ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2019 Том 7 № 4 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2019 Vol. 7 Iss. 4 ISSN 2307-1303 http://www.itt.sut.ru

МОДЕЛЬНО-АНАЛИТИЧЕСКИЙ ИНТЕЛЛЕКТ АГЕНТОВ ОБНАРУЖЕНИЯ ВНЕЗАПНО ПОЯВЛЯЮЩИХСЯ СОБЫТИЙ

Д. М. Паскин, Л. К. Птицына*

Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: ptitsina_lk@inbox.ru

Аннотация
Описаны объективные причины востребованности в цифровой экономике интеллектуальных систем обнаружения внезапно появляющихся событий. Представлены принципы формирования математического обеспечения агентов обнаружения внезапно появляющихся событий. Рассмотрены типовые условия функционирования агентов. Выбран метод обнаружения внезапно появляющихся событий. Определены показатели качества обнаружения. Раскрыты приемы моделирования процессов обнаружения. Сформирован модельно-аналитический интеллект агентов обнаружения внезапно появляющихся событий.

Ключевые слова
Появляющееся событие, обнаружение, программный агент, метод, качество обнаружения, показатели, модельно-аналитический интеллект.

Информация о статье
УДК 004.7:004.422.8
Язык статьи – русский.
Поступила в редакцию 30.03.2019, принята к печати 30.12.19.

Ссылка для цитирования: Паскин Д. М., Птицына Л. К. Модельно-аналитический интеллект агентов обнаружения внезапно появляющихся событий // Информационные технологии и телекоммуникации. 2019. Том 7. № 4. С. 43–49. DOI 10.31854/2307-1303-2019-7-4-43-49.

MODEL ANALYTICAL INTELLIGENCE OF AGENTS FOR DETECTING SUDDEN EVENTS

D. Paskin, L. Ptitsyna*

The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

*Corresponding author: ptitsina_lk@inbox.ru

Abstract—The objective reasons for the demand in the digital economy of intelligent systems for detecting suddenly occurring events are described. The principles of the formation of software for agents for detecting sudden events are presented. Typical conditions for the functioning of agents are considered. A method for detecting sudden events has been selected. Detection quality indicators are determined. Revealed techniques for modeling detection processes. Formed model analytical intelligence agents detecting suddenly occurring events.

Keywords—An occurring event, detection, software agent, method, detection quality, indicators, model analytical intelligence.

Article info
Article in Russian.
Received 30.03.2019, accepted 30.12.19.

For citation: Paskin D., Ptitsyna L.: Model Analytical Intelligence of Agents for Detecting Sudden Events // Telecom IT. 2019. Vol. 7. Iss. 4. pp. 43–49 (in Russian). DOI 10.31854/2307-1303-2019-7-4-43-49.

Жизненный цикл сложных техногенных систем традиционно сопровождался системами мониторинга и функционального диагностирования, обеспечивающих своевременное обнаружение и адекватное реагирование на проявляющиеся внештатные события. Накапливаемые знания в этой сфере профессиональной деятельности распространялись и на биотехнические системы, и на медицинские системы, и на социологические системы.

В условиях развития информационного общества, цифровой экономики, искусственного интеллекта проблемная область обнаружения внезапно появляющихся событий масштабно разрослась по всем направлениям, связанным с обеспечением необходимого качества функционирования и деятельности, требуемых надежности, устойчивости, стабильности, живучести и безопасности. По мере усиления влияния глобализации на безопасность жизнедеятельности в социуме значимость обнаружения внезапно появляющихся событий угрожающего характера многократно возросла. Возросшая значимость прослеживается по всему многообразию направлений обеспечения безопасности, в том числе и информационной безопасности [1, 2].

Другие, не менее важные, аспекты значимости обнаружения внезапно появляющихся событий, ассоциируются с развитием интеллектуальных цифровых технологий, с которыми неразрывно связано обеспечение национального технологического суверенитета. Подобная ассоциация объясняется тем, что интеллек-

туальные цифровые технологии становятся активным звеном в процессах изменения структуры и содержания отраслевых отношений, определяющих необходимость непрерывного совершенствования информационных инфраструктур в направлении обеспечения их оперативной гибкости по отношению к различным ситуациям в экономике и окружающем мире. Особенно остро возрастающая актуальность обнаружения внезапно появляющихся событий проявляется по отношению к тем ситуациям, которые имеют крайне негативные или катастрофические последствия в национальном или мировом масштабе.

При предупреждении негативных или катастрофических последствий важнейшая роль отводится интеллектуальным информационным системам и технологиям, в которых ведущие функциональные позиции закрепляются за вычислительным интеллектом в виде программных агентов [3]. Программные агенты, в функциональную спецификацию которых вводится обнаружение внезапно появляющихся событий, рассматриваются как обязательные компоненты механизмов оперативного реагирования в целях предупреждения, исключения или снижения последствий, связанных с ними.

В контексте представленной актуальности при разработке наукоемкого ядра рассматриваемых технических объектов особое внимание должно уделяться: методам решения задач обнаружения появляющихся событий в условиях априорной неопределённости знаний относительно статистических свойств контролируемых признаков и момента времени их изменения; методам анализа качества обнаружения появляющихся событий; формированию модельно-аналитического интеллекта внезапно появляющихся событий, обеспечивающего управление качеством их обнаружения.

Среди известных методов выделенной направленности указанным условиям в полной мере соответствует метод невязок, предусматривающий формирование модели наблюдаемого контрольного признака и рекуррентное оценивание её параметров по мере накопления данных в условиях отсутствия каких-либо изменений.

В связи с описанным целеполаганием рассматриваются два типовых условия функционирования программного агента. Первое условие касается отсутствия каких-либо изменений статистических свойств наблюдаемого контрольного признака, в второе условие – проявления скачкообразного изменения статистических свойств наблюдаемого контрольного признака.

Предлагаемый подход к формированию модельно-аналитического интеллекта программного агента основывается на разработке аналитических моделей для определения основных свойств решающего правила, соответствующего методу невязок.

При исследовании определяются основные составляющие характеристики обнаружения появляющихся событий: вероятность ложного обнаружения, среднее число шагов до ложного обнаружения и среднее число шагов запаздывания в обнаружении.

Определение качества обнаружения начинается с рассмотрения случая отсутствия появляющихся событий, т. е. с рассмотрения ложных тревог. Пусть наблюдается последовательность контролируемого признака, являющегося нормальным стационарным процессом. В этой ситуации последовательность значений контролируемого признака представляется стохастической моделью в виде

авторегрессии. В таком случае $G(n, j)$ решающая функция внутри области допустимых значений, характеризуемой интервалом $-H < G(n, j) < H$, описывается с помощью преобразования из таблицы 1, где H – абсолютное значение порога обнаружения, n – текущее дискретное время, j – текущее время в течение периода накопления информации, N – период накопления информации, Z_n – белый шум.

Таблица 1

Решающая функция $G(n, j)$ при отсутствии событий

Преобразование
$G(n,j) = y\sqrt{\frac{j-1}{j}} + \frac{z_n^2 - 1}{\sqrt{2j}},$ $y = \frac{\sum_{i=1}^{j-1}\left[(z_{n-j+i})^2 - 1\right]}{\sqrt{2(j-1)}},$ $j = 1,2,...,N,1,2,...,N,...; n = 1,2,...$

Тогда вероятность объявления ложной тревоги определяется соотношением:

$$P_л = \sum_{k=1}^{N} \frac{\prod_{i=1}^{k}(1 - P_{i-1})}{\sum_{k=1}^{N}\prod_{i=1}^{k}(1 - P_{i-1})} P_k .$$

Вероятности $P_1, P_2, ..., P_{N-1}$ приближенно определяются как безусловные вероятности выхода решающей функции, принадлежащей выделенным совокупностям, за заданные границы $-H, H$:

$$P_{i-1} \approx \begin{cases} 1 - F_{i-1}(H\sqrt{2(i-1)} + i - 1), -\sqrt{\frac{i-1}{2}} > -H \\ 1 - F_{i-1}(H\sqrt{2(i-1)} + i - 1) + F_{i-1}(-H\sqrt{2(i-1)} + i - 1), -\sqrt{\frac{i-1}{2}} \le -H \end{cases}.$$

Входящая в найденное соотношение функция распределения соответствует следующему описанию:

$$F_{i-1}(u) = \frac{1}{2^{(i-1)/2}\Gamma((i-1)/2)} \int_0^u G^{\frac{i-1}{2}-1} e^{-\frac{G}{2}} dG .$$

Значения функции $F_{i-1}(u)$ вычисляются по интерполяционной схеме Эйткена.

В результате описания поведения решающей функции в классе марковских цепей устанавливается, что среднее число шагов до объявления первой ложной тревоги $\overline{N_{\text{л}}}$ определяется соотношением:

$$\overline{N_{\text{л}}} = \frac{1 + \sum_{j=2}^{N} \prod_{i=1}^{j-1} (1 - P_i)}{1 - \prod_{i=1}^{N} (1 - P_i)}.$$

Сопоставление результатов аналитического моделирования с результатами имитационного моделирования показывает, что по приведённым соотношениям находится верхняя граница для вероятности объявления ложной тревоги и нижняя граница для среднего числа шагов до этого события.

Далее формируется аналитическая модель для определения среднего числа шагов запаздывания в обнаружении появляющегося события, приводящего к внезапному изменению всех или любого из параметров авторегрессионной модели контролируемого признака первого порядка.

Рассматриваемая решающая функция после появлении события описывается преобразованием, представленными в таблице 2, где $\mu^{(1)}$, $\mu^{(2)}$ – математические ожидания контролируемого признака до и после появления события, $\alpha_1^{(1)}$, $\alpha_1^{(2)}$ – параметры уравнения авторегрессии до и после появления события, $\beta^{(1)}$, $\beta^{(2)}$ – остаточные среднеквадратичные отклонения до и после появления события, $\sigma^{(2)}$ – среднеквадратичное отклонение после появления события.

Таблица 2

Решающая функция $G(n, j)$ после появления события

Преобразование
$G(n,j) \approx a_j z_n^2 + c_j, a_j = (\beta^{(2)}/\beta^{(1)})^2 \frac{1}{\sqrt{2j}},$
$c_j = \frac{1}{\sqrt{2}(\beta^{(1)})^2}\left[\frac{j-1}{\sqrt{j}}(\beta^{(2)})^2 + (\alpha_1^{(2)} - \alpha_1^{(1)})^2(\sigma^{(2)})^2\sqrt{j} + \sqrt{j}(\mu^{(2)} - \mu^{(1)})^2(1-\alpha_1^{(1)})^2\right] - \sqrt{j/2},$
$j = 1,2,...,k,...,N$

Согласно описанию, из таблицы 2 определяется среднее число шагов запаздывания;

$$\overline{N_{\zeta}} = \frac{1 + \sum_{j=2}^{N} \prod_{i=1}^{j-1} (1 - I'_j)}{1 - \prod_{i=1}^{N} (1 - I'_j)},$$

$$I'_j = \begin{cases} 1 - F_1\left(\dfrac{H - c_j}{a_j}\right), & \text{если} - H \le c_j < H, \\ 1 - F_1\left(\dfrac{H - c_j}{a_j}\right) + F_1\left(\dfrac{-H - c_j}{a_j}\right), & \text{если} - H > c_j, \\ 1, & \text{если} c_j \ge H. \end{cases}$$

Представленные результаты аналитического моделирования поведения решающей функции после появления события найдены с помощью формализаций в классе конечных цепей Маркова.

При вычислениях значений $\overline{N_\zeta}$ по приведённым формулам получаются заниженные оценки по сравнению с результатами имитационного моделирования.

Полученные выражения для оценки показателей качества образуют модельно-аналитический интеллект агентов обнаружения внезапно появляющихся событий.

Модельно-аналитический интеллект позволяет проводить анализ влияния порога и относительного периода накопления решающей функции на качество обнаружения появляющихся событий в различных условиях их проявлений и выбирать параметры решающего правила в соответствии с необходимыми требованиями.

Литература

1. Птицына Л. К., Паскин Д. М. Анализ рисков срыва временного регламента по обнаружению угроз информационной безопасности // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23–25 октября 2019 г.: материалы конференции, СПОИСУ. – СПб., 2019. – С. 466–468.

2. Птицына Л. К., Паскин Д. М. Определение рисков срыва временного регламента по обнаружению угроз информационной безопасности // Региональная информатика и информационная безопасность: сборник трудов, СПОИСУ. – СПб., 2019. Вып. 7. – С. 126–128.

3. Птицына Л. К. Интеллектуальные системы и технологии : учебное пособие: СПбГУТ. – СПб., 2019. – 231 с.

References

1. Ptitsyna L., Paskin D. Analysis of Temporary Regulations Detection on Information Security Threat Detection // Information Security of Russian Regions (ISRR-2019). XI St. Petersburg Interregional Conference, St. Petersburg, November 23-25, 2019: Proceedings of the conference, 2019. pp. 466–468.

2. Ptitsyna L., Paskin D. Determination of The Risk of the Temporary Regulations on Detection of Information Security Threat // Proceedings Regional Informatics and Information Security. The Issue No 7. pp. 126–128.

3. Ptitsyna L. K. Intellektualnyye sistemy i tekhnologii : uchebnoye posobiye: SPbGUT. – SPb., 2019. – 231 s.

Паскин Дмитрий Михайлович – студент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, paskin@iac.spb.ru

Птицына Лариса Константиновна – доктор технических наук, профессор, заведующая кафедрой, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, ptitsina_lk@inbox.ru

Paskin Dmitry – Student, SUT, St. Petersburg, 193232, Russian Federation, paskin@iac.spb.ru

Ptitsyna Larisa – Doctor of Engineering Sciences, Full Professor, Head of the Department, SUT, St. Petersburg, 193232, Russian Federation, ptitsina_lk@inbox.ru