”. – Хабаровск, 2001. – С.18-22.
10. *Райан Дж., Лин Менг-Джанг, Миккулайнен Р.* Обнаружение атак с помощью нейросетей. /пер. с англ. А.В. Лукацкого, Ю.Ю. Цаплева. – 2002. [http://neurnews.iu4.bmstu.ru/ book/security/inst.htm].
11. *Барский А.В.* Нейронные сети: распознавание, управление, принятие решений. – М.: Финансы и статистика, 2004.
12. *Маркин В.И.* Логика предикатов // Новая философская энциклопедия в 4-х т. – Т.2. – М.:

Мысль, 2000.
13. *Яхъяева Г.Э.* Нечеткие множества и нейронные сети. – М.: Бином, 2006.
14. *Комарцова Л.Г., Максимов А.В.* Нейрокомпьютеры. – М.: МГТУ, 2004.
15. *Круглов В.В., Борисов В.В.* Искусственные нейронные сети. Теория и практика. – М.: Горячая линия–Телеком, 2002.
16. *Каллан Р.* Основные концепции нейронных сетей. – М.: Вильямс, 2001.
17. *Осовский С.* Нейронные сети для обработки информации. – М.: Финансы и статистика, 2002.
18. *Смоленцев Н.К.* Основы теории вейвлетов. Вейвлеты в MATLAB. – М.: ДМК, 2005.
19. *Амосов О.С., Магола Д.С.* Применение нечеткого логического вывода при вейвлет-анализе сигналов // Тр. межрегион. науч.-практ. конф. “Информационные и коммуникационные технологии в образовании и научной деятельности” – Хабаровск, 2008. – С.238-246.
20. Вейвлет-анализ сигналов: Св. 2008610136 Российская Федерация, / Магола Д.С., Амосов О.С. – №2007614335; заявл. 02.11.07; опубл. 09.01.08.

Статья представлена к публикации членом редколлегии А.М. Шпилев.