Рекомендуется использовать четное количество временных параметров, так чтобы один из них был равен **1**, а остальные были симметричны относительно **0.5**. Например, $\{0.2,0.5,0.8,1\}$ $(0.2 = 0.5 - 0.3, 0.8 = 0.5 + 0.3)$.

Таблица – Рекомендуемое сочетание параметров $n$ и $N$

| $N$ | Размерность $n$. Рекомендуемый интервал | Наилучшее значение $n$ | Длины последовательностей, бит |
|---|---|---|---|
| 768 – 1024 | 15 – 25 | $N/50$ | 115200 – 25600 |
| 324 – 767 | 10 – 20 | $N/35$ | 3240 – 15340 |
| 196 – 323 | 5 – 15 | $N/30$ | 980 – 4845 |
| 96 – 195 | 2 – 10 | $N/20$ | 192 – 1950 |
| 32 – 95 | 2 – 8 | $N/10$ | 64 – 760 |

## VIII Выводы

Приведенный статистический тест, основанный на использовании многомерных случайных процессов, позволяет эффективно анализировать случайные и псевдослучайные битовые последовательности. Данный тест ориентирован на работу с короткими и средними последовательностями и позволяет также тестировать очень короткие последовательности. Тест дает возможность анализировать неравновероятные битовые последовательности.

*Литература:* ***1.*** *Коваленко И. Н., Левитская А. А., Савчук М. Н. Избранные задачи вероятностной комбинаторики. – К.: Наук. думка, 1986, - 224с.* ***2.*** *Афифи А., Эйзен С. Статистический анализ. Поход с использованием ЭВМ. – М.: Мир, 1982. – 488с.* ***3.*** *Турчак Л. И. Основы численных методов: Учеб. пособие. – М.: Наука. Гл. ред. физ-мат. лит., 1987. – 320 с.* ***4.*** *ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння.*

**УДК 681.3:621.396**

# СПЕЦИАЛЬНЫЕ СИСТЕМЫ ПРИНЯТИЯ РЕШЕНИЙ В ТЕЛЕКОММУНИКАЦИЯХ И КРИТЕРИИ ОЦЕНКИ ИХ ЭФФЕКТИВНОСТИ

***Геннадий Максименко***
*Национальная Комиссия по вопросам регулирования связи Украины, Киев*

*Аннотация*: **Изложены общетеоретические и концептуальные подходы к построению специальных систем поддержки принятия решений, используемых в телекоммуникационных сетях для выявления и анализа критических событий с целью устранения преднамеренных или непреднамеренных негативных воздействий на сеть. Приведены критерии оценки эффективности функционирования таких систем**.

*Summary*: **This article deals with theoretical and conceptual ideas to crate special intellectual expert systems for detection and analysis critical anomaly events in telecommunication networks. The aim of this expert systems to prevent network negative influences. In article gives performance criteria's of this expert systems.**

*Ключевые слова*: **Система поддержки принятия решений, мониторинг, аномалия сети, прогнозирование**.

## I Введение

Одной из наиболее важных задач в системе государственного управления является создание систем оценки кризисных ситуаций и негативных явлений в сетях связи, их комплексная оценка, анализ и прогнозирование наиболее вероятных сценариев развития, а также оценка рисков и выработка мер по минимизации последствий.

Выявления критических событий в сети, обусловленных аномальной активностью за пределами сети или внутри нее, основано, как правило, на сравнении текущих значений параметров активности со значениями, которые на данный момент признаны нормальными. В качестве таких параметров или исходных данных могут выступать, например, количественные показатели использования системных ресурсов, интенсивности обращений к ресурсам или системным сервисам.

Актуальность данной работы вызвана недостаточным освещением в литературе принципов построения специализированных систем поддержки принятия решений в телекоммуникационных системах. В известных публикациях [1, 2], в основном, освещаются вопросы, связанные с построением узкоспециализированных экспертных систем по обеспечению безопасности компьютерных сетей. Однако, на данный момент актуальным становится построение более универсальных систем поддержки принятия решений, способных анализировать и охватывать широкий круг вопросов анализа функционирования сетей.

Цель данной работы – предложить теоретический и, отчасти, методологический подход к созданию специальных систем поддержки принятия решений (СППР) в телекоммуникационных сетях общего пользования для выявления и прогнозирования аномальных ситуаций.

## II Принципы построения и функционирования сетей

Основными принципами создания специальных СППР по выявлению угроз и воздействий на инфраструктурные и социальные объекты сетей связи являются следующие [3].

1. Принцип оптимальности. Разработка специальной СППР должна проводиться с учетом того, что каждый из методов обнаружения критических ситуаций позволяет достаточно эффективно и достоверно выявлять только определенные виды угроз. Поэтому, при создании СППР должно быть найдено некоторое оптимальное соотношение между методами обнаружения критических ситуаций, возможными механизмами их нейтрализации и способами их применения в составе системы.

2. Принцип адекватности. Разрабатываемые для реализации в СППР проектные решения по обнаружению и противодействию должны быть дифференцированы в зависимости от частоты, вероятности и ожидаемого ущерба от успешной реализации каждого типа угроз.

3. Принцип полноты. Данный принцип заключается в использовании для выявления критических ситуаций информации о состоянии и значениях основных параметров всех основных элементов сети телекоммуникаций и подсистемы радиочастотного мониторинга. В случае необходимости может быть задействован анализ сообщений на основных информационных потоках.

4. Принцип адаптивности. В СППР должны быть предусмотрены механизмы адаптации и самообучения системы к изменяющимся условиям функционирования.

Использование рассмотренных принципов позволит создать перспективную систему, обеспечивающую эффективное и своевременное обнаружение и нейтрализацию критических ситуаций при сохранении оперативности выполнения технологических циклов управления.

В составе специальной СППР по выявлению критических ситуаций могут быть следующие подсистемы:

радиочастотного мониторинга, мониторинга телекоммуникационной сети, обнаружения признаков критической ситуации, анализа и прогнозирования, визуализации и администрирования, противодействия угрозам, регистрации и учета. Возможная структура специальной СППР выявления критических событий представлена на рис. 1.

Подсистема мониторинга телекоммуникационной сети предназначена для сбора и проведения первичного анализа информации о состоянии контролируемых параметров сети в целях выявления наиболее простых видов угроз и, в случае обнаружения каких-либо аномалий в собранной информации, передачи ее для дальнейшего исследования подсистеме обнаружения признаков критической ситуации. В состав данной подсистемы входят датчики коммуникационного оборудования, датчики оборудования цифровых сетей передачи данных, датчики контроля системы сигнализации ОКС-7, датчики средств защиты информации.

Подсистема радиочастотного мониторинга предназначена для контроля параметров радиочастотной обстановки, выявления аномалий в работе радиоканалов и сетей, обнаружение незарегистрированных радиоэлектронных средств (РЭС) и определение их принадлежности. Данная подсистема состоит из стационарных и подвижных пунктов радиомониторинга и сенсорных датчиков радиоконтроля.

Подсистема обнаружения аномалий и признаков критической ситуации предназначена для выявления аномалий в радиочастотной обстановке и возможных угроз информационно-коммуникационным сетям и социальным объектам на основе информации, поступающей от подсистем мониторинга. В состав подсистемы входят средства сбора данных (датчики и сенсоры) о состоянии функционирования объектов,

фильтры событий, а также средства анализа признаков на основе сигнатурных, статистических и поведенческих методов.

Подсистема анализа и прогнозирования предназначена для распознавания критических событий в сети или за ее пределами на основе классификационных признаков, определения тенденций их дальнейшего развития и выдачи рекомендаций по их предотвращению или нейтрализации.

Подсистема визуализации и администрирования предназначена для наглядного представления администратору информации о текущем состоянии сетей связи, значениях основных контролируемых параметров и обнаруживаемых угрозах и критических событиях за пределами сетей, а также для управления функционированием системы и отдельных ее элементов.

Подсистема противодействия угрозам предназначена для прекращения несанкционированного доступа к информационным ресурсам или элементам сетей, деструктивного воздействия на элементы сетей или социальные объекты. В состав подсистемы входят:

- средства анализа и выбора способов противодействия;
- средства противодействия атакам на оборудование цифровых сетей передачи данных;
- средства противодействия угрозам на беспроводные сети передачи данных;
- средства противодействия распространению информации воздействия на социальные группы и объекты.

Подсистема регистрации и учета предназначена для хранения информации о конфигурации системы, исходных данных, необходимых для нормального функционирования подсистем обнаружения признаков критической ситуации, анализа и прогнозирования, противодействия угрозам, а также для хранения результатов функционирования системы и выдачи отчетов по запросам администратора. Конкретная реализация данной подсистемы должна представлять собой совокупность баз данных и обеспечивать хранение следующей информации:

- конфигурации телекоммуникационных сетей в целом и их элементов;
- статистических данных, необходимых для подсистемы обнаружения аномалий и признаков критической ситуации;
- сигнатур информационных воздействий и атак на сети;
- каталог сценариев противодействия угрозам и нейтрализации критических событий;
- профилей нормального поведения сетей и РЧО;
- информационных сообщений, обнаруженных в сетях;
- журналов регистрации событий;
- журнал учета директив и распоряжений.

Для того, чтобы система принятия решений могла обобщать данные, полученные от различных подсистем мониторинга, необходимо преобразовать формат сообщений об аномалиях и угрозах, посылаемых этими подсистемами к виду, пригодному для дальнейшей обработки в СППР. Это преобразование осуществляется в подсистеме обнаружения признаков.

Подсистема обнаружения признаков должна передавать для принятия решения в блок анализа и прогнозирования вектор вида $\overline{S} = \left(A, C, G, T, M, P, P_H, P_B\right)$, где $A$ – системный идентификатор обнаружителя аномалии или угрозы, $C$ – идентификатор самой угрозы или аномалии, $G$ – вид угрозы, $T$ – системное время возникновения угрозы или аномалии, $M$ – идентификатор метода, которым выявлена угроза или аномалия, $P$ – вероятность реализации угрозы или атаки, $P_{\text{в}}$ и $P_{\text{н}}$ – соответственно, нижняя и верхняя вероятность реализации угрозы или атаки.

Процедура обобщения сигналов о возникновении возможных угроз состоит из 3-х этапов.

1. Сбор сигнальной информации с датчиков и сенсоров.

2. Фильтрация сигналов в анализаторах по видам и типам воздействий и угроз, привязка к единой временной оси.

3. Выделение для каждой возможной угрозы или негативного воздействия определенного временного интервала для анализа и принятия решения.

Привязка сообщений об угрозах, атаках или просто аномальных событиях к единой временной оси, позволяет учитывать при принятии решения информацию от разных подсистем и датчиков и генерировать более обоснованное решение. С целью последующего анализа для каждого типа аномальных событий или внешних воздействий должен быть сформирован свой ряд упорядоченных по времени сообщений (рис. 2). При анализе должен учитываться не только тип угрозы или аномального события, но и предполагаемый объект воздействия. Например, должны группироваться сообщения о воздействии на один и тот же информационный центр или одну и ту же социальную группу.

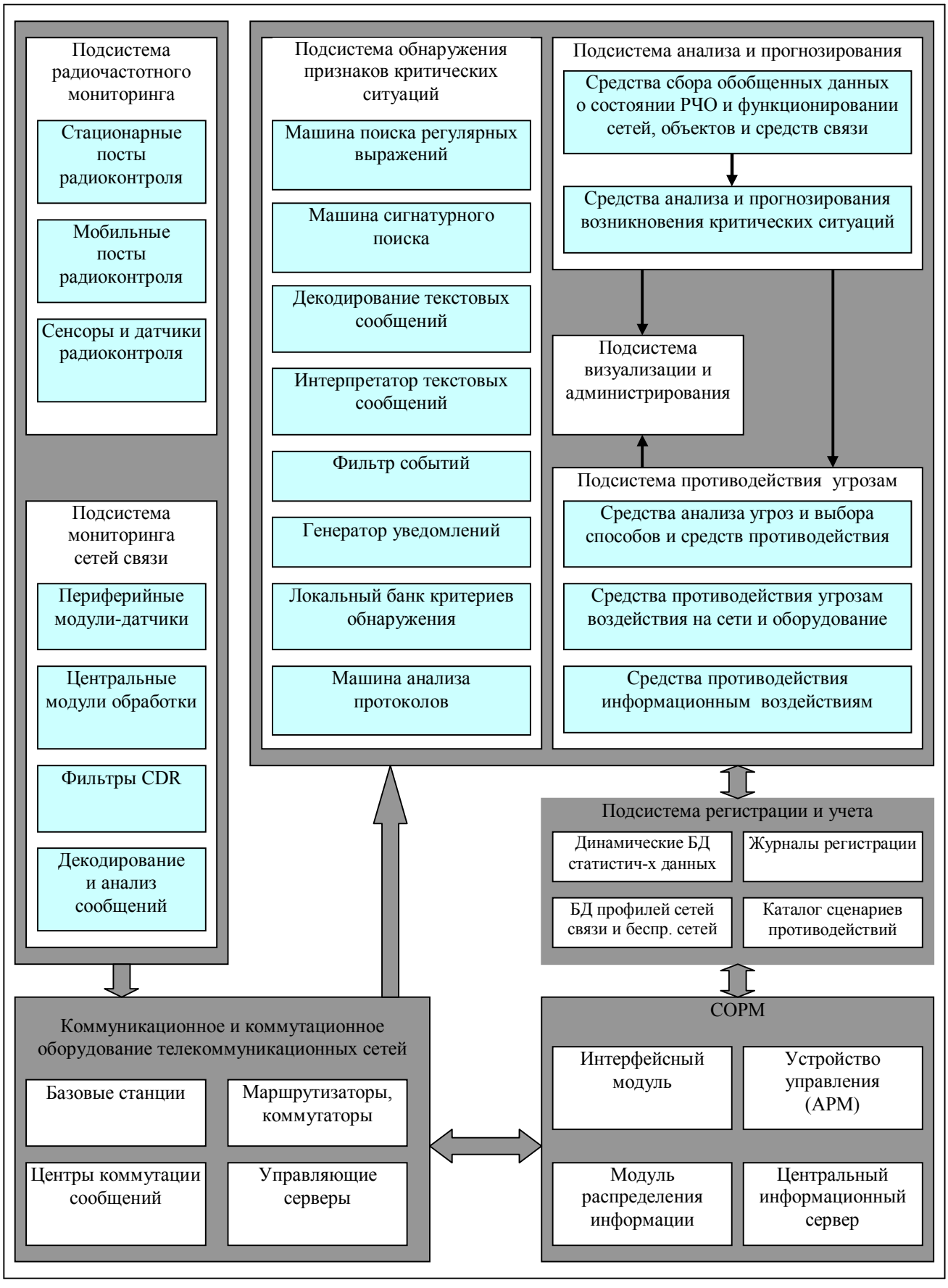


**Рисунок 1 – Структура специальной СППР выявления критических событий**

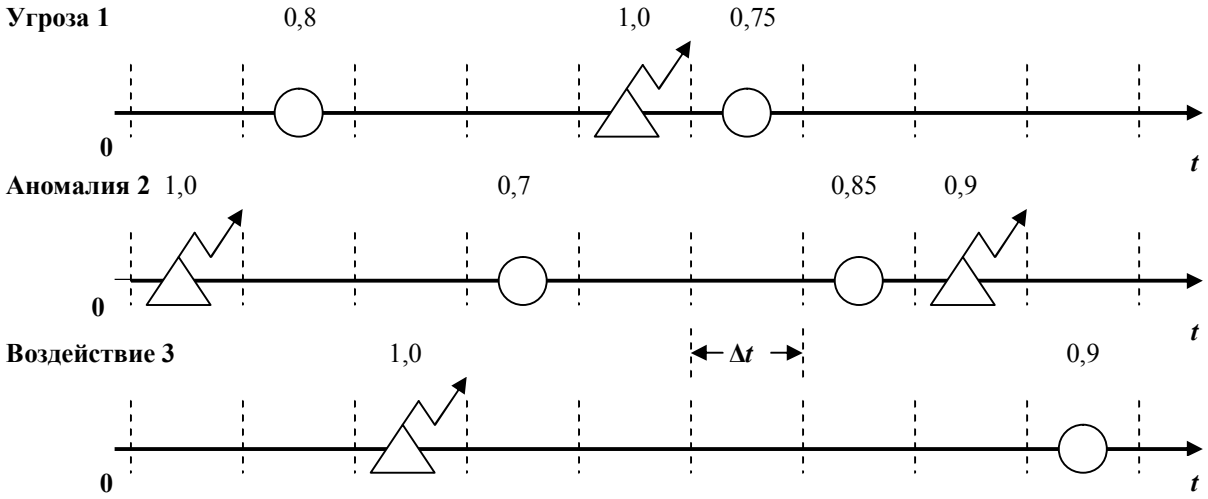


**Рисунок 2 – Фильтрация сообщений по видам аномалий, угроз, воздействий и привязка их к единой временной оси ( △ – подсистема радиочастотного мониторинга; ○ – подсистема мониторинга телекоммуникационной сети)**

Последующая обработка производится раздельно для каждого из видов угроз или воздействий. Временная ось разбивается на интервалы анализа $\Delta t$. Длина интервала анализа выбирается из минимально необходимого времени для обнаружения и классификации угрозы или воздействия. В каждом интервале $\Delta t$ производится анализ сообщений с целью оценки обобщенной вероятности реализации угрозы или негативного воздействия. Для уменьшения вероятности ложной тревоги предлагается использовать мажоритарный критерий для принятия решений. Если в системе присутствует несколько сетевых датчиков или сенсоров, выявляющих данный вид угрозы или воздействия, то решение о его наличии принимается в случае, если оно выявлено более чем тремя датчиками или сенсорами. В случае, когда обнаружители (анализаторы) не просто фиксируют факт аномалии в сети, но и оценивают вероятность угрозы или негативного воздействия, то решение о наличии конкретного вида атаки может приниматься при выполнении следующего условия $\frac{1}{N}\sum_{i=1}^{N} P_i \geq \xi$, где $\xi$ – порог, выбираемый в зависимости от вида негативного воздействия, а также количества обнаружителей (анализаторов) задействованных в системе.

Развитием мажоритарного подхода является применение при вычислении вероятности угрозы, атаки или другого воздействия априорной информации о свойствах используемых подсистем. Это реализуется на основе вычисления взвешенной суммы значений $P_i$, где в качестве весов применяется степень доверия к тому или иному анализатору (подсистеме мониторинга) при рассмотрении каждого возможного воздействия или угрозы. Тогда вероятность обнаружения $k$ - й угрозы или воздействия может быть представлена выражением [6] $P_{k\,\text{об}}(\Delta t_i) = \sum_{j=1}^{m} w_{kj} \cdot P_{kj}$, где $m$ – число анализаторов, используемых в подсистеме мониторинга; $P_{kj}$ – вероятность угрозы $k$, переданная $j$ – м анализатором на интервале $\Delta t_i$, а $w_{kj}$ – степень доверия результатам работы анализатора $j$ при обнаружении угрозы или воздействия типа $k$. Следует помнить, что $\sum_{j=1}^{m} w_{kj} = 1$.

## III Критерии оценки эффективности специальных систем принятия решений

В качестве критериев оценки для СППР можно использовать базовые характеристики качества классификации, параметры производительности вычислительной системы, вероятность своевременного распознавания критической ситуации, пропускную способность (производительность) системы принятия решений с учетом размера и сложности системы.

**Базовые характеристики качества классификации.** К ним можно отнести уровни ошибок первого и второго рода (error rates) и коэффициент обнаружения или эффективности (detection rate). Ошибка первого рода – это "ложный пропуск" (false negative), когда интересующее нас событие ошибочно не обнаруживается. Ошибка второго рода – "ложное обнаружение" (false positive), когда при отсутствии

события ошибочно выносится решение о его присутствии. Коэффициент эффективности определяет процент обнаружения искомых событий (вредоносных действий) среди всех искомых событий, которые имели место, и выражает общую способность классификатора принимать правильные решения.

Часто характеристики качества классификатора пытаются улучшить за счет комбинации нескольких алгоритмов классификации или применения обратной связи для дообучения классификаторов. В данной работе предлагается улучшение качества классификации за счет введения нового типа решения – "Неопределенность" и логической изоляции поведения системы в том случае, когда оно классифицируется как неопределенное. Пример работы классификатора приведен на рис. 3.

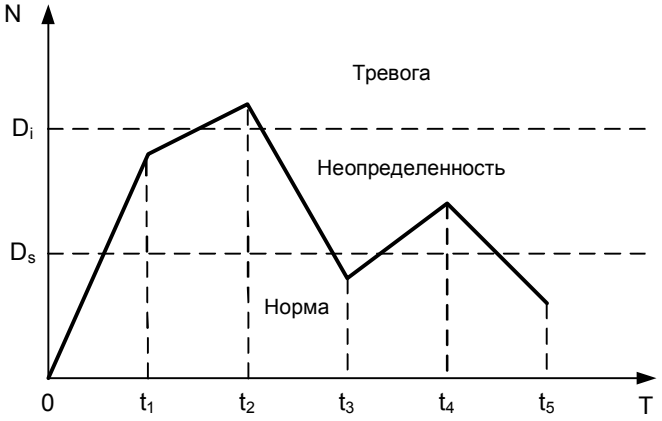


**Рисунок 3 – Пример работы классификатора**

Для реализации классификатора на базе трех видов решений $Y$ = {Норма, Неопределенность, Тревога}, предлагается ввести два критерия классификации, по которым будет приниматься то или иное решение. Первый критерий классификации выражает величину порога неопределенности $D_s$, а второй критерий – величину порога тревоги $D_i$. Данные величины определяются расстоянием входного вектора признаков от эталонных значений классификатора и позволяют варьировать соотношение характеристик качества классификатора.

**Производительность системы**. Оценить производительность системы принятия решений можно с помощью специального критерия, учитывающего два фактора: суммарный дефицит времени для своевременной выработки рекомендаций ССПР и суммарное время простоя вычислительной системы при отсутствии информации о конфликтных ситуациях. Критерий имеет вид [4, 5]:

$$Q = \alpha_1 T_{\text{деф}} + \alpha_2 T_{\text{пр}}, \tag{1}$$

где $\alpha_1$ и $\alpha_2$ - весовые коэффициенты, учитывающие потери, связанные с несвоевременным устранением конфликтных ситуаций и простоем процессора; $\alpha_1 + \alpha_2 = 1$. Практически, методом моделирования установлено, что целесообразно иметь $\alpha_1 = 0{,}65 \div 0{,}75$; $\alpha_2 = 0{,}25 \div 0{,}45$.

Вероятность своевременного распознавания критической ситуации, т. е. $P_{\text{кс}}(t) = P_{\text{кс}}(t < t_{\text{доп}})$.

**Пропускная способность системы принятия решений**. Продолжительность (период) оперативной обработки исходных данных и сведений о критической ситуации должна удовлетворять требованиям по допустимому времени обработки.

При оперативной обработке исходных данных основными решаемыми задачами являются: сбор, систематизация, выборка необходимых данных, сообщений и сведений, представление их в формализованном виде реализаций признаков, установление местоположения исследуемых РЭС и объектов, распознавание источников и объектов специального мониторинга, определение текущей ситуации в сети или за ее пределами и доведение готовых решений для СППР. Поэтому одним из основных показателей функционирования СППР можно считать вероятность того, что время, затрачиваемое на решение этих задач, не превысит допустимой величины:

$$P_{\text{реш}}(t) = P_{\text{кс}}(t_{\text{обр}} < t_{\text{доп}}) = \int_0^{t_3} \mathrm{d}F(t_{\text{обр}}), \tag{2}$$

где Рреш – вероятность своевременной обработки исходных данных в цикле управления; F(tобр) – функция распределения времени обработки; tобр – время полного цикла оперативной обработки; tз – время, заданное для решения задачи распознавания критической ситуации и выработки мер противодействия.

Таким образом, своевременность решения всех отдельных задач обработки исходных данных и в целом эффективность функционирования СПР можно выразить таким показателем, как вероятность полного цикла обработки исходной информации и данных за время, не более заданного, т. е. вероятностью своевременной обработки $P_{\text{реш}}$.

Процесс обработки полученных данных, сообщений и сведений является стохастическим. Это определяется вероятностным характером входного потока данных и сообщений от подсистем мониторинга, случайными моментами времени выборки, распознавания и принятия решения. В общем виде вероятность своевременной обработки $P_{\text{реш}}(t)$ будет определяться в зависимости от:

$$P_{\text{реш}}(t) = f(\lambda, S, m, n, \mu, T_{\text{обр}}), \tag{3}$$

т. е. интенсивности входного потока собираемых данных и сообщений λ, старения собранных данных и сообщений S, построения структуры оперативной обработки (m числа фаз и n каналов сбора и обработки), организационно-технических возможностей (интенсивности обработки μ) и среднего времени обработки Тобр.

Допустимое время оперативной обработки сообщений и данных определяется динамикой сбора необходимой информации и процессов обработки. Число фаз и каналов обработки определяется ее структурой. Функции распределения допустимого времени оперативной обработки *m*-фазной системой обработки выражается формулой [7]:

$$F(t_{\text{обр}}) = 1 - \sum_{i=1}^{m} \exp(-\alpha_i t_{\text{обр}}) \prod_{i \neq j}^{m} \frac{\alpha_j}{\alpha_j - \alpha_i}, \tag{4}$$

где $\alpha_i = \mu_i n_i - \lambda_{\text{вх}\,i}$, λвхі – интенсивность входного потока данных и сообщений на каждую из фаз обработки; μі – интенсивность обработки в і-й фазе; j – номер фазы обработки.

В ходе обработки старение собранных данных и сообщений происходит объективно, а интенсивность старения есть величина, обратная времени, необходимого для принятия решения.

При экспоненциальном законе старения собранных данных и сообщений о критической ситуации с интенсивностью *S* вероятность своевременной обработки будет:

$$P_{\text{реш}}(t) = \int_0^{\infty} \exp(-S \cdot t_{\text{обр}}) \mathrm{d}F(t_{\text{обр}}). \tag{5}$$

Подставив (4) в (5), получим:

$$P_{\text{реш}}(t) = \int_0^{\infty} \exp(-S \cdot t_{\text{обр}}) \left[ \sum_{i=1}^{m} \alpha_i \exp(-\alpha_i t_{\text{обр}}) \prod_{\substack{i \neq j \\ j=1}}^{m} \frac{\alpha_j}{\alpha_j - \alpha_i} \right] \mathrm{d}t_{\text{обр}}. \tag{6}$$

Преобразовав выражение (6) окончательно получаем вероятность того, что время затрачиваемое на принятие решения по критической ситуации, не превысит допустимого:

$$P_{\text{реш}} = \prod_{i=1}^{m} \alpha_i \sum_{i=1}^{m} \frac{1}{(\alpha_i + S) \prod_{\substack{j=1 \\ j \neq i}}^{m} (\alpha_j - \alpha_i)}. \tag{7}$$

**Размер системы** можно определять на основе количества выполняемых операций; количества организаций; количества людей, участвующих в спецификации системы; количества подсистем; количества интерфейсов.

**Сложность системы** можно определять на основе количества переменных; степени независимости переменных; количества баз данных и возможности их обновления; логической сложности; степени динамичности.

## Выводы

1. Системы беспроводных телекоммуникаций стали глобальными и покрывают значительные (до 90%) территории развитых стран. Кроме того, беспроводные телекоммуникационные технологии стали доступны каждому члену общества и охватывают до 85% населения практически любой страны.

2. В силу перечисленных обстоятельств они становятся привлекательными для злоумышленных действий со стороны террористических организаций и организованных преступных группировок.

Реализованные угрозы с их стороны и негативные информационные воздействия на социальные объекты и группы могут привести к возникновению серьезных критических ситуаций в национальном масштабе.

3. Для своевременного выявления этих угроз и негативных информационных воздействий и их нейтрализации необходима разработка и реализация комплекса организационных и научно-технических мероприятий по противодействию. В основе этих мероприятий лежит создание единой системы радиочастотного и сетевого мониторинга, объединенного со СППР.

4. Основной функцией данной интеллектуальной системы будет выявление по ряду косвенных и прямых признаков возможных угроз и негативных воздействий на телекоммуникационные сети и социальные объекты, а также выработка мер по их своевременной нейтрализации.

5. Для реализации этих возможностей СППР должна иметь определенную структуру и возможности. В данной работе определены структура и основные требования к системе поддержки принятия решений и ее основным элементам. В частности, в подсистеме радиочастотного мониторинга должна быть обеспечена возможность распознавания и анализа сигналов и их декодирование. В самой СППР должна быть обеспечена возможность анализа и интерпретации текстовых сообщений для выявления негативных информационных воздействий.

*Литература*: ***1.*** *Семенюченко А. В. IPS – современные технологии обнаружения и предотвращения атак // «IT спец», журнал для IT – профессионалов. – 2007.-№5. – с.46 – 55.* ***2.*** *Зайцев О. Н. Oracle – безопасность сервера // «IT спец», журнал для IT – профессионалов. – 2007.-№11. – с.46 – 50.* ***3.*** *Джексон П. Введение в экспертные системы. Пер с англ.: Учебное пособие – М.: Издательский дом «Вильямс», 2001. – 624 с.* ***4.*** *Информационно-вычислительные системы принятия решений / В. В. Хаджинов, В. А. Быков, И. А. Храмова, В. Г. Усачев – Киев: Наукова думка, 1992. – 140 с.* ***5.*** *Человеко-машинные системы принятия решений с элементами искусственного интеллекта / Б. М. Герасимов, В. А. Тарасов, И. В. Токарев – Киев: Наукова думка, 1993.– 184 с.* ***6.*** *Горелик А. Л., Скрипкин В. А. Методы распознавания. Уч. пособие для вузов. – М.: Высшая школа, 1977. – 222 с.* ***7.*** *Хореев А. А. Теоретические основы оценки возможностей технических средств разведки: Монография. М.: МО РФ, 2000. – 255 с.*

**УДК 511.215**

# РАЗРЯДНЫЙ ПОДХОД К ФАКТОРИЗАЦИИ ЧИСЛА – ПРОИЗВЕДЕНИЯ ДВУХ ПРОСТЫХ ЧИСЕЛ

***Артём Жилин***

*Институт специальной связи и защиты информации НТУУ «КПИ»*

*Анотація:* **Розглянуто розрядний підхід до факторизації чисел, який за допомогою функції nat(a) зводиться до рішення системи рівнянь, яка має вид поліномів Жегалкіна. Для рішення системи рівнянь запропоновано «ваговий» підхід із нормалізацією системи рівнянь.**

*Summary:* **The bit going is considered near factorization of numbers, which is taken by the entered function of nat(a) to the decision of the system of equalizations, having the appearance of Zhegalkin's polynomials. For the decision of the system of equalizations «gravimetric» approach is offered with normalization of the system of equalizations.**

*Ключевые слова:* **Факторизация, система булевых уравнений, «весовой» подход.**

## I Введение

Концепция асимметричных криптосистем (криптографии с открытым ключом) была предложена Уитфилдом Диффи и Мартином Хеллманом [1]. Основным пунктом концепции было предложение использовать ключи парами, состоящими из ключа зашифрования и ключа расшифрования, которые невозможно вычислить один из другого.

Как правило, алгоритмы, используемые для реализации асимметричных криптосистем, основываются на решении одной из трудных математических задач. Классическим примером такой задачи является факторизация (разложение на простые множители) большого числа. В частности, на этой задаче основан один из самых известных криптоалгоритмов - RSA.