УДК 001.891:[51:004]

Птицына Л. К., Птицын Н. А.

РАСШИРЕНИЕ ЗНАНИЙ О РАННЕМ ОБНАРУЖЕНИИ ПОЯВЛЯЮЩИХСЯ ИЗМЕНЕНИЙ

Лариса Константиновна Птицына
доктор технических наук, профессор
ptitsina_lk@inbox.ru
ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича» (СПбГУТ), Россия, Санкт-Петербург
Никита Алексеевич Птицын
nikita_pti@inbox.ru
ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» (Университет ИТМО), Россия, Санкт-Петербург

EXTENSION OF KNOWLEDGE ABOUT EARLY DETECTION OF APPEARING CHANGES

Larisa Konstantinovna Ptitsyna
Federal State Educational Budget-Financed Institution of Higher Education the Bonch-Bruevich Saint-Petersburg State University of Telecommunications, SPbSUT, Russia, Saint-Petersburg
Nikita Alexeyevich Ptitsyn
Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Russia, Saint-Petersburg

Аннотация. *Представлены основания для развития математического обеспечения систем раннего обнаружения появляющихся изменений. Описаны условия обнаружения появляющихся изменений. Предложен перспективный*

прием интеллектуализации систем раннего обнаружения на основе подключения модельно-аналитического интеллекта. Выбран метод обнаружения появляющихся изменений. Определены основные приемы формирования модельно-аналитического интеллекта для систем раннего обнаружения появляющихся изменений.

***Abstract**. The reasons for the development of software for early detection of emerging changes are presented. The conditions for detecting emerging changes are described. A promising technique for the intellectualization of early detection systems based on the connection of model-analytical intelligence is proposed. The method for detecting emerging changes has been selected. The basic techniques for the formation of model-analytical intelligence for early detection systems of emerging changes are determined.*

***Ключевые слова:** цифровая экономика, обнаружение изменений, интеллектуализация, характеристики обнаружения, комплексирование, управление качеством обнаружения.*

***Keywords:** digital economy, change detection, intellectualization, detection characteristics, integration, detection quality management.*

Согласно стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, программе цифровой экономики Российской Федерации, национальной стратегии развития искусственного интеллекта основным фактором обеспечения технологического суверенитета становятся интеллектуальные цифровые технологи. В стратегическом контексте интеллектуальные цифровые технологии ориентированы на повышение качества жизни в стране. В технократическом контексте интеллектуальные цифровые технологии становятся активным звеном, изменяющим структуру и содержимое отраслевых отношений, предопределяющих необходимость интенсивного совершенствования информационных инфраструктур в направлении обеспечения их гибкости по отношению к различным ситуациям в экономике и окружающем мире.

Подобная гибкость становится возможной при запуске механизмов оперативного реагирования на всевозможные изменения. По указанным причинам актуализируется интеллектуализация систем раннего обнаружения появляющихся изменений. Особая значимость оперативного реагирования проявляется при защите информации [1].

Представляемая интеллектуализация ориентируется на развитие математического обеспечения систем раннего обнаружения появляющихся изменений посредством введения в его состав модельно-аналитического интеллекта для управления их качеством.

Модельно-аналитический интеллект разрабатывается с применением методов теории вероятностей, методов теории принятия решений, методов теории временных рядов и методов теории искусственного интеллекта и математического аппарата генерации системно-аналитического ядра безопасных информационных технологий, раскрытого в [2].

Проведённый обзор известных методов обнаружения изменений контролируемых признаков позволил условно разделить задачи на 3 класса:

- задачи обнаружения появляющихся изменений в условиях априорной определённости знаний относительно статистических свойств контролируемых признаков, когда входные параметры наблюдаемой системы заранее известны или хорошо прогнозируемы;
- задачи обнаружения появляющихся изменений в условиях априорной неопределённости знаний относительно статистических свойств контролируемых признаков;
- задачи обнаружения появляющихся изменений при априорной неопределённости параметров плотностей распределения контролируемого признака и вероятностных характеристик момента их смены.

Для задач обнаружения появляющихся изменений в условиях априорной определённости знаний относительно статистических свойств контролируемых признаков уже существуют апробированные методы и алгоритмы. К ним отно-

сятся стабильные обнаружители, использующие минимаксное правило Неймана–Пирсона, асимптотически оптимальные стабильные обнаружители, стабильные субоптимальные обнаружители.

В настоящее время проявляется высокая востребованность методов решения задач обнаружения появляющихся изменений в условиях априорной неопределённости знаний относительно статистических свойств контролируемых признаков и момента времени их изменения. Среди известных методов подобной направленности указанным условиям в полной мере соответствует лишь метод невязок.

Исследованный метод обнаружения появляющихся изменений ориентирован на оценивание момента времени появления «разладки» при априорной неопределённости параметров плотностей распределения контролируемого признака и вероятностных характеристик момента их смены.

При расширении математического обеспечении системы представления знаний о качестве обнаружения появляющихся изменений выведены новые аналитические зависимости для определения вероятности ложного обнаружения появляющегося изменения и среднего времени до ложного обнаружения.

Процесс расширения распространен и на определение среднего времени запаздывания в обнаружении появляющегося изменения. На основании нового математического обеспечения определен порядок нахождения характеристик обнаружения появляющихся изменений.

При дальнейшем расширении математического обеспечении системы представления знаний о качестве обнаружения появляющихся изменений проанализирована типовая ситуация, связанная с комплексированием решений. При этом рассмотрена модель объединения групп решений по булевой функции «ИЛИ», которая по сравнению с рассмотренным в [3] вариантом отличается повышением скорости реагирования на появляющиеся изменения.

Построенная модель для определения показателей качества обнаружения появляющихся изменений позволяет выявить эффект от комплексирования решений по принципу «невязок» наблюдений.

Разработанное новое математическое обеспечение проанализировано на корректность посредством проверки соблюдения аналитических инвариантов.

После подтверждения корректности нового математического обеспечения проведен анализ влияния элементов параметрического пространства на характеристики обнаружения появляющихся изменений.

Научная новизна результатов исследований заключается в том, что впервые сформирован модельно-аналитический интеллект систем раннего обнаружения появляющихся изменений, реализующей метод невязок в условиях варьируемой размерности набора контролируемых признаков.

Практическая значимость результатов исследований предопределяется обеспечением возможностей вычисления характеристик обнаружения появляющихся изменений и управления качеством обнаружения в условиях варьируемой размерности набора контролируемых признаков в реальных системах.

Список литературы

1. Птицын, А. В. Аналитическое моделирование комплексных систем защиты информации / А. В. Птицын, Л. К. Птицына. – Гамбург. Saarbrucken : LAP LAMBERT Academic Publishing, 2012. – 293 с.

2. Птицын, А. В. Генерация системно-аналитического ядра безопасных информационных технологий / А. В. Птицын, Л. К. Птицына. – Санкт-Петербург : Изд-во Политехн. ун-та, 2011. – 263 с.

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