УДК 519.687.4

С.Н. Кириллов, Л.С. Крупнов

СИСТЕМА ОБНАРУЖЕНИЯ И КЛАССИФИКАЦИИ СЕТЕВЫХ АТАК НА ОСНОВЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Рассматривается задача обнаружения и классификации сетевых атак (СА), воздействующих на распределенные компьютерные системы (КС). Обоснована возможность решения задачи с помощью искусственных нейронных сетей (ИНС). Обучение ИНС произведено с помощью математической модели безопасности Клементса – Хоффмана, дополненной алгоритмом формализации параметров КС. Результаты работы полученной системы обнаружения и классификации позволяют в автоматическом режиме оперативно реагировать на СА, что значительно снижает эффективность их воздействия на распределенные КС.

Ключевые слова: *искусственные нейронные сети, сетевые атаки, распознавание, классификация, защита.*

Введение. Для эффективного решения задач по защите информации в распределенной КС необходимо постоянно следить за состоянием объектов сетевой инфраструктуры, отслеживать наличие СА и оперативно применять меры по устранению возникающих неисправностей и угроз. Однако с ростом сложности защищаемых КС возрастает объем информации, который необходимо постоянно обрабатывать администратору службы безопасности для получения актуальной и объективной оценки состояния КС. Ключевым элементом здесь является возможность оперативного применения имеющихся механизмов защиты (МЗ) КС, что требует наличия эффективной системы обнаружения СА [1]. С другой стороны, для принятия решения о применении того или иного МЗ необходимо классифицировать обнаруженную угрозу, выявить ее источник и объекты воздействия. После решения перечисленных задач вопрос ликвидации угрозы, связанной с конкретной СА, сводится к применению соответствующих данному классу МЗ, согласно модели безопасности с полным перекрытием (модели Клементса – Хоффмана) [2].

Для эффективного решения поставленной задачи требуется произвести сужение области исследований [3]. Необходимость оперативного реагирования ограничивает перечень МЗ до класса программных воздействий на конфигурацию различных узлов КС. В качестве источников информации о СА при этом выступают выборки пакетов данных, которыми обмениваются устройства КС, а также журналы операционных систем, приложений и сервисов оконечного оборудования. Таким образом, реализация системы обнаружения и классификации (СОК) СА в описанной области исследований позволит оперативно реагировать на СА, что значительно снижает эффективность их воздействия на распределенную КС.

Цель работы – разработать и обосновать структуру СОК СА, а также протестировать ее работу на примере КС офиса малого предприятия.

Обоснование структуры СОК. Применяя системный подход, задача обнаружения и классификации разбивается на 3 этапа: обнаружение атаки, ее классификация и выявление характеристик атаки. Поскольку основная область поиска находится на уровне обмена пакетами данных, подавляющее количество информации об атаках исходит от снифферов сетевого трафика. Снифферами трафика выступают как программные модули на основе библиотек перехвата трафика WinPcap, расположенные на оконечном оборудовании, так и программно-аппаратные датчики, расположенные в наиболее важных участках КС. В качестве дополнительных источников данных также выступают сигнальные сообщения от сторонних инструментов защиты КС (антивирусы, спам-фильтры и т.п.).

Для решения задачи обнаружения факта присутствия СА предложено применение математической модели Клементса – Хоффмана [2], дополненной алгоритмом формализации параметров КС [4]. Предложенная дополненная модель позволяет получить универсальную оценку опасности СА, которая используется в качестве

индикатора присутствия СА. Также модель позволяет оценить риск от применения несоответствующего МЗ в случае ошибочной классификации СА или ложного срабатывания, либо от не применения МЗ вовсе, в случае пропуска СА.

Задача классификации СА не может быть решена аналитическим способом ввиду слабой формализации и высокой сложности взаимосвязей устройств современных КС. Это связано с появлением *качественно* новых свойств КС при одновременном изменении свойств ее отдельных компонент, что не сводится к простой сумме изменений этих компонент. В связи с этим предлагается задачу классификации СА решать с применением ИНС, предварительно обученной с помощью типовых атакующих воздействий на КС [5]. Поскольку классы атак известны заранее, в данном блоке применяется архитектура ИНС типа многослойный персептрон.

Задача восстановления полного вектора признаков атаки $\vec{Q}$ для дальнейшего поиска и устранения нарушителей безопасности является наиболее сложной. Из-за специфических особенностей атак, принадлежащих разным классам, выявление отдельных признаков атаки необходимо производить для каждого класса отдельно. Для решения поставленной задачи предлагается использовать рекуррентные сети Хопфилда [6]. Выбор подобной архитектуры обусловлен наличием у сетей Хопфилда свойств ассоциативной памяти, что позволяет запоминать, а потом восстанавливать даже при неполной входной информации различные векторы признаков сетевых атак $\vec{Q}$. Структурная схема СОК при этом имеет вид (рисунок 1):

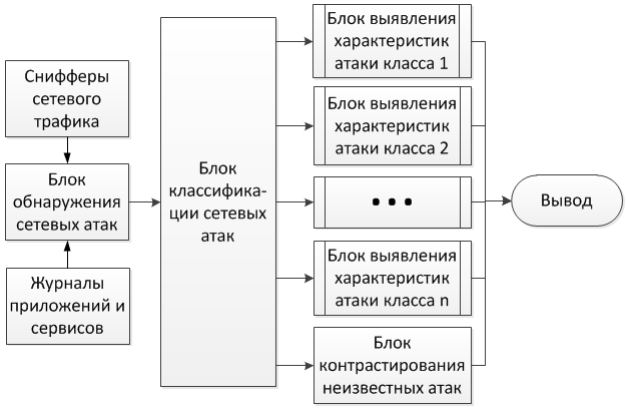

Рисунок 1 – Структура нейросетевой системы обнаружения и классификации СА

Теоретическая часть. Для выявления факта присутствия СА, а также для обоснования критериев оценки эффективности разрабатываемой СОК необходимо формализовать процесс защиты КС. Для этого используется математическая модель с полным перекрытием, в которой подразумевается, что для каждой угрозы $u \in U$ существует один или более механизм защиты $m \in M$, который снижает вероятность успешного проведения СА.

Для описания системы защиты информации в КС с полным перекрытием рассматривается пять множеств [7].

1. Множество угроз $U = \{u_i\}, i = \overline{1,m}$.
2. Множество объектов защиты $O = \{o_j\}, j = \overline{1,n}$.
3. Множество механизмов защиты $M = \{m_k\}, k = \overline{1,r}$.
4. Множество уязвимых мест *V*, определяемое подмножеством декартова произведения $U \times O$: $v_p = \langle u_i, o_j \rangle$.
5. Множество барьеров *B*, определяемое декартовым произведением $V \times M$: $b_q = \langle u_i, o_j, m_k \rangle$.

Таким образом, процесс защиты информации можно представить с помощью 5–мерного кортежа $S=\{O, U, M, V, B\}$. Система защиты с полным перекрытием должна предусматривать средства защиты на каждый возможный путь проникновения. В такой системе каждому уязвимому месту v_p соответствует барьер b_q (рисунок 2).

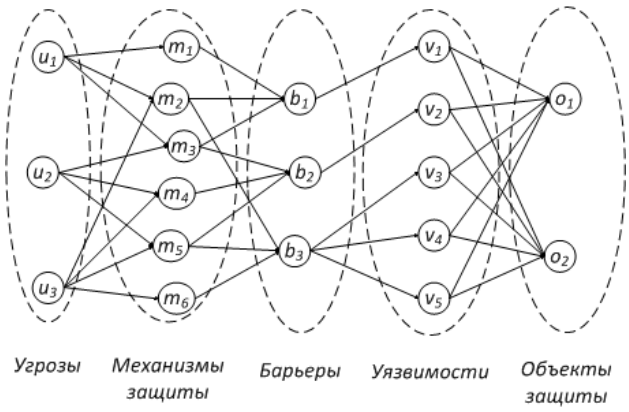

Рисунок 2 – Модель системы защиты информации с полным перекрытием

Величину защищенности всей системы при этом можно определить по формуле [7]

$$S = \frac{1}{\sum_{(\forall b_q \in B)} \left(P_i \cdot Q_j \cdot \left(1 - P_q\right)\right)}, \quad (1)$$
$$P_i, Q_j \in (0,1), P_q \in [0,1)$$

где P_i – вероятность появления угрозы y_i; Q_j – величина ущерба при удачном осуществлении угрозы y_i в отношении защищаемого объекта o_j; P_q – степень сопротивляемости барьера b_q, характеризующаяся вероятностью его преодоления. Знаменатель формулы (1) является суммой

рисков от воздействия множества угроз на КС.

Данная модель не учитывает зависимость работоспособности объектов защиты друг от друга, что, как правило, не имеет места на практике. Также для корректной оценки защищенности необходимо получить значение величины ущерба от угрозы Q_j. Для решения данных проблем можно использовать алгоритм оценки опасности различных сетевых атак на основе метода группового учета аргументов [4]. В качестве объектов защиты при этом выступают рабочие процессы R_i КС, а величина ущерба от угрозы получается из разности значений целевой функции состояния КС y:

$$y(r_1, r_2 ... r_n) = \sum_{i=1}^{n} a_i R_i , \quad (2)$$

$$R = a_0 x_1^{k_1} x_2^{k_2} ... x_m^{k_m} = a_0 \prod_{j=1}^{m} x_j^{k_j} , \quad (3)$$

$$Q_j = \sum_{i=1}^{n} a_i \left(\prod_{j=1}^{m} x_j^{k_j} - \prod_{j=1}^{m} (x + \Delta x)_j^{k_j} \right), \quad (4)$$

где x_i – показатели качества системы, Δx – изменения показателей качества системы при воздействии атаки, a_i, k_j – весовые коэффициенты полинома. Таким образом, показателем качества полученной СОК будет являться величина защищенности системы S, вычисленная по формуле (1), после применения соответствующих МЗ для выявленных в КС атак.

Данная математическая модель может использоваться для обнаружения факта присутствия СА. Поскольку одни и те же действия пользователей могут классифицироваться как безопасные, так и вредоносные, в зависимости от ситуации, это особенно актуально для внутренних атак от самих пользователей КС. Если в качестве индикатора присутствия СА использовать параметр S, то СА считается любая последовательность действий или событий, которая переводит КС из начального состояния S_0 в состояние S, если $S_0 - S > \Delta S$, где ΔS – порог чувствительности СОК.

Классификация сетевых атак. Каждую СА можно в общем случае разбить на 5 этапов (таблица 1) [8]. В реальной ситуации некоторые шаги могут быть пропущены.

Таблица 1 – Основные классы сетевых атак

Класс сетевой атаки	Описание класса
1. Исследование	Получение общей информации о КС
1.1 Социотехника	Получение информации посредством вежливого втирания в доверие по телефону, электронной почте и т.п.
1.2 Непосредственное вторжение	Получение информации посредством физического доступа к оборудованию сети
1.3 Разгребание мусора	Получение информации из мусорных корзин или архивов
1.4 Поиск в Web	Получение информации из интернета посредством общедоступных поисковых систем
1.5 Изучение WHOIS	Получение информации из регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем
1.6 Изучение DNS зон	Получение информации посредством использования сервиса доменных имен
2. Сканирование	Получение информации об инфраструктуре и внутреннем устройстве КС
2.1 Поиск активных устройств	Получение информации об активных устройствах КС
2.2 Трассировка маршрутов	Определение топологии КС
2.3 Сканирование портов	Получение информации об активных сервисах, функционирующих в КС
3. Получение доступа	Получение привилегированных прав на управление узлами КС
3.1 Переполнение стека	Выполнение произвольного кода в результате вызванного злоумышленником сбоя в программном обеспечении
3.2 Атака на пароли	Подбор паролей из списка стандартных или по специально сгенерированному словарю [9], перехват паролей
3.3 Атаки на Web-приложения	Получение доступа в результате эксплуатации уязвимостей в открытых web-приложениях КС
3.4 Снифинг	Получение доступа посредством пассивного (прослушивание) и активного (подмен адресатов) перехвата трафика КС
3.5 Перехват сеанса связи	Получение доступа вследствие перехвата авторизационных данных текущих сеансов пользователей КС

Окончание таблицы 1

4. Полезная нагрузка	Эксплуатация полученных прав для достижения целей взлома
4.1 Поддержание доступа	Установка систем удаленного администрирования
4.2 DOS – атаки	Вывод из строя устройств и отдельных сервисов КС
4.3 Обработка конфиденциальной информации	Перехват, копирование и/или уничтожение информации
5. Заметание следов	Сокрытие факта проникновения в КС от систем защиты
5.1 Стирание системных логов	Удаление данных архивов приложений и сервисов КС
5.2 Сокрытие признаков присутствия в сети	Туннелирование внутри стандартных протоколов (HTTP, ICMP, заголовков TCP и т.п.)

На основе данных таблицы 1 в задачу классификации входит разделение множества обнаруженных атак A на 5 классов либо отнесение атаки к неизвестному классу (что формально является шестым классом атак). Объектом исследования при этом являются показания датчиков, зафиксированные в период перехода системы из нормального состояния S_0 в состояние $S < S_0 - \Delta S$.

Для решения поставленной задачи предлагается применить нейронную сеть прямого распространения. Обучение сети при этом происходит с учителем на основе типовых атакующих воздействий. В состав ИНС входят базовые процессорные элементы (или нейроны), осуществляющие отображение вектора входных сигналов $\vec{R}^n \{r_1, r_2, \ldots, r_n\}$, поступающих с датчиков СОК, в выходной сигнал q, отражающий принадлежность обрабатываемого вектора $\vec{R}^n$ одному из описанных классов сетевой атаки [6]:

$$q = f\left(\sum_{j=1}^{n} w_j r_j + w_0 r_0\right) = f\left(\sum_{j=0}^{n} w_j r_j\right), \qquad (5)$$

где $w_0, w_1 \ldots w_n$ – весовые коэффициенты синаптических связей базового процессорного элемента (БПЭ), $f(s)$ – монотонная непрерывная функция активации. Схема БПЭ изображена на рисунке 3.

Согласно рекомендациям [7,8] ИНС имеет 3 слоя: входной, скрытый и выходной. Количество нейронов входного слоя зависит от количества датчиков исходной информации (по одному нейрону на каждый датчик), или количества признаков сетевой атаки. При этом количество нейронов скрытого слоя равно удвоенному количеству входных. Количество нейронов выходного слоя равно числу возможных решений, т.е. 6-ти для рассматриваемой задачи.

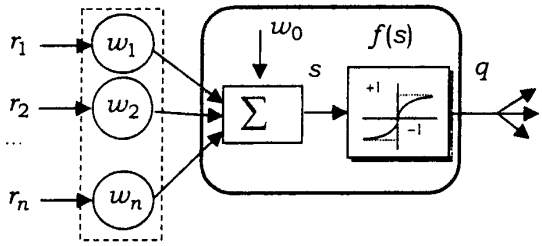

Рисунок 3 – Схема базового процессорного элемента

Основная сложность заключается в выборе критериев оптимизации ошибки обучения ИНС. Исходя из условий задачи классификации, используется критерий минимума средней функции риска разделения K классов входного сигнала на K_p классов решений при $K > K_p$ [10]. Риск определяется исходя из возможных потерь при ошибочной классификации, которые определяются матрицей коэффициентов потерь:

$$L = \begin{bmatrix} l_{11} & l_{12} & \ldots & l_{1K_p} \\ l_{21} & l_{22} & \ldots & l_{2K_p} \\ \ldots & \ldots & \ldots & \ldots \\ l_{K1} & l_{K2} & \ldots & l_{KK_p} \end{bmatrix},$$

где l_{ij} – коэффициент потерь при отнесении атак класса i к атакам класса j. Выражения для условных функций риска в данном случае имеют вид:

$$f_i = \sum_{k_p=1}^{K_p} \left(\int_{S^{K_p}(x)>0} l_{ik_p} f_i(x) dx \right), \qquad (6)$$

где $S^{k_p}(x) > 0$ – область многомерного пространства признаков атаки $\vec{X}$, соответствующей k_p-му классу. $f_i(x)$ – закон распределения пространства признаков атаки i-го класса. Интегральное выражение отражает условный риск от ошибочной классификации с учетом коэффициентов матрицы L.

Таким образом, оптимально обученной считается ИНС, минимизирующая значение средней функции риска [10]:

$$F = \sum_{k_p=1}^{K_p} \left(\int_{S^{K_p}(x)>0} \sum_{i=1}^{K} \left[l_{ik_p} f_i(x) \right] dx \right). \qquad (7)$$

Поскольку обучение ИНС происходит с учителем, функции $f_i(x)$ и области $S^{k_p}(x)$ можно оценить с помощью статистического анализа признаков типовых атакующих воздействий.

Предлагается коэффициенты матрицы L рассчитывать следующим образом:

$$l_{ij} = (S_i - S_j) / \sum_{i=1}^{K} \sum_{j=1}^{K_p} (S_i - S_j), \qquad (8)$$

где S_i и S_j – величины защищенности системы, полученные по формуле (1), рассчитанные при условии воздействия атаки i-го класса на КС, в которой применены МЗ i-го и j-го класса соответственно. Вычисление коэффициентов матрицы L по формуле (8) позволяет вносить динамические изменения в расстановку приоритетов защиты, что позволяет всей СОК адаптироваться к изменениям конфигурации или топологии КС, либо к смене режима функционирования КС.

В случае отнесения отдельной атаки к неизвестному классу управление передается на блок контрастирования, предназначенный для выявления основных признаков неизвестной сетевой атаки. В данном случае применение ИНС, обученных с учителем, нецелесообразно, поскольку характеристики подобных атак априори неизвестны. В данном блоке предлагается использовать ИНС Кохонена для кластер-анализа и классификации без учителя [5].

Основная задача сети – выделить среди множества неизвестных векторов признаков атак $\vec{R}^n$ ядра классов $\vec{c}_1 ... \vec{c}_k$, которые будут минимизировать величину близости неизвестной атаки $\vec{r}$ к определенному ядру класса $\vec{c}$. В качестве меры близости примем коэффициент корреляции между вектором признаков сетевой атаки $\vec{r}$ и вектором признаков ядра класса $\vec{c}$

$$d(\vec{r}, \vec{c}) = \sum_j \frac{(r_j - M_r)(c_j - M_c)}{\sigma_r \sigma_c},$$

где r_j, c_j – отдельные признаки сетевой атаки и ядра класса соответственно, $M_r = \frac{1}{n} \sum_j r_j$, (и аналогично M_c), n – размерность пространства признаков, $\sigma_r = \sqrt{\frac{1}{n} \sum_j (r_j - M_r)^2}$, (и аналогично для σ_c).

Полученные при этом векторы признаков $\vec{c}$ будут являться типичными представителями соответствующих классов атак, что значительно упрощает анализ неизвестных атакующих воздействий и сокращает время устранения возникшей угрозы администратором системы безопасности.

Этап выявления характеристик сетевой атаки. На данном этапе решается задача восстановления полного вектора признаков атаки $\vec{Q}$ из входного вектора $\vec{R}^n$ для дальнейшего поиска и устранения нарушителей безопасности. Эта задача решается с помощью рекуррентной сети Хопфилда [6]. Данная сеть состоит из одного слоя БПЭ, соединенных между собой обратными связями через элемент задержки $z^{-1} = e^{-\Delta t q_i}$, где Δt – период съема информации с датчиков СОК (рисунок 4).

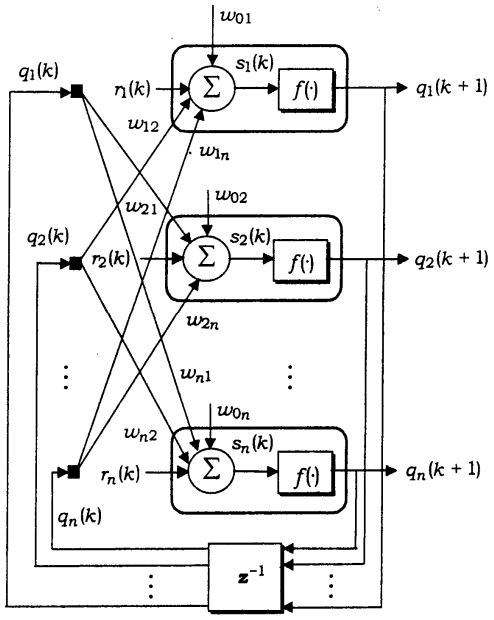

Рисунок 4 – Структура однослойной сети Хопфилда

В данном случае параметры выходного вектора $\vec{Q}$ вычисляются по формуле:

$$q_i = f\left(\sum_{j=1, j \neq i}^{n} w_{i,j} (q_j + r_i) - w_{0i} \right). \qquad (9)$$

Из-за наличия обратных связей возникает проблема сходимости последовательности $q_i(k) \overset{k \to \infty}{\to} q_i \in \{0,1\}$, которая может привести к появлению незатухающих обратных сигналов. Данная проблема решается с помощью выбора весовых коэффициентов $w_{ii} = 0$, $w_{ij} = w_{ji}$ [6]. Полученная ИНС обладает ограниченной емкостью и способна запомнить в среднем $0,1n$ различных векторов признаков $\vec{Q}$ внутри каждого класса атак. Данные сети крайне полезны в качестве универсального хранилища сигнатур СА, и используются для интерпретации причин срабатывания СОК.

Экспериментальная часть. Для проверки работоспособности СОК собран тестовый стенд, имитирующий работу тестовой КС малого офиса, в состав которого входит 12 устройств: корневой коммутатор, сервер базы данных (БД), рабочие места администратора системы и пользователей БД, вспомогательные устройства коммутации. Функционирование всей тестовой КС

разбивается на отдельные независимые рабочие процессы, которые в сумме составляют множество объектов защиты $O = \{o_j\}, j = \overline{1,n}$. После этого с помощью методики, приведенной в работе [4], производится оценка коэффициентов a_i, которые отражают относительную важность рабочего процесса для работы всей КС (таблица 2).

Таблица 2 – Рабочие процессы тестовой КС

Рабочий процесс	Задачи, решаемые в рамках рабочего процесса	a_i
Доступность БД	Обеспечение физического доступа к БД для пользователей КС	0,114
Учет пользователей БД	Строгая идентификация пользователей БД (на основе паролей, MAC-адресов и т.п.)	0,257
Проверка прав доступа пользователей БД	Реализация и контроль присвоения пользователям соответствующих прав на чтение, модификацию или удаление информации БД	0,286
Защита информации БД	Защита информации БД от несанкционированного уничтожения	0,201
Доступ в интернет	Обеспечение доступа пользователей в интернет	0,057
Мониторинг КС	Отслеживание состояния всех устройств КС, в том числе и для нужд СОК	0,052
Обеспечение принципа минимума привилегий	Присвоение пользователям КС только необходимых для работы прав доступа к оборудованию КС	0,032

При этом подразумевается, что КС функционирует нормально только при условии, что все рабочие процессы выполняются в штатном режиме. Любая СА, нарушающая нормальную работу КС, приведет к возникновению ущерба Q_j. Тестовый стенд подвергался воздействию 43 типов различных СА всех 5-ти классов (согласно таблице), на основе чего были получены средние значения ущерба Q_j для каждого класса (рисунок 5).

Полученные результаты говорят о том, что СА 1-го и 2-го классов практически не влияют на общую работоспособность КС, так как большинство из них реализуются с помощью разрешенных либо неконтролируемых в КС функций.

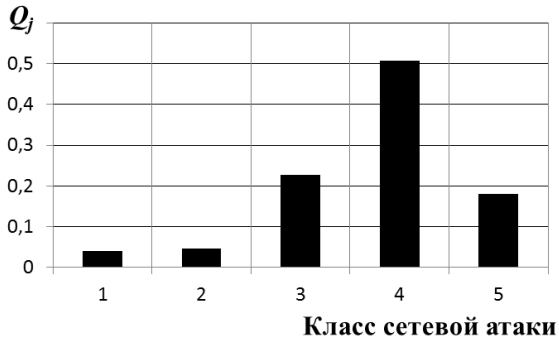

Рисунок 5 – Зависимость среднего значения ущерба Q_j от класса СА

С помощью программного пакета Statistica Neural Networks [11] создана и обучена ИНС типа многослойный персептрон для классификации СА. Обучение происходило на основе воздействия как простых СА, принадлежащих одному классу, так и комплексных, включающих СА всех пяти классов. Общее количество обучающих примеров достигло значения 17804 (60 % примеров для обучающей выборки, 20 % – для тестовой и 20 % для контрольной выборки). На рисунке 6 изображена гистограмма соотношения ошибок классификации в рамках каждого класса СА.

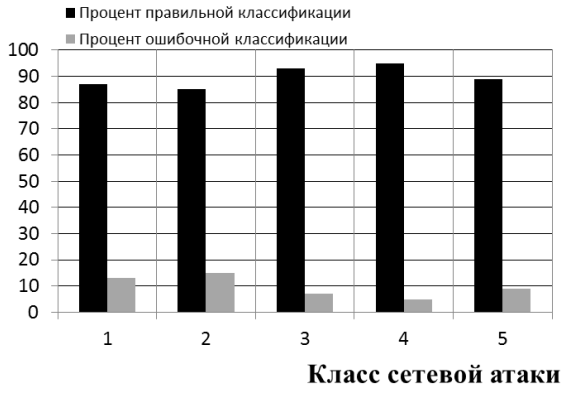

Рисунок 6 – Соотношение количества успешной и ошибочной классификации СА в рамках каждого класса

Большое количество ошибок классификации внутри 1-го и 2-го классов связано с тем, что угроза от реализации этих СА в общем случае минимальна. Это приводит к тому, что СОК, с учетом матрицы коэффициентов потерь L, чаще классифицирует СА 1-го и 2-го классов как более серьезные, нежели наоборот. Это, тем не менее, не приводит к опасному снижению итоговой защищенности КС S. С другой стороны, неверная классификация или пропуск СА 3-го или 4-го класса может привести к серьезным последствиям, что иллюстрирует рисунок 7.

Здесь под СА 6-го класса понимается отсутствие атаки, если речь идет о реальном классе

СА (ось *x*), либо пропуск атаки СОК, если речь идет об обнаруженной атаке (ось *z*).

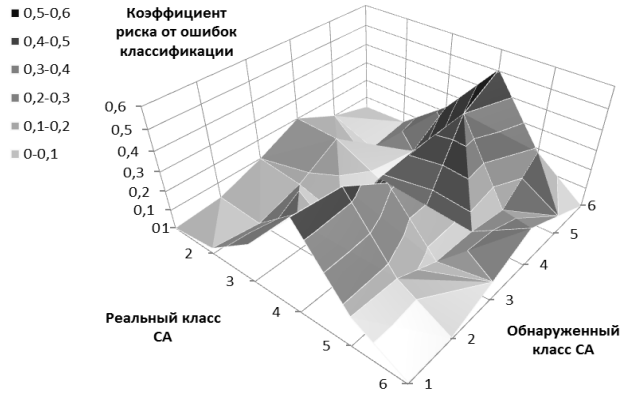

Рисунок 7 – Графическая иллюстрация матрицы коэффициентов потерь от ошибок классификации СА

Обучение ИНС Хопфилда, используемых в блоке выявления характеристик СА, произведено с помощью тех же обучающих примеров, дополненных информацией, которую невозможно получить от датчиков СОК. Среди этих характеристик указываются реальный источник СА, объекты воздействия, уровень привилегий атакующего, а также специфические для каждого класса СА параметры. Поскольку результат работы данного блока имеет вспомогательный характер, точность восстановления характеристик оценивается эмпирически. Результат работы блока выявил, что ИНС способна запомнить и восстановить сложные шаблоны СА своего класса, что при необходимости значительно упрощает поиск источников СА в автоматизированном режиме.

Заключение. Разработана и обоснована структура СОК СА, которая позволяет в автоматическом режиме обнаруживать и ликвидировать различные СА путем применения соответствующих классу СА МЗ. Обнаружение СА производится на основе имитационной модели КС, которая также позволяет оценить риски в случае неверной классификации или пропуске СА. Классификация и выявление характеристик СА производится с помощью ИНС, что дает возможность оперативно применять необходимые МЗ для известных СА, и структурирует информацию о неизвестных СА, что в значительной степени упрощает их анализ и ликвидацию в автоматизированном режиме. Работа СОК протестирована на стенде, имитирующем работу КС офиса малого предприятия. Результаты тестирования позволяют наглядно отобразить наиболее опасные классы СА для конкретной КС. Полученная точность распознавания СА, которая составляет от 85 % до 95 % в зависимости от класса СА, свидетельствует о возможности применять СОК в автоматическом режиме.

Библиографический список

1. *Лукацкий А.В.* Обнаружение атак. СПб.: БХВ – Перетбург, 2001. – 624 с.

2. *Хоффман, Л. Д.* Современные методы защиты информации / Л.Д. Хоффман; под ред. В.А. Герасименко. – М.: Сов. радио, 1980. – 264 с.

3. *Уотерман Д.* Руководство по экспертным системам / пер. с англ.; под ред. В.Л. Стефанюка. – М.: Мир, 1989. – 392 с.

4. *Крупнов Л.С.* Разработка алгоритма формализации параметров компьютерной системы для оценки опасности сетевых атак // Вестник Рязанского государственного радиотехнического университета. 2014. № 49. С. 67-72.

5. *Горбань А.Н.* Нейроинформатика. Новосибирск: Наука, 1998. – 296 с.

6. *Терехов В.А., Ефимов Д.В., Тюркин И.Ю., Антонов В.Н.* Нейросетевые системы управления. СПб.: Изд-во СПбУ, 1999. 265 с.

7. *Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.* Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса – Хоффмана. Брянск: БГТУ, 2007.

8. *Скудис Эд.* Противодействие хакерам, полное руководство по компьютерным атакам и эффективной защите / Пер. с англ. М.: ДМК-Пресс, 2003. 502 с.

9. *Кириллов С.Н., Крупнов Л.С.* Энтропия паролей как мера оценки стойкости к машинному перебору // Вестник Рязанского государственного радиотехнического университета. 2015. № 51. С. 60-66.

10. *Галушкин А.И.* Нейронные сети. Основы теории. Изд-во: Горячая линия-Телеком, 2010. - 496 с.

11. *Боровиков В.П.* Нейронные сети. Statistica Neural Networks. Методология и технологии современного анализа данных. М.: Горячая линия - Телеком, 2008. – 392 с.