3. Лебедев О.Ю., Рыбников Д.Ю., Руденко А.В. Математическая модель движения судна для определения основных характеристик маневров в произвольном сносном потоке., научные исследования XXI века, 2020
4. Павленко В.Г., Бавин В.Ф. и др. Ходкость и управляемость судов. - Транспорт, 1991.- 400 с.
5. Смирнов Е.Л. Речная справочная книжка // URL: <https://russrivership.ru/ships> (дата обращения 10.11.2020)
6. Цурбан А.И. Определение маневренных элементов судна. – М.: Транспорт, 1977.
7. Экспериментальное и теоретическое определение маневренных элементов судов НМП для составления формуляров маневренных характеристик. Отчет о НИР УДК. 629.12.072/076. – Новороссийск, 1989.
8. Юдин Ю.И., Позняков С.И. Маневренные характеристики судна как функции параметров его математической модели. – Москва, изд МГТУ, 2006.

Курина А.Д.

Модель сертификации средств защиты информации от несанкционированного доступа

*Волгоградский Государственный Университет
(Россия, Волгоград)*

doi: 10.18411/lj-01-2021-07

idsp: ljjournal-01-2021-07

Аннотация

В статье представлена модель сертификации средств защиты информации от несанкционированного доступа. В результате сформулирована задача формализации и автоматизации процесса сертификации средств защиты информации от несанкционированного доступа.

Ключевые слова: техническая защита информации, безопасность, анализ, сертификация, угроза, несанкционированный доступ.

Abstract

The certification model for information protection against unauthorized access is presented in article. As a result, the task of formalizing and automating the process of certification of information security tools against unauthorized access is formulated.

Keywords: technical protection of information, security, analysis, certification, threat, unauthorized access.

Необходимость сертификации и создание систем сертификации заключается в реализации требований нормативно-правовых документов, в обеспечении безопасности, в создании условий качественного и эффективного производства. Обязательной сертификации подлежат средства защиты информации, предназначенные для защиты сведений, составляющих государственную тайну, а также другой информации с ограниченным доступом, подлежащей защите в соответствии с действующим законодательством, систем управления экологически опасными производствами, объектами, имеющими важное оборонное или экономическое значение и влияющими на безопасность государства, средства общего применения, предназначенные для противодействия техническим разведкам. Обязательной сертификации подлежат средства защиты информации, приведенные в Положении о системе сертификации средств защиты информации. В остальных случаях сертификация носит добровольный характер и осуществляется по инициативе заявителя средств защиты информации.

Для решения задачи формализации процесса сертификации средств защиты информации от несанкционированного доступа предлагается использовать многокритериальную оценку, основанную на количественной нормированной шкале. Сформируем вектор критериев

$$K = (K_1, K_2, K_3, K_4), \quad (1)$$

где K_1 – схема сертификации СЗИ

$$K_1 = \begin{cases} 1 & \text{– для единичных образцов СЗИ;} \\ 0,5 & \text{– для партии СЗИ;} \\ 0 & \text{– для серийного производства СЗИ.} \end{cases} \quad (2)$$

K_2 – классификация видов СЗИ от НСД

$$K_2 = \begin{cases} 0,2 & \text{– средства авторизации;} \\ 0,2 & \text{– мандатное управление доступом;} \\ 0,2 & \text{– избирательное управление доступом;} \\ 0,2 & \text{– управление доступом на основе ролей;} \\ 0,2 & \text{– протоколирование (аудит)} \end{cases} \quad (3)$$

K_3 – классы защищенности СЗИ

$$K_3 = \begin{cases} 0 & \text{– 4 группа (включает 7 класс);} \\ 0,5 & \text{– 3 группа (включает 6 и 5 классы);} \\ 0,2 & \text{– 2 группа (включает 4,3 и 2 классы);} \\ 1 & \text{– 1 группа (включает 1 класс)} \end{cases} \quad (4)$$

K_4 – основные угрозы НСД:

$$K_4 = \begin{cases} 0,3 & \text{– угрозы проникновения в ОС компьютера} \\ & \text{с использованием штатного ПО;} \\ 0,3 & \text{– угрозы создания нештатных режимов работы} \\ & \text{программных (программно – аппаратных) средств} \\ & \text{за счет преднамеренных изменений служебных данных;} \\ 0,3 & \text{– угрозы внедрения вредоносных программ.} \end{cases} \quad (5)$$

Значение критерия K_i представляет сумму оценок по частным групповым критериям K_{ij} и в своем максимальном значении не превышает единицу

$$K_i = \sum_{j=1}^m K_{ij} \leq 1 \quad (6), \text{ где } m - \text{число частных критериев в каждой группе. Существует}$$

наилучший вектор K^* , в котором все значения критериев соответствуют максимальным значениям. Для всех критериев это значение 1.

$$K^* = (1, 1, 1, 1) \quad (7).$$

Для оценки стоимости и необходимости сертификации СЗИ от НСД вводится скалярная величина равная Евклидову расстоянию между наилучшим вектором и вектором критериев, полученным для i -го оцениваемого признака: $K^i = (K_1^i, K_2^i, K_3^i, K_4^i)$ (8). Евклидово расстояние для i -го оцениваемого признака высчитывается по формуле: $P = \sqrt{\sum_{j=1}^4 (K_j^* - K_j^i)^2}$ (9). Числовые значения критериев, полученные при расчете, могут быть распределены по категориям для дальнейшего анализа и использования.

Для реализации выше определенной многокритериальной оценки и дальнейшей разработки программного комплекса модели рассмотрим следующую архитектуру модели сертификации средств защиты информации от несанкционированного доступа. Модель имеет графический вид и предназначена для ввода данных, вывода результатов и организации взаимодействия пользователя с программой (рисунок 1).

Рисунок 1 – Формализованная модель средства сертификации СЗИ от НСД

Разработанная модель может быть использована для автоматизации процедуры сертификации средств защиты информации от несанкционированного доступа.

1. Положение о системе сертификации средств защиты информации, утв. приказом ФСТЭК России от 3 апреля 2018 г. № 55 [Текст], введ. 2018-04-03. (Дата обращения: 05.10.2020).
2. Основы защиты от технических разведок (Меньшаков Ю.К. Москва, 2010). (Дата обращения: 01.12.2020)
3. Бабенко А. А., Козунова С. С. Модель оценки и прогнозирования рисков инвестирования информационной безопасности промышленных предприятий// Научный результат. Сер. Информационные технологии. - 2016. - Т.1, №4.-С. 29-35. - DOI: 10.18413/2518-1092-2016-1-4-29-35 (Babenko A.A., Kozunova S.S. Model of estimation and forecasting of risks of investment of information security of industrial enterprises // Scientific Result. Ser. Information Technologies. - 2016. - T.1, №4.-С. 29-35. - DOI: 10.18413/2518-1092-2016-1-4-29- 35). (Дата обращения: 05.01.2019).

Лавренков Ю.Н.

Формирование нейросетевых структур с самоподдерживающейся ритмической активностью с применением искусственного нейрогенеза

*Калужский филиал МГТУ им. Н.Э. Баумана
(Россия, Калуга)*

doi: 10.18411/lj-01-2021-08

idsp: ljjournal-01-2021-08

Аннотация

Рассмотрена процедура построения осцилляторной нейронной сети, формирование которой производится при помощи моделирования процесса нейрогенеза. Такой способ построения нейросетевого вычислителя приводит к генерации нейросетевых архитектур, способных поддерживать длительный процесс самоподдерживающейся ритмической активности.

Ключевые слова: осцилляторные нейронные сети, самоорганизация нейронных структур, алгоритм обучения, рециркуляционный контур памяти.

Abstract

The procedure for constructing an oscillatory neural network, the formation of which is carried out by modeling the process of neurogenesis, is considered. This method of constructing a neural network computer leads to the generation of neural network architectures capable of supporting a long-term process of self-sustaining rhythmic activity.

Keywords: oscillatory neural networks, self-organization of neural structures, learning algorithm, recirculating memory circuit.