5. *Петров А.П.* Экономическое стимулирование комплексного использования древесного сырья. – М.: Лесная пром-сть, 1980. – 104 с.
6. *Леоненков А.В.* Самоучитель UML. – СПб.: БХВ-Санкт-Петербург. 2001. – 304 с.
7. *Буч Г.* Язык UML. Руководство пользователя. – М.: Бином, 1999. – 560 с.
8. *Ефремова С.А.* Оптимизация использования производственных ресурсов лесопромышленных предприятий: дис. … канд. экон. наук. – СПб.: Изд-во ГЛТА, 1998. – 179 с.

УДК 004 (075.8)

И.Н. Кирко, В.П. Кушнир

ОПТИМИЗАЦИЯ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В РАМКАХ ПРОТОКОЛА IPSEC

Объединение обширной информации в рамках IPSec предоставляет возможность оптимально сформировать разные классы защиты.

Методы поисковой оптимизации открывают путь к построению и поддержанию на оптимальном уровне, на основе протокола IPSec, множества виртуальных сетей, различающимися своими параметрами.

***Ключевые слова**: протокол, оптимизация, политика, безопасность, переходная вероятность, симплекс.*

I.N. Kirko, V.P. Kushnir

SAFETY MECHANIZM OPTIMIZATION WITHIN THE FRAMES OF IPSEC PROTOCOL

Vast information gathering within the frames of IPSec gives the possibility to form various classes of safety in the optimal way. Search optimization methods open the door to formation and optimal maintenance on the basis of IPSec protocol of a lot of virtual nets, which differ in their parameters.

***Key words**: protocol, optimization, policy, safety, transition probability, simplex.*

Совокупность механизмов безопасности, предлагаемая в рамках протокола IPsec – это основа, на которой может строиться реализация виртуальных частных сетей, обеспечиваться защищенное взаимодействие мобильных систем с корпоративной сетью, защита прикладных потоков данных и т.п. Работа в рамках стандартов **IPsec** обеспечивает полную защиту информационного потока данных от отправителя до получателя.

Средства безопасности для **IP** описываются семейством спецификаций **IPsec**. Протоколы **IPsec** обеспечивают управление доступом, целостность вне соединения, аутентификацию источника данных, защиту от воспроизведения, конфиденциальность и защиту от анализа трафика.

Архитектура средств безопасности для IP-уровня – это, прежде всего, протоколы обеспечения аутентичности (протокол аутентифицирующего заголовка – **Authentication Header, AH**) и конфиденциальности (протокол инкапсулирующей защиты содержимого – **Encapsulating Security payload, ESp)**, а также механизмы управления криптографическими ключами. На более низком архитектурном уровне располагаются конкретные алгоритмы шифрования, контроля целостности и аутентичности. Наконец, роль фундамента выполняет домен интерпретации (**Domain of Interpretation, DOI**), являющийся базой данных, хранящей сведения об алгоритмах, их параметрах, протокольных идентификаторах и т.п. Для задания алгоритмов IPsec используется протокол ассоциаций (набор параметров) безопасности и управления ключами – **ISAKMP**.

Протоколы обеспечения аутентичности и конфиденциальности в **IPsec** не зависят от конкретных криптографических алгоритмов.

Алгоритмическая независимость протоколов требует предварительного согласования набора применяемых алгоритмов и их параметров, поддерживаемых общающимися сторонами, т.е. стороны должны выработать общий контекст безопасности (**Security Association, SA**) и затем использовать такие его элементы, как алгоритмы и их ключи. За формирование контекстов безопасности в **IPsec** отвечает особое семейство протоколов.

Системы, реализующие **IPsec**, должны поддерживать две базы данных:

- базу данных политики безопасности (**Security policy Database, SpD**);
- базу данных протокольных контекстов безопасности (**Security Association Database, SAD**).

Все IP-пакеты (входящие и исходящие) сопоставляются с упорядоченным набором правил политики безопасности. При сопоставлении используется фигурирующий в каждом правиле селектор – совокупность анализируемых полей сетевого уровня и более высоких протокольных уровней.

Системы, реализующие **IPsec**, функционируют как межсетевые экраны, фильтруя и преобразуя потоки данных на основе предварительно заданной политики безопасности [1].

Протокольный контекст безопасности в **IPsec** – это однонаправленное соединение (от источника к получателю), предоставляющее обслуживаемым потокам данных набор защитных сервисов в рамках одного протокола (**AH** или **ESp**). В случае симметричного взаимодействия партнерам придется организовать два контекста (по одному в каждом направлении). Если используются **AH** и **ESp**, потребуется четыре контекста.

Протокольный контекст создается на базе управляющего с использованием ключевого материала и средств аутентификации и шифрования последнего. Протокольные контексты являются средством проведения в жизнь политики безопасности. Политика безопасности должна быть задана для каждого сетевого интерфейса с задействованными средствами **IPsec** и для каждого направления потоков данных (входящие/исходящие). Согласно спецификациям **IPsec**, политика рассчитывается на бесконтекстную (независимую) обработку IP-пакетов.

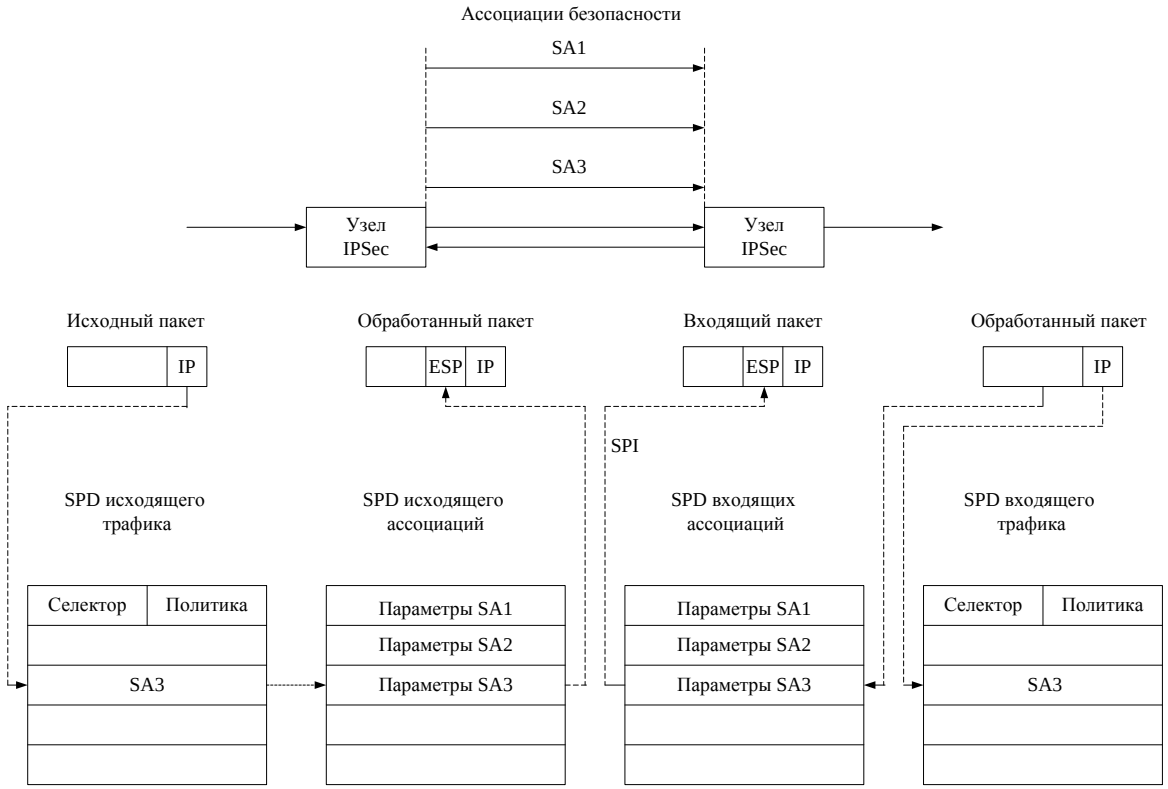

Рис. 1. Установление соответствия между IP-пакетами и правилами их обработки

База данных политики безопасности (SpD) представляет собой упорядоченный набор правил. Каждое правило задается как пара:

- совокупность селекторов;
- совокупность протокольных контекстов безопасности.

Селекторы служат для отбора пакетов, контексты задают требуемую обработку. Если правило ссылается на несуществующий контекст, оно должно содержать достаточную информацию для его (контекста) динамического создания. Очевидно, в этом случае требуется поддержка автоматического управления контекстами и ключами. В принципе функционирование системы может начинаться с задания базы **SpD** при пустой базе контекстов (**SAD**); последняя будет наполняться по мере необходимости.

Дифференцированность политики безопасности определяется селекторами, употребленными в правилах. Обработка исходящего и входящего трафика не является симметричной. Для исходящих пакетов

просматривается база **SpD**, находится подходящее правило, извлекаются ассоциированные с ним протокольные контексты и применяются соответствующие механизмы безопасности. Во входящих пакетах для каждого защитного протокола уже проставлено значение **SpI**, однозначно определяющее контекст. Просмотр базы **SpD** в таком случае не требуется; можно считать, что политика безопасности учитывалась при формировании соответствующего контекста.

Сложность процесса формирования механизмов безопасности приводит к большим затруднениям в выборе и поддержании оптимальных режимов работы в рамках протокола **IPsec**. Эти трудности обусловлены многообразием факторов, их сложной взаимозависимостью, наличием неконтролируемых возмущений.

Методы оптимизации могут быть различными в зависимости от конкретной формулировки задачи, объема и качества исходной информации, выбранных критериев оптимальности. Среди методов, получивших наибольшее распространение в промышленной оптимизации, достойное место занимает последовательный симплексный метод поиска и его модификации из-за их простоты и эффективности при поиске в сложных условиях.

Сущность симплексных методов состоит в том, что в *k*-мерном пространстве управляемых переменных x_i движение к оптимуму осуществляется последовательным отражением вершин симплекса. Симплекс представляет собой фигуру с *k*+1 вершинами, не принадлежащими ни одному пространству меньшей размерности. В случае *k*=1 – это прямая, при *k* =2 – треугольник, *k*=3 тетраэдр и т.д. Целевая функция вычисляется в каждой из вершин симплекса. При поиске максимума вершина с наименьшим значением целевой функции отбрасывается и строится новый симплекс. Направление последнего перемещения симплекса в факторном пространстве достаточно близко к направлению градиента линейного приближения целевой функции.

На разных этапах ставятся различные задачи оптимизации, например, для этапа восхождения – максимум математического ожидания смещения центра симплекса к цели, а на этапе доводки – достижение заданной точности. Характер оптимизации во время доводки обусловлен расстоянием до цели: при малых расстояниях симплекс в среднем удаляется от точки экстремума целевой функции, при больших – приближается к этой точке. Поэтому локальные характеристики процесса доводки зависят от расстояния до цели и для изучения движения симплекса, представляющего собой случайное блуждание в районе цели, применяются интегральные статистические характеристики поиска. Условное математическое ожидание смещение центра симплекса к цели зависит от соотношения расстояния ρ до цели и длины шага λ. Для каждого значения отношения полезного сигнала *A,* определяемого как произведение *L* |*grad Q*| *(L* – длина ребра симплекса) к среднеквадратичному отклонению помехи δ при заданных λ и *к* существует расстояние ρ =*R*, при котором *M*[λ /ρ] =0. Величина *R* называется радиусом стационарной орбиты, к которой в среднем тяготеет центр симплекса, блуждая вокруг цели. Радиусу *R* соответствует относительный радиус стационарной орбиты *S*=*R*/λ, позволяющий анализировать влияние параметров поиска на точность отыскания экстремума.

Локальная плотность распределения перехода центра симплекса любой ориентации из состояния ξ в состояние q представляется в виде [2]

$$fs\,(q|\xi) = \sum_{j=1}^{k+1} P_j\left(\frac{A_j(\xi)}{\sigma}\right)\,\delta\left[q-\left(\xi+\frac{g_j}{\lambda}\right)\right], \qquad (1)$$

где $P_j\left(\frac{A_j(\xi)}{\sigma}\right)$ – вероятность отражения *j*-й вершины; δ – дельта-функция; g_j – значение величины λ при отражении *j*-й вершины.

Каждый шаг поиска вблизи экстремума зависит как от ориентации симплекса, так и от расстояния его центра до цели. Состоянием системы $a, b_1, b_2, c_1, c_2, c_3, d_1\ldots$ соответствуют расстояния до цели $\rho_{a_1}, \rho_{b_1}, \rho_{b_2}, \rho_{c_1}, \rho_{c_2}, \rho_{c_3}, \rho_{d_1},\ldots$ (рис. 2). Относительному радиусу *S* стационарной орбиты *R* блуждания симплекса вокруг экстремума соответствует определенное минимальное количество шагов поиска достижения цели при условии, что длина ребра симплекса постоянная. Так состояния системы *a* соответствует 0–й орбите, состояния системы b_1, b_2 – 1–й орбите и т.д. Последовательность простых состояний $a, b_1, b_2,\ldots$ образуют сложные состояния системы при построении многосвязной марковской цепи. В [2] показано, что в результате синтеза структуры марковской цепи, описывающей процесс поиска на этапе доводки, оптимальным будет алгоритм со свободным отражением. Данный алгоритм является базовым для оптимизации переходных вероятностей при поиске с распознаванием состояний.

Оптимизация переходных вероятностей осуществляется введением в алгоритм симплексного поиска правила распознавания состояний.

$$z = \begin{cases} 1 \text{ при } (m_j \le k+2) \cap (y_n - y_{n-q} \ge 0); \\ 2 \text{ при } (m_j < k+2) \cap (y_n - y_{n-q} \ge 0); \\ 3 \text{ при } (m_j \le k+2) \cap (y_n - y_{n-q} < 0); \\ 4 \text{ при } (m_j > k+2) \cap (y_n - y_{n-q} < 0), \end{cases} \quad (2)$$

где m_j – число последовательных шагов поиска, в ходе которых вершина с номером *j* – не отражалась*; j=1,…,k+1*; y_n – значение измеряемой величины в вершине симплекса V_n; *q* – глубина предыстории.

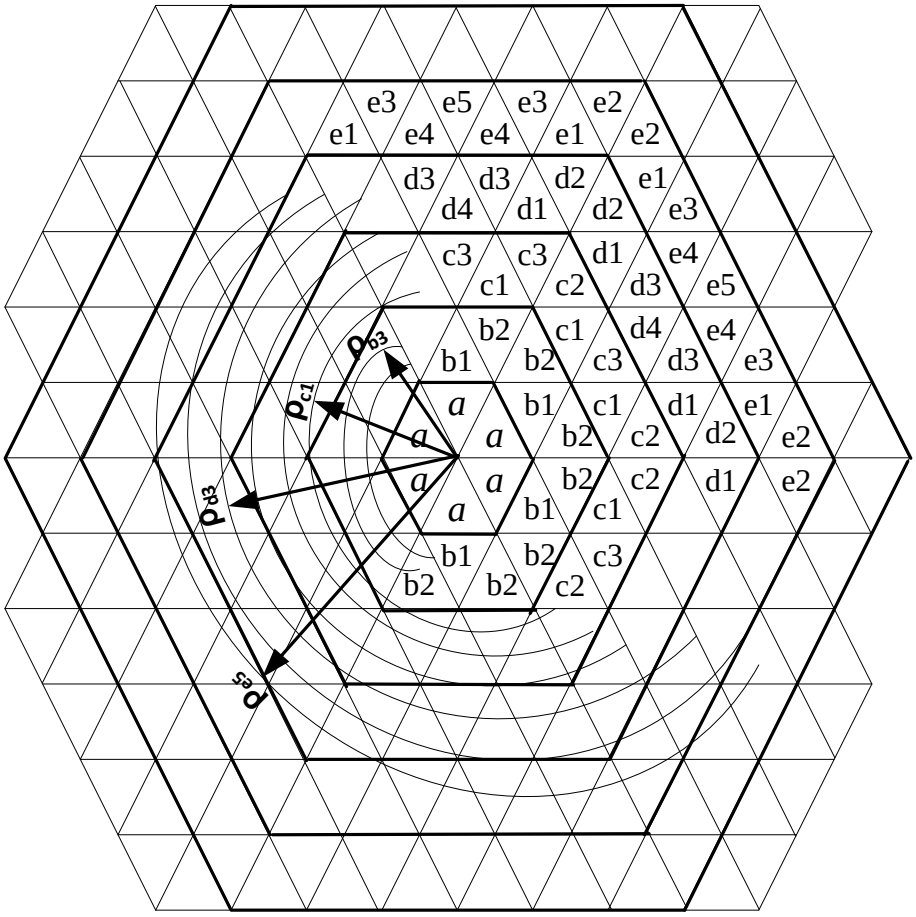

Рис. 2. Блуждание симплекса вблизи экстремума

Данное правило позволяет в случае удаления симплекса от цели исключить переходы, связывающие состояния марковской цепи (рис. 3) 2→6, 6→17, 17→27, 7→13, 13→18, 22→28, 30→24, 20→14, 14 → 8, 31→21, 21→9, 9→4 (т.е. P_{26} =0, $P_{6,17}$=0,…P_{94}=0).

Приведем основные правила алгоритма симплексного поиска с распознанием состояний, полученные в результате оптимизации переходных вероятностей стохастического графа, описывающего процесс блуждания симплекса вокруг экстремума.

1. Из всех вершин симплекса выбрать вершину V_r с наименьшим значением *y*.
2. Присвоить *m*=z.
3. Оценить состояние на данном шаге поиска согласно (2):
   а) если *z=1,4,* перейти к п. 4.
   б) если *z=2,3,* перейти к п. 7.
4. Отразить вершину с номером m относительно противоположной грани симплекса.
5. Определить значение $y_m^{(H)}$ во вновь полученной вершине.

6. Перейти к п. 1.
7. Из всех вершин симплекса, кроме V_r, выбрать вершину V_P с наименьшим значением у.
8. Присвоить *m=P*.
9. Перейти к п. 4.

Приведенные правила процесса поиска на этапе доводки назовем алгоритмом симплексного поиска с запретом прямолинейного движения.

При определении переходных вероятностей используется методика, рассмотренная в [2], однако в данном случае необходимо учитывать величину полезного сигнала в соответствии с ориентацией симплекса.

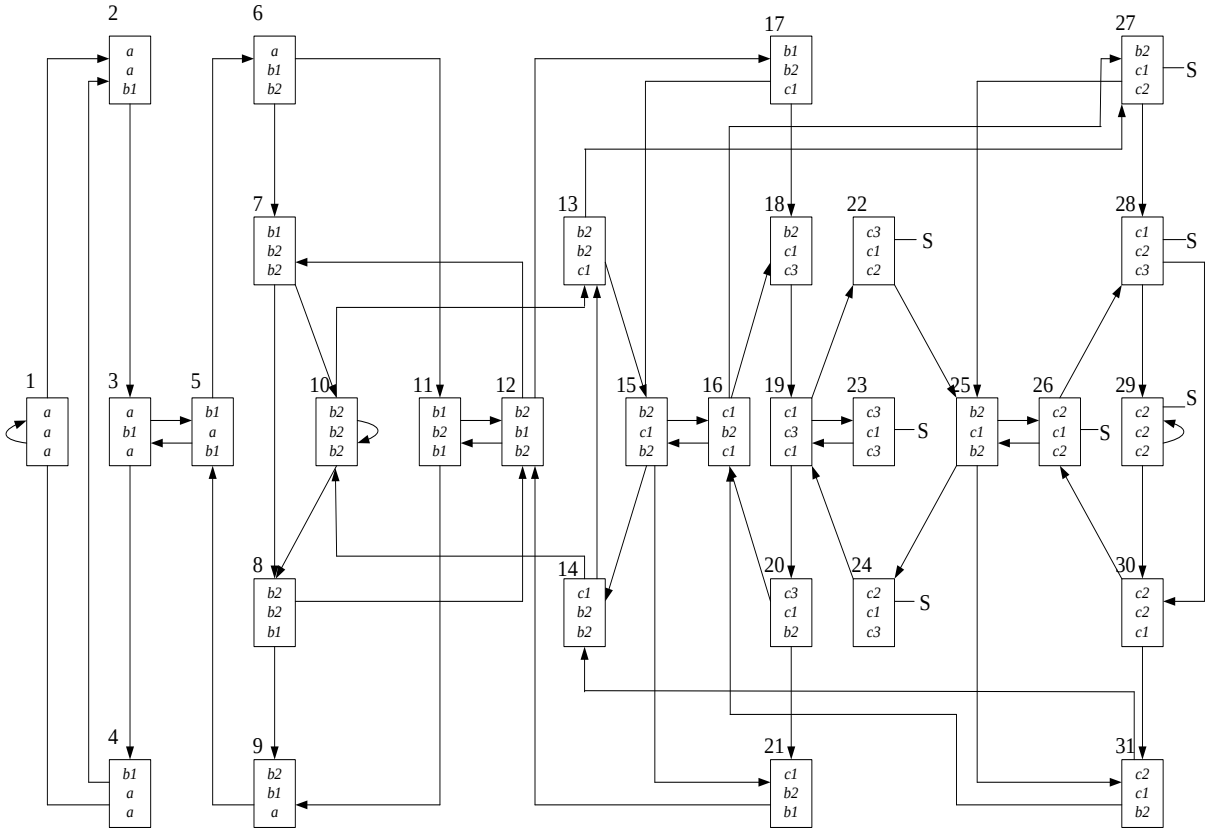

Рис. 3. Граф стохастического блуждания симплекса вокруг экстремума

Предельные вероятности простых состояний *a*, b_1, b_2, c_1, c_2, c_3 определяем путем суммирования вероятностей сложных состояний, имеющих одинаковые последние состояния:

$$\begin{gathered} P_a=P_1+P_3+P_4+P_9, \\ P_{b_1}=P_2+P_5+P_8+P_{11}+P_{21}, \\ P_{b_2}=P_6+P_7+P_{10}+P_{12}+P_{14}+P_{15}+P_{20}+P_{27}+P_{31}, \\ P_{c_1}=P_{13}+P_{16}+P_{17}+P_{19}+P_{25}+P_{30}, \\ P_{c_2}=P_{22}+P_{26}+P_{28}+P_{29}, \\ P_{c_3}=P_{18}+P_{23}+P_{24}. \end{gathered} \tag{3}$$

На основе вероятностей (3) получаем предельную плотность вероятности нахождения центра симплекса на орбите R:

$$f_s(\xi) = P_a\delta(\xi - \frac{\rho_a}{\lambda}) + P_b\delta(\xi - \frac{\rho_b}{\lambda}) + P_c\delta(\xi - \frac{\rho_c}{\lambda}), \tag{4}$$

где $P_b=P_{b_1}+P_{b_2}$, $P_c=P_{c_1}+P_{c_2}+P_{c_3}$,

$$\rho_b = \frac{\rho_{b_1}+\rho_{b_2}}{2}, \quad \rho_c = \frac{\rho_{c_1}+\rho_{c_2}+\rho_{c_3}}{3}.$$

Характеристика (4) позволяет оценить точность доводки, определить вероятность того, что в процессе случайного блуждания в районе цели симплекс не выйдет из заданной области.

Сопоставление зависимости плотности распределения *fs*(ξ) для алгоритмов со свободным отражением вершин, запретом возврата и запретом прямолинейного движения показывает, что применение алгоритма с запретом прямолинейного движения можно в 1,2÷1,3 раза повысить точность оптимизации, поддерживать оптимальный режим работы протокола IPsec в рамках заданной политики безопасности.

Литература

1. *Шаньгин В.Ф.* Защита компьютерной информации: учеб. – М.: ДМК Пресс, 2008. – С. 544.
2. *Дамбраускас А.П.* Симплексный поиск: учеб. – М., 1979. – С. 175.

УДК 57.025

В.А. Лоренц, В.Л. Гавриков, Р.Г. Хлебопрос

АНАЛИЗ ОБУЧЕНИЯ НЕЙРОННОЙ СЕТИ ЗАДАЧАМ, СОДЕРЖАЩИМ СКРЫТУЮ ЗАКОНОМЕРНОСТЬ

Анализируется динамика ошибок обучения нейронной сети в процессе решения задач, содержащих скрытую закономерность. Выявлено сходство обучения нейронной сети и способностей животных и человека.

***Ключевые слова**: нейронная сеть, обучение, ошибка, динамика, скрытая закономерность.*

V.A. Lorents, V.L. Gavrikov, R.G. Khlebopros

ANALYSIS OF THE NEURAL NETWORK TRAINING TO THE TASKS CONTAINING HIDDEN LAW

The dynamics of the neural network training error in the process of task solving which contain hidden law is analyzed. The similarity of neural network training and animal and human being abilities is revealed.

***Key words**: neural network, training, error, dynamics, hidden law.*

Введение. Область науки, специализирующаяся на разработке и исследовании нейронных сетей, развивается в настоящее время очень интенсивно, это обусловлено фундаментальным интересом во всем мире к созданию искусственного интеллекта, а также широким применением нейронных сетей для решения различных практических задач, связанным с уникальным свойством нейросетей решать задачи, не поддающиеся человеческим способностям.

То обстоятельство, что нейронная сеть является совокупностью простых элементов, взаимодействие которых порождает новые свойства, не присущие каждому ее элементу в отдельности, породило идею о потенциальной возможности сопоставления нейронных сетей с природными объектами. Предполагается, что нейросеть может выступать в роли универсального эвристического модельного объекта «живого» и использоваться для выявления общих зависимостей поведения системы от ее структуры и свойств ее компонентов [1].

Среди всех возможных функций, осуществляемых живыми организмами, одной из важнейших является их способность к обучению. Исследовать это эволюционно значимое качество живых систем можно разнообразными способами, и сравнительный подход, включающий параллельное рассмотрение естественных и искусственных адаптивных систем, представляется весьма плодотворным.

Количество публикаций в области исследования обучения живых систем чрезвычайно велико, так как данная тема находится на стыке многих научных дисциплин – нейрофизиологии, психологии, педагогики, математики, нейрокомпьютинга – и каждая из них претендует на особую значимость в сфере исследования