Prof. Valerij Pakhotin — I. Kant Baltic Federal University, Kaliningrad.
E-mail: VPakhotin@kantianf.ru

Dr Kseniya Vlasova — Ass. Prof., BSAFF, Kaliningrad.
E-mail: p_ksenia@mail.ru

Prof. Svetlana Molostova — I. Kant Baltic Federal University, Kaliningrad.
E-mail: VPakhotin@kantianf.ru

УДК 281.5.015



*Д. В. Березкин*

# СЕМИОТИЧЕСКИЙ ПОДХОД К ПОСТРОЕНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

*Предложен семиотический подход к проектированию информационных систем в области безопасности, основанный на извлечении знаний из слабоструктурированных источников. Рассмотрены вопросы выработки оптимальных вариантов по предотвращению угроз для систем поддержки принятия решений. Предложена методика постоянного мониторинга текстовых сообщений, выявления событий и ситуаций, выработки сценариев возможного развития кризисных ситуаций.*

*The paper is devoted to issues of semiotic approach for the design of information security systems, based on knowledge extraction from semi-structured sources. The problems of developing of optimal variants for the prevention of threats to decision support systems. The technique continuous monitoring of text messages, identify the events and situations and develop scenarios possible development of crisis situations is proposed.*

**Ключевые слова:** семиотические системы, модели рисков и угроз, извлечение знаний, искусственный интеллект, системы поддержки принятия решений, экспертные системы.

**Key words:** semiotic systems, risk and threats models, knowledge extraction, artificial intelligence, decision support systems, expert systems.

## Ведение

В современном мире возрастает актуальность различных решений задач, связанных с обеспечением безопасности, которые охватывают все сферы общественной жизни. В связи с усложнением технологий современного производства, совершенствованием вооружения, обострением конфликтов в ряде регионов мира появляются новые угрозы безопасности, которые часто трудно прогнозировать. Тенденция к глобализации современного мира приводит к тому, что региональные угрозы в какой-то сфере могут быстро распространяться на другие регионы и влиять на процессы в совершенно иных областях общественной жизни

или производственной деятельности. Обеспечение выработки оптимальных мер по предотвращению имеющихся угроз или снижению риска их возникновения является приоритетной задачей современного общества и требует широкого использования современных информационных технологий.

Требования к обеспечению безопасности и мероприятия в области безопасности закреплены в различных нормативно-правовых документах. Так, основные принципы соблюдения прав граждан и их безопасности закреплены Конституцией РФ. Конкретные правовые нормы раскрываются в Федеральных законах, указах Президента РФ, ежегодных Посланиях Президента РФ, других нормативных актах. Эти документы создают правовую основу для создания системы мониторинга угроз национальной безопасности Российской Федерации. Более частные вопросы и требования к обеспечению безопасности закреплены в нормативных документах министерств и ведомств РФ, в государственных, отраслевых стандартах и т. д.



Стратегия оптимального управления для предотвращения угроз безопасности должна быть направлена на уменьшение рисков реализации соответствующих угроз на величину ниже некоторого приемлемого порога, величина которого должна быть научно обоснована и утверждена в установленном законодательством РФ порядке. Подобный подход применяется для разных областей, в которых возможны угрозы (экономика, экология, техногенные катастрофы и т. д.). Например, угрозы, изложенные в Стратегии национальной безопасности Российской Федерации [1], могут быть отправной точкой для определения соответствующих рисков.

Для решения задач предотвращения угроз национальной безопасности необходимо создание сложных информационных систем (ИС). Характерной тенденцией, оказывающей сильное влияние на архитектуру современных ИС, является бурное развитие Интернета, где информация содержится, как правило, в неструктурированном виде. Кроме этого, существует большое число документальных систем, в которых информация традиционно представлена в слабоструктурированном виде. С развитием Интернета, а также других средств связи появляется возможность эффективной удаленной работы с такими системами. Отмеченные особенности определяют требования к архитектуре современной ИС, которая должна быть способной манипулировать информацией в текстовой форме, причем эти тексты могут иметь различные наборы знаков и объединять различные модели данных и знаний. Такая архитектура была нами проработана и доведена до программной реализации [2].

## Подход к созданию семиотической системы

С учетом рассмотренных выше особенностей ИС в области безопасности и предъявляемым к ним требованиям предлагается строить их на основе принципов построения семиотических систем.

Основы данного направления в искусственном интеллекте и теории построения такого класса систем в России были заложены и развиты в работах таких ученых, как А. Д. Поспелов, Ю. И. Клыков, Г. С. Осипов, В. Б. Тарасов и других авторов. Основные информационные единицы, с которыми оперируют семиотические системы, обладают такими свойствами, как именованность, структурированность, иерархичность, связность, активность и рефлексивность, в них поддерживаются различные связи и отношения между этими информационными единицами. Такие системы должны иметь механизмы динамического изменения этих информационных единиц и их отношений, а также использовать различные модели для их представления.



Согласно [3] семиотическая система можно описать выражением

$$SS = (T, R, A, P, \alpha(T), \beta(R), \gamma(A), \delta(P)), \quad (1)$$

где $T$ — множество базовых элементов (алфавит системы); $R$ — множество синтаксических правил; $A$ — множество аксиом; $P$ — множество правил вывода; $\alpha(T)$, $\beta(R)$, $\gamma(A)$, $\delta(P)$ — правила изменения соответствующих компонентов формальной системы.

Принципиальной особенностью семиотической системы (1) является возможность моделировать изменения различных параметров формальной системы: аксиом, правил вывода, ограничений, стратегий поиска решений, ценностных ориентаций и других, что принципиально важно для построения современных ИС в области безопасности.

Согласно работам [4; 5] семиотические системы тесно связаны с системами ситуационного управления, в которых знания и законы управления сложно формализовать, и они описываются семантическими представлениями естественно-языковых описаний. В предлагаемом подходе источником ситуационных моделей и их формальных описаний стали тексты сообщений на естественном языке.

Изменение параметров семиотической системы (1) предлагается реализовать за счет постоянного мониторинга текстовых сообщений, выявления событий и ситуаций, информация о которых содержится в этих сообщениях, и выработки сценариев возможного развития ситуаций, на основе которых вырабатываются предложения и готовятся мероприятия по предотвращению тех или иных выявленных угроз безопасности. Предлагаемая методика выявления и предотвращения угроз получила обозначение «4С + П» (Сообщение – Событие – Ситуация – Сценарии – Предложение). С ее помощью возможно реагировать на изменения ситуации с учетом динамики развития тех или иных угроз, а также обнаруживать риск возникновения таких угроз, модель которых нам заранее неизвестна.

Методика состоит из нескольких крупных этапов.

1. Сбор сообщений из различных источников.

2. Выделение из текстового потока аналитических статей и новостных сообщений.

3. Задание тем для отслеживания.

4. Обнаружение событий в потоке новостных сообщений. Формирование кластеров документов, соответствующих событиям.

5. Установление связей между событиями и темами.

6. Объединение выявленных событий в ситуации.

7. Сопоставление выявленных ситуаций с известными аналогами или экспертными сценариями.

8. Формирования возможных сценариев развития кризисной ситуации.

9. Формирование предложений по преодолению кризисных ситуаций на основе различных критериев эффективности и качества для оценки принимаемых мер.



**Постановка задачи управления рисками**

Стратегия оптимального управления для предотвращения угроз должна быть направлена на уменьшение рисков реализации соответствующих угроз на величину ниже некоторого приемлемого порога, величина которого должна быть научно обоснована и утверждена руководством страны. Подобный подход применяется для разных областей, в которых возможны угрозы (экономика, экология, техногенные катастрофы и т. д.). В работах специалистов Рабочей группы при Президенте РАН «Риск и безопасность» (председатель член-корреспондент РАН Н. А. Махутов) анализируются подобные риски и предлагается стратегия управления рисками.

В частности, в этих работах предлагается на основе требований документов стратегического планирования определить ключевые критерии перспективного развития и обеспечения национальной безопасности, такие как сохранение и преумножение страны $N_R(\tau_k) > N_R(\tau_0)$ и устойчивое социально-экономическое развитие $V_R(\tau_k) > V_R(\tau_0)$. Исходя из этих критериев, можно определить соответствующие оценки рисков:

$$R_N(\tau) \leqslant [R_N(\tau)],\ R_N(\tau_k) < R_N(\tau_0), \tag{2}$$

$$R_V(\tau) \leqslant [R_V(\tau)],\ R_V(\tau_k) < R_V(\tau_0), \tag{3}$$

где $R(\tau)$ — величина реализующихся рисков соответствующих типов, а $[R(t)]$ — величина приемлемых рисков на заданном временном интервале $t$. На основе неравенств (2)—(3) можно получить научно обоснованную стратегию управления, обеспечивающую требуемый уровень национальной безопасности и защищенности человека, общества и государства:

$$Z(\tau) \geqslant [Z(\tau)],\ Z(\tau_k) > Z(\tau_0). \tag{4}$$

В [6] показана связь затрат $Z(t)$, направленных на достижение требуемого уровня безопасности с учетом формирующихся рисков $R(t)$:

$$R(t) = F_R\{P(t),\ U(t)\} \leqslant [R(t)] = R_c(t)/n_R = m_Z \cdot Z(t), \tag{5}$$

где $F_R\{P(t),\ U(t)\}$ — некоторая функциональная зависимость, связывающая вероятности возникновения рисков $P(t)$ и величину ущерба $U(t)$;

$R_c(t)$ — величина предельных (недопустимых) рисков; $n_R$ — запас по этим видам риска; $m_Z$ — коэффициент эффективности экономических затрат на снижение экономических рисков ($m_Z \geqslant 1$).

В работе [6] предлагается определять величину рисков $R(t)$ на основе исследований по социальным, естественным и техническим наукам в трех основных сферах жизнедеятельности — социальной ($N$), природной ($S$) и техногенной ($T$), составляющих единую сложную систему «человек — природа — инфраструктура», функционирующую во времени $t$ согласно выражению

$$R(t) = F_R \{R_N(t), R_S(t), R_T(t)\} \quad (6)$$



В предлагаемом подходе оценка рисков, входящих в выражение (6), и выработка оптимальной стратегии по их уменьшению (выражения (4—5)) производятся на основе анализа документов, извлекаемых из слабоструктурированных разнородных источников, содержащих тексты, таблицы и наборы метаданных для этих документов.

### Выбор оптимального варианта устранения угроз

Выше было отмечено, что угрозы, изложенные в Стратегии национальной безопасности Российской Федерации [1], могут быть отправной точкой для определения соответствующих рисков. Для принятия научно обоснованных решений по выбору предпочтительного варианта устранения возникающих угроз или преодоления кризисных ситуаций требуется рассмотрение их во всей совокупности. Для этого необходимо использовать методы решения многокритериальных задач и, в частности, теорию важности критериев.

Кратко рассмотрим постановку этой задачи и подходы к ее решению. Согласно работе [7] модель ситуации принятия решения при многих критериях можно представить в виде

$$\text{МПР} = \{\mathbf{V}, \mathbf{K}, \mathbf{R}_{el}\},$$

где $\mathbf{V}$ — множество вариантов; $\mathbf{K}$ — векторный критерий; $\mathbf{R}_{el} = \{P, I\}$ — отношения предпочтения ($P$) и безразличия ($I$) лица, принимающего решения (ЛПР) о выборе лучшего варианта из $\mathbf{V}$.

Векторный критерий $\mathbf{K} = \{K_1, \ldots, K_i, \ldots, K_m\}$ состоит из значений частных критериев $K_i$, $i = 1, \ldots, m$. В качестве частных критериев для нашего случая примем оценки рисков по разным видам угроз, т. е. $K_i = R_i$, где i принимает значения в зависимости от выбранной модели угроз. Например, $i = \{N, S, T\}$ для модели, определяемой выражением (6).

Критерий $K_i$ можно рассматривать как некоторую функцию, которая устанавливает соответствие между каждым из вариантов $v_j \in \mathbf{V}$ и значением $x \in X_i$, называемым шкалой: $v_j \xrightarrow{Ki} x$.

С учетом специфики решаемой задачи оценки рисков можно утверждать, что эти значения могут быть разными для разных критериев.

Таким образом, задачу оптимального выбора варианта $v_j$ предотвращения выявленных или потенциальных угроз можно представить как поиск оптимальной (с точки зрения ЛПР) векторной оценки **X**:

$$\mathbf{X} = \text{opt}\,(R_1(v_j), \ldots, R_m(v_j)) = \mathbf{X}(v_j),\ (j = 1, \ldots, N). \qquad (7)$$

Можно указать следующие основные подходы для решения задачи оптимального выбора, описываемой выражением (7).

1. Использование обобщенного критерия вида

$$\Phi = \sum_{i=1,\ldots,m} \alpha_i \mathrm{R}_i, \text{ где } \sum_{i=1,\ldots,m} \alpha_i = 1.$$



2. С применением метода анализа иерархий (МАИ).

3. С использованием методов теории важности критериев.

4. С применением методов нечеткой логики.

После детального анализа этих подходов был выбран и реализован МАИ.

При использовании МАИ для оценки угроз безопасности с целью выработки обобщенного показателя выполняется операция попарного сравнения различных угроз между собой.

В предлагаемом подходе алгоритм решения задачи поиска оптимального варианта (7) учитывает специфику извлечения исходных данных из слабоструктурированных источников. Такой подход сочетает преимущества экспертного подхода и возможности автоматического анализа текстов документов.

При анализе количественных оценок важности критериев и при формировании матриц попарных сравнений МАИ можно учитывать коэффициенты риска $r_i = N_i/N$, а также его оценку с учетом прогноза $r_i^*$, где $N_i$ — количество найденных документов, соответствующих $i$-й угрозе, а $N$ — общее число документов определенного типа. Подробное рассмотрение вопросов автоматического анализа текстов документов выходит за рамки настоящей статьи.

## Особенности реализации подхода

Для реализации предлагаемого подхода проведена разработка методов, алгоритмов и программного обеспечения интеллектуальной информационной системы, основанной на принципах семиотической системы. Архитектура программного обеспечения выполнена в микросервисном стиле. Разработанное программное обеспечение может функционировать под различные программные платформы (*Windows*, различные диалекты *Linux*, в том числе *Astra Linux Special Edition*). При создании интерфейсных компонентов программ использовались средства веб-разработки, поэтому программы могут использоваться на различных программно-аппаратных платформах (стационарные устройства, планшеты, смартфоны и т. д.). Схематичное представление предлагаемого подхода показано на рисунке.

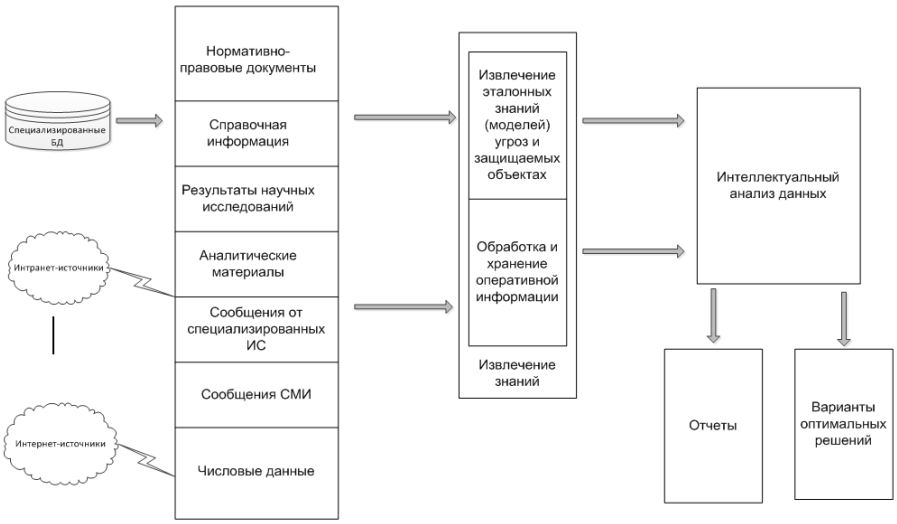


Рис. Схематичное представление предлагаемого подхода

## Заключение

Согласно работе [3] семиотическую систему в смысле Д. А. Поспелова (1) можно задать в виде

$$SS = (\{FS\}, M), \tag{8}$$

где $\{FS\}$ — множество формальных систем, а $M = \{M_i\}$ — семейство моделей модификации формальных систем, которые в нашем случае строятся в результате непрерывного мониторинга событий, происходящих во внешней среде. Анализируемый поток текстовых сообщений моделирует открытую динамическую среду, в которой функционирует система. Результаты такого мониторинга лежат в основе выявления различных угроз и выработки вариантов по их предотвращению. Возможность модификации модели системы (8) позволяет обнаруживать те угрозы, которые заранее неизвестны, т. е. модели угроз могут создаваться или уточняться в процессе работы информационной системы.

В настоящей работе показано применение семиотического подхода для выявления различных угроз и выработки оптимальных вариантов по их предотвращению или недопущению в будущем. Целью дальнейших исследований и разработок может стать построение комплексной системы управления рисками, использующей такой подход. При этом необходимо оценивать качество принятых решений по управлению рисками и вырабатывать новые решения с учетом принятых ранее решений и отклонений поведения защищаемой системы от требуемых параметров. В качестве путей возможного решения этой задачи представляется целесообразным использовать методы построения и анализа динамических интеллектуальный систем, например, предложенные в работах [7; 8].

**Список литературы**

1. *Стратегия* национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31 декабря 2015г. №683) : [Интернет-портал Российской газеты]. URL: http://www.rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения: 05.03.2016).

2. *Березкин Д.*. Технология управления разнородными знаниями // Гибридные и синергетические интеллектуальные системы : матер. 2-го Междунар. Поспеловского симпозиума. Калининград, 2014. С. 45—53.

3. *Тарасов В. Б.* Логико-лингвистические модели в искусственном интеллекте: прошлое, настоящее, будущее. URl: http://posp.raai.org/data/posp2005/Tarasov/tarasov.html (дата обращения: 07.03.2016).



4. *Поспелов Д. А.* Прикладная семиотика и искусственный интеллект // Программные системы и продукты. 1996. № 3. С. 14—28.

5. *Осипов Г. С.* От ситуационного управления к прикладной семиотике // Новости искусственного интеллекта. 2002. № 6. С. 3—7.

6. *Махутов Н. А.* Научные основы задачи по формированию системы оценки рисков // Проблемы анализа риска. 2009. Т. 6, № 3. С. 82—91.

7. *Подиновский В. В.* Введение в теорию важности критериев в многокритериальных задачах принятия решений. М., 2007.

8. *Осипов Г. С.* Динамические интеллектуальные системы // Искусственный интеллект и принятие решений. 2008. № 1. С. 47—54.

9. *Жожикашвили А. В., Стефанюк В. Л.* Динамические интеллектуальные системы // Искусственный интеллект и принятие решений. 2008. № 1. С. 4—14.

**Об авторе**

Дмитрий Валерьевич Березкин — старший преподаватель, МГТУ им. Н. Э. Баумана, Москва.

E- mail: berezkind@bmstu.ru

**About the author**

Dmitry Berezkin — Senior Lecturer, Bauman Moscow State Technical University, Moscow.

E- mail: berezkind@bmstu.ru

УДК 621.391,621.396

*Р. В. Симонов, В. А. Пахотин*

# АЛГОРИТМЫ ПОИСКА ЭКСТРЕМУМА В МЕТОДЕ МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ

*Произведена сравнительная оценка метода наискорейшего спуска и метода отжига (симуляции восстановления) для минимизации функционала правдоподобия при решении задачи разрешения радиоимпульсов по времени. Предложен комбинированный алгоритм, позволяющий повысить быстродействие. Дана оценка области его применимости.*