DOI 10.37882/2223–2966.2020.11.35

МЕТОДИКА ИНТЕЛЛЕКТУАЛЬНОГО МНОГОАГЕНТНОГО УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фисун Владимир Владимирович
К.т.н., доцент, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
wfisun@gmail.com

Аннотация. Рассматриваются основные подходы к построению интеллектуальных методов и алгоритмов оценки и управления рисками информационной безопасности (ИБ) объектов критической информационной инфраструктуры информационно-телекоммуникационных систем (ИТКС КИИ) [1,2,3]. Анализируются требования по управлению рисками ИБ, определяемые как международными, так и отечественными стандартами. Проведённый анализ показал, что стандарты не определяют конкретные методы и алгоритмы управления рисками ИБ ИТКС КИИ. На основании проведённого анализа разрабатываются метод и алгоритм управления рисками ИБ ИТКС КИИ. Предложено построение подсистемы управления рисками ИБ на основе технологии распределённых интеллектуальных мультиагентов, основой которой является технология «агент-менеджер» [4]. Рассмотрены основные особенности применения данной технологии и её основные свойства. Показано, что неполнота, неопределённость и слабая структуризация исходных данных при анализе рисков ИБ ИТКС КИИ приводят к необходимости применения интеллектуальных методов управления, математической основой которых являются теория нечётких множеств и методы нечёткого вывода. Выполнен численный эксперимент на разработанной математической модели и приведены результаты её анализа. Показано, что применение предложенных методов при построении системы управления рисками ИБ ИТКС КИИ повышает оперативность и достоверность принятия управленческих решений и позволяет находить управленческие решения в области Парето-оптимальных решений. Предложенные решения приводят к существенному повышению устойчивости подсистемы ИБ ИТКС КИИ, а также существенному снижению объёма служебного трафика.

Ключевые слова: компьютерная атака, классификация, база знаний, экспертная система, неопределенность идентификатора, интеллектуальная система, управление информационной безопасностью, управление рисками информационной безопасности.

METHODS OF INTELLIGENT MULTI-AGENT INFORMATION SECURITY RISK MANAGEMENT

V. Fisun

Summary. The main approaches to the construction of intelligent methods and algorithms for assessing and managing information security risks of objects of critical information infrastructure of information and telecommunication systems are considered [1,2,3]. The requirements for information security risk management, determined by both international and domestic standards, are analyzed. The analysis showed that the standards do not define specific methods and algorithms for information security risk management of information infrastructure of information and telecommunication systems. Based on the analysis carried out, a method and algorithm for managing information security risks of information infrastructure of information and telecommunication systems are being developed. It is proposed to build an information security risk management subsystem based on the technology of distributed intelligent multiagents, which is based on the "agent-manager" technology [4]. The main features of the application of this technology and its main properties are considered. It is shown that the incompleteness, uncertainty and weak structuring of the initial data in the analysis of system risks lead to the need to use intelligent control methods, the mathematical basis of which is the theory of fuzzy sets and methods of fuzzy inference. A numerical experiment is performed on the developed mathematical model and the results of its analysis are presented. It is shown that the use of the proposed methods in the construction of a risk management system for information security of information infrastructure of information and telecommunication systems increases the efficiency and reliability of management decisions and makes it possible to find management decisions in the field of Pareto-optimal decisions. The proposed solutions lead to a significant increase in the stability of the information security subsystem of the information infrastructure of information and telecommunication systems, as well as to a significant decrease in the volume of service traffic.

Keywords: computer attack, classification, knowledge base, expert system, identification uncertainty, intelligent system, information security management, information security risk management.

Введение

В рамках концепции Государственной системы обнаружения и предупреждения компьютерных атак (КА) (ГосСОПКА) при формировании базы знаний КА, как многоагентной экспертной системы поддержки и принятия решений должностными лицами объектов критической информационной инфраструктуры (КИИ) и ситуационных ведомственных центров ГосСОПКА, предложено методику формирования сценариев управляющих решений по ситуации информационной безопасности (ИБ), дополнить интеллектуальными инструментами:

• методикой интеллектуального многоагентного управления рисками информационной безопасности объектов КИИ;

Это позволит перейти к решению задач синтеза управления ИБ как эффективной оперативно-технической государственной интеллектуальной системы, с учетом решаемых государственными регуляторами задач.

Методика интеллектуального мультиагентного управления рисками информационной безопасности

В настоящее время существуют как отечественные, так и международные стандарты управления рисками ИБ [9,10]. Однако эти стандарты не предоставляют какой-либо определенной методологии для осуществления управления рисками, связанных с информационной безопасностью, отсутствуют практические рекомендации по формированию режима безопасности и его поддержке в условиях меняющейся внешней среды и структуры самой ИТКС КИИ.

Первым этапом управления рисками ИБ ИТКС КИИ является этап их оценки, необходимый для обеспечения компромисса между степенью ИБ ИТКС КИИ и ее функциональными характеристиками.

Основные этапы анализа риска ИБ ИТКС КИИ можно сформулировать в следующем виде:

- этап идентификации активов ИТКС КИИ;
- этап анализа угроз ИБ ИТКС КИИ;
- этап оценки рисков;
- выбор и проверка защитных мер.

Учитывая разноплановость, многокритериальность, большую размерность решаемых задач по управлению рисками ИБ ИТКС КИИ, процедуру управления рисками ИБ ИТКС КИИ, а также процедуры их оценки предлагается строить на основе технологии интеллектуальных мультиагентов (ИМА), основой которых является технология «агент-менеджер» [5].

Особенностями интеллектуальных мультиагентных систем являются следующие их свойства:

1. *Адаптация.* Агенты системы адаптируются к сетевой архитектуре и адекватно отвечают на изменения в конфигурации сетевого оборудования.
2. *Рациональность распределения ресурсов.* Элементы ИМА равномерно распределены по всему периметру защиты ИТКС КИИ, что позволяет рационально (оптимально) распределить вычислительные ресурсы.
3. *Отказоустойчивость.* Подсистема защиты не имеет выделенного центра управления (центра принятий решений), так как агенты распределены по всей системе, следовательно, атаковать ИТКС КИИ сложнее, нежели сеть с централизованным сервером защиты. Распределенная по сети информация и распределенная защита требуют от злоумышленника проводить атаку многих узлов одновременно.
4. *Возможность централизованного управления.* Внесение изменений в работу агентов могут производиться централизованно и по протоколам взаимодействия агентов передаваться на все точки обеспечения безопасности.

Основным функциональным назначением ИМА оценки риска является:

- интеллектуальный анализ системного и прикладного программного обеспечения ИТКС КИИ на предмет наличия аномалий;
- интеллектуальный анализ аномалий входящего трафика ИТКС;
- обнаружение и предотвращение вторжений;
- интегральная оценка риска ИТКС КИИ;
- информирование вышестоящего элемента управления о степени риска ИБ;
- выработка и принятие решения по минимизации риска ИБ ИТКС;
- обмен информацией о своем состоянии с другими ИМА ИТКС КИИ.

Структура системы нечеткого вывода

Система нечеткого вывода в своей структуре содержит следующие основные функциональные модули (Рисунок 1) [6]:

- *модуль кластеризации и ранжирования* — функциональный модуль, на который информация мониторинга с сетевых сенсоров поступает для анализа. Этот модуль выполняет процедуры кластеризации рисков угроз по заданным метрикам (признакам), выполняет функцию классификации рисков, а также производит их ранжирование;

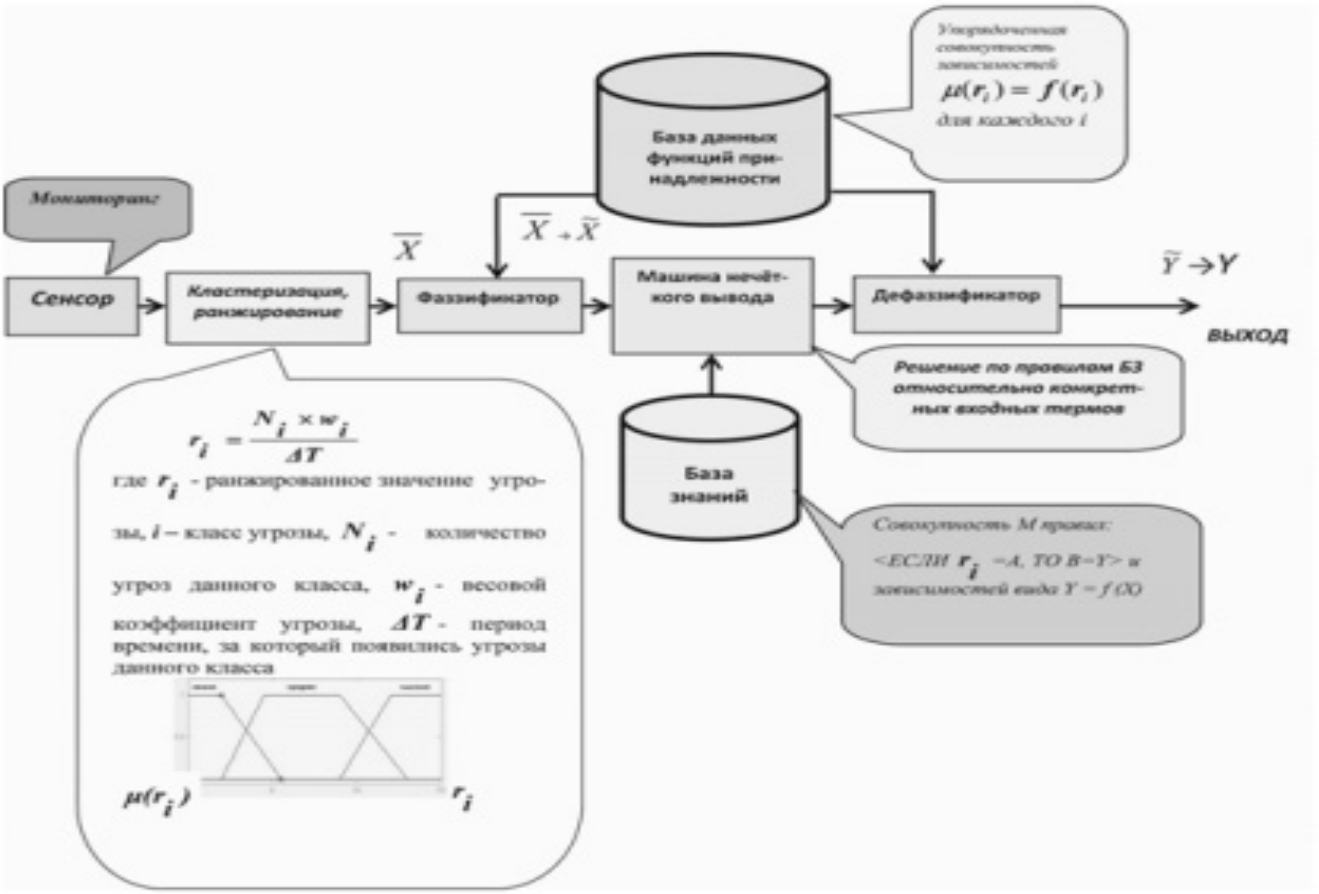

Рис. 1. Функциональная схема интеллектуального агента в части принятия решений по оценке риска ИБ

- *фаззификатор* — функциональный модуль, преобразующий фиксированный вектор влияющих факторов ***(X)*** *в* вектор нечетких множеств ***X***, которые необходимы для нечеткого вывода;
- *нечеткая база знаний* — функциональный модуль, заданный в виде совокупности нечетких правил и содержащий информацию о зависимости $Y = f(X)$ в виде лингвистических правил;
- *машина нечеткого логического вывода* — функциональный модуль, который на основе правил базы знаний определяет значение выходной переменной в виде нечеткого множества **Y**, соответствующего нечетким знаниям входных переменных (**X**)′,
- *дефаззификатор* — функциональный модуль, преобразующий выходное нечеткое множество **Y** в четкое число **У**.

Реализация метода

Интеллектуальные функции ИМА предлагается реализовать на основе аппроксимации зависимостей «входы — выход», построенных на основе логических высказываний [5]:

$$<ЕСЛИ\ A \Rightarrow B,\ ТО\ C \Rightarrow D>. \quad (1)$$

Лингвистические входные переменные задаются в виде:

$$\langle \mathrm{x}, \mathrm{T}, \mathbf{U}, \mathbf{G}, \mathrm{M} \rangle \quad (2)$$

где **x** — имя переменной; T — терм-множество, каждый элемент которого задается нечетким множеством на универсальном множестве U;

G — синтаксические правила, порождающие функции принадлежности (ФП) названия термов; M — семантические правила, задающие функции принадлежности нечетких термов, порожденных синтаксическими правилами из **G**. Нечеткий логический вывод предлагается проводить на основе метода Мамдани [7,8], который выполняется по базе знаний, имеющей вид:

$$(x_1 = a_{1j}\theta j x_2 = a_{2j}\theta j \ \ldots\ \theta j x_n = a_{nj})\ \mathbf{x}$$
$$w_j \Rightarrow y_j = d_j j = 1,\ m. \quad (3)$$

где a_{ij} — нечеткий терм, которым оценивается переменная x_i, в j-ом правиле базы знаний, d_j — заключение

j-ого правила, m — количество правил в базе знаний, $\Rightarrow$ — операция нечеткой импликации, w_j $(0 \le |w_j| \le 1)$ — весовые коэффициенты для каждого j-ого правила базы знаний, θ — логическая операция, связывающая посылки в j-ом правиле базы знаний.

В выражении (3) все значения входных и выходных переменных заданы нечеткими множествами. Предположим:

$\mu_j(x_i)$ — функция принадлежности входа $x_i \in [x_i, x^i]$, соответствующая нечеткому терму a_{ij};

$\mu_{dj}(y)$ — функция принадлежности выхода $y_j \in [y_j, y^j]$ для нечеткого терма d_{ij}.

Тогда степень выполнения $\boldsymbol{j}$ — го правила для текущего конкретного входного вектора определяется как:

$$\mu_j(X^*) = (\mu_j(x^*_1)\ \gamma_j \mu_j(x^*_2)\ \gamma_j \ldots\ \gamma_j \mu_j(x^*_n)) \ \mathbf{x}\ w_j,\ j=1,\ m. \quad (4)$$

где оператор γ_j определяется следующим образом:

$$\gamma_j = \begin{cases} \boldsymbol{t} - \text{норма, если } \boldsymbol{\gamma j} = <\text{И}>, \\ \boldsymbol{s} - \text{норма, если } \boldsymbol{\gamma j} = <\text{ИЛИ}> \end{cases} \quad (5)$$

Результат нечеткого вывода можно представить как

$$\boldsymbol{y^*} = \left\{ \frac{\boldsymbol{\mu 1}(x*)}{\boldsymbol{d1}}, \frac{\boldsymbol{\mu 2}(x*)}{\boldsymbol{d2}}, \ldots, \frac{\boldsymbol{\mu m}(x*)}{\boldsymbol{dm}} \right\} \quad (6)$$

Носителем нечеткого множества (5.7) является множество нечетких термов $\{d_1, d_2, \ldots, d_m\}$. Для перехода к нечеткому множеству, заданном на носителе $[y_i\, y^i]$, выполняются операции импликации и агрегирования [6].

В результате выполнения операции дефаззификации нечеткого множества y^m, которую можно провести, например, с помощью метода определения центра тяжести [6], получается четкое значение выхода y^i.

Экспериментальная оценка метода

В процессе математического моделирования оценивались следующие риски ИБ ИТКС [5]:

1) аномалии общесистемного и специального программного обеспечения (ОПО и СПО);
2) анализ аномалий входящего и исходящего сетевого графика;
3) обнаружения вторжений.

Кроме этого, производится интегральная оценка рисков ИБ сетевых элементов (СЭ) ИТКС. На каждый анализатор с сенсоров поступает входная информация в виде лингвистических переменных. Пусть анализаторы провели экспертное ранжирование и определение шкал значений степени риска по каждому входу. Параметрические функции принадлежности задаются в трапециевидной форме [11].

Базы знаний формируются согласно правилу (4). Веса $\boldsymbol{w_j}$ для всех правил выбраны равными единице, так как рассматриваемые риски имеют одинаковое влияние на степень ИБ ИТКС. Выходами математической модели ИМА в данном примере являются следующие лингвистические переменные:

- риск несанкционированного изменения общесистемного (ОПО) и специального (СПО) программного обеспечения СЭ;
- риск удаленных атак на СЭ;
- риск несанкционированного вторжения;
- интегральная оценка риска ИБ СЭ ИТКС.

Поэтому по всем модулям логического вывода задаются не только их терм-множества, но и определяются их функции принадлежности, что позволяет произвести детальную классификацию типа риска возможной угрозы ИБ СЭ.

На рис. 2, в качестве примера, представлены функции принадлежности модуля анализа аномалий ОПО и СПО СЭ, на рис. 3 — поверхности функций принадлежности модуля интегральной оценки риска ИБ СЭ.

Предложенные алгоритмы реализованы в среде MATLAB [12].

Анализ результатов численного исследования предложенной математической модели оценки возможных рисков угроз ИБ СЭ ИТКС КИИ показал устойчивость её функционирования к неопределенностям входных переменных, а также соответствие между лингвистическими и численными значениями полученных выходных значений.

Так, если хотя бы одна входная лингвистическая переменная имеет значение <ВЫСОКИЙ>, то на выходе получается значение <ВЫСОКИЙ>. Если все входные переменные имеют значение <НИЗКИЙ>, то выходные значения тоже имеют такие значения. Таким образом, выходное значение формируется как максимальное значение входных переменных.

Вывод по методике

Предложенная математическая модель оценки рисков ИБ СЭ ИТКС КИИ достаточно просто реализуется в виде встраиваемого программного средства как на языке высокого уровня, так и на средствах программирования микроконтроллеров, сигнальных процессоров или программируемых логических интегральных схем.

Рис. 2. ФП модуля анализа аномалий ОПО и СПО СЭ

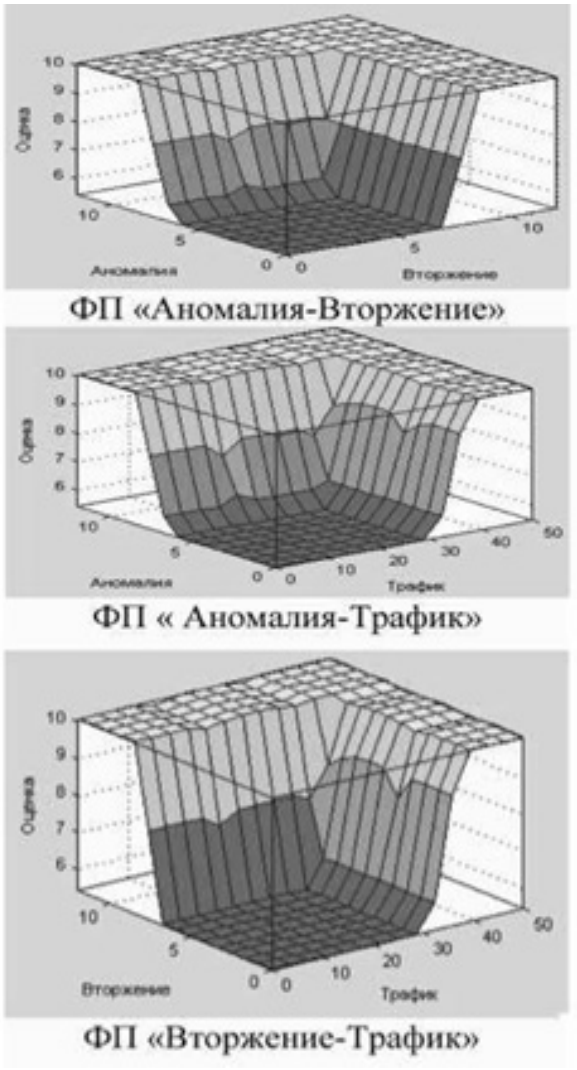

Рис. 3. Поверхности ФП интегральной оценки риска ИБ СЭ

Большинство решений по оценке рисков ИБ СЭ ИТКС КИИ подобное программное средство может принимать самостоятельно, что позволяет повысить оперативность выработки управленческих решений, а также снизить объём передаваемого технологического трафика в сети.

Значения выходных лингвистических переменных могут уточняться с помощью применения метода α- сечений [13].

Рассмотренный подход, как показали проведенные исследования, позволяет поддерживать основные сетевые целевые функции в части оценки и управления рисками ИБ ИТКС КИИ в области Парето-оптимальных значений, что в условиях динамично изменяющихся внешних условий и воздействий на ИТКС КИИ возможных деструктивных факторов, является достаточным условием успешного ее функционирования.

ЛИТЕРАТУРА

1. Гречишников Е.В., Горелик С. П., Белов А. С. Способ управления защищенностью сетей связи в условиях деструктивных программных воздействий // Телекоммуникации. 2014. № 3. С. 18–22.
2. Добрышин М. М., Диденко П. М. Оценка защищённости беспроводных сетей связи // Радиотехника, электроника и связь. II Международная научно-техническая конференция. Омск: 2013. С. 155–159.
3. Поспелов Д. А., 1998. Многоагентные системы — настоящее и будущее // Информационные технологии и вычислительные системы. № 1.

4. Хорошевский В.Ф., 1999. Поведение интеллектуальных агентов: модели и методы реализации // В сб. трудов 4-го международного семинара по прикладной семиотике, семиотическому и интеллектуальному управлению ASC/ IC99.M.
5. Агеев С.А., Саенко И. Б. Метод интеллектуального многоагентного управления рисками информационной безопасности в защищенных мультисервисных сетях специального назначения // T-Comm: Телекоммуникации и транспорт.— 2015.— № 1.— С. 5–10.
6. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. И. Б. Паращук, Ю. Н. Иванов, П. Г. Романенко ВАС, 2010. 104с.
7. Baddar S.A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2014. vol. 5. no. 4. pp. 29–64.
8. Gyanchandani M., Rana J. L., Yadav R. N. Taxonomy of Anomaly Based Intrusion Detection System: A Review // International Journal of Scientific and Research Publications. 2012. vol. 2. Issue 12. pp. 1–13.
9. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
10. «Trusted Computer System Evaluation Criteria», The Orange Book, Department of Defense, NCSC, National Computer Security Centre, DoD5200.28-STD, December 1985.
11. Борисов В.В., Круглов В. В., Федулов А. С. Нечеткие модели и сети.— М.: Горячая линия — Телеком, 2012.— 284 с.
12. Штовба С. Д. Проектирование нечетких систем средствами MATLAB.— М.: Горячая линия — Телеком, 2007.— 288 с
13. Ярушкина Н. Г. Основы теории нечетких и гибридных систем.— Москва: «Финансы и статистика», 2004.— 320 с.

© Фисун Владимир Владимирович (wfisun@gmail.com).

Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Краснодар