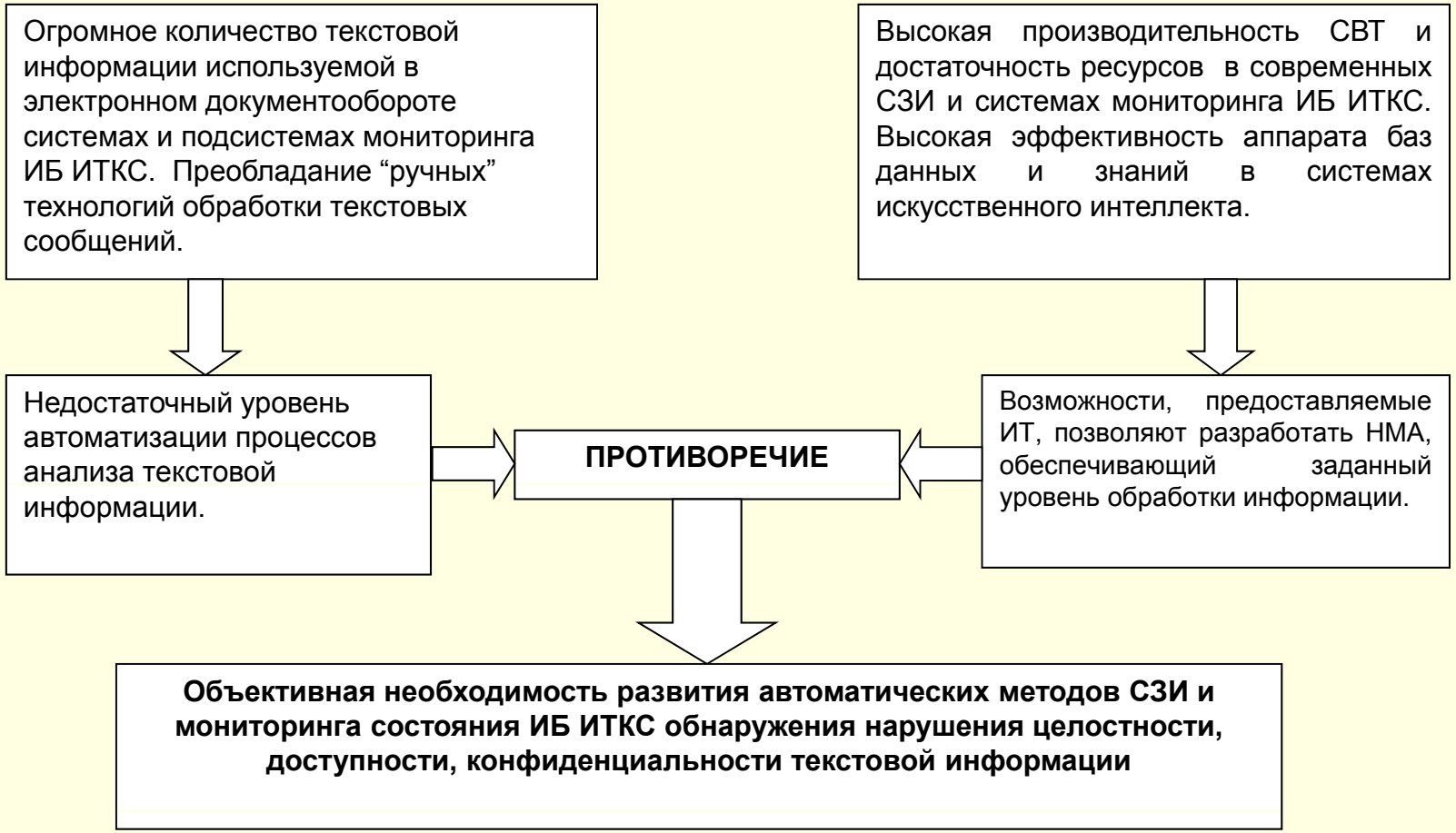
Методология обнаружения угроз нарушения информационной безопасности в открытых компьютерных сетях на основе функциональной модели естественного языка

Специальность: 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность



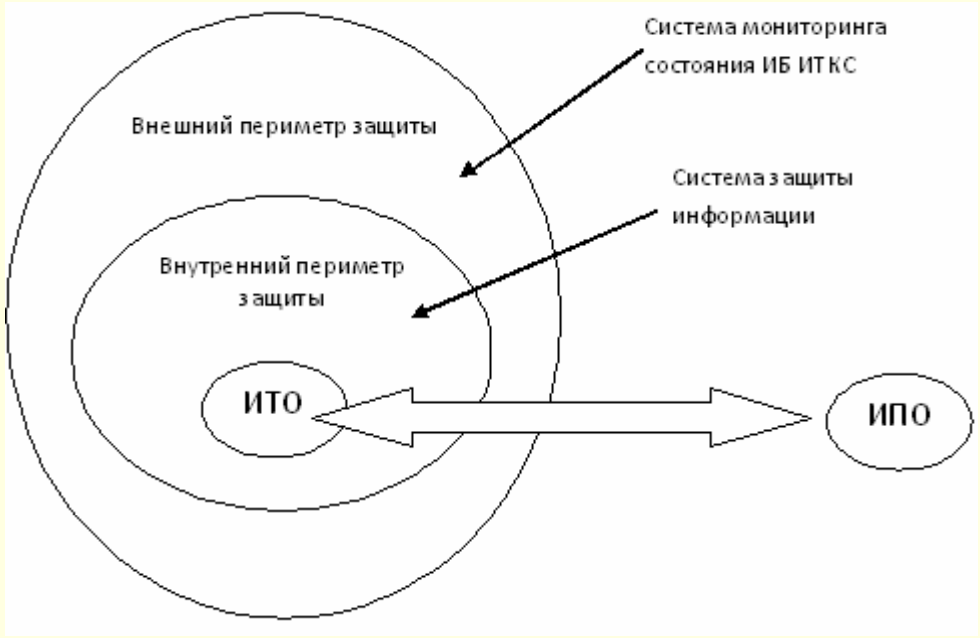
Объект и предмет исследования

- Системы мониторинга состояния информационной безопасности, обрабатывающие предметно ориентированные ЕЯ тексты и сообщения в ИТКС

- Методы и средства обнаружения и противодействия угрозам нарушения информационной безопасности, основанные на обработке и анализе текстов документов

Особенности объекта и предмета исследования

- 1.**Направление**:
  - Защита информации
  - Защита от информации
- 2.**Объект угрозы**:
  - ИТО ИТКС
    - Механизмы управления
    - Ресурсы
    - Структуры
  - ИПО ИТКС
    - Механизмы управления
    - Ресурсы
    - Структуры
- 3.**Средство осуществления угрозы ИБ**
  - Текстовая информация



Научная проблема

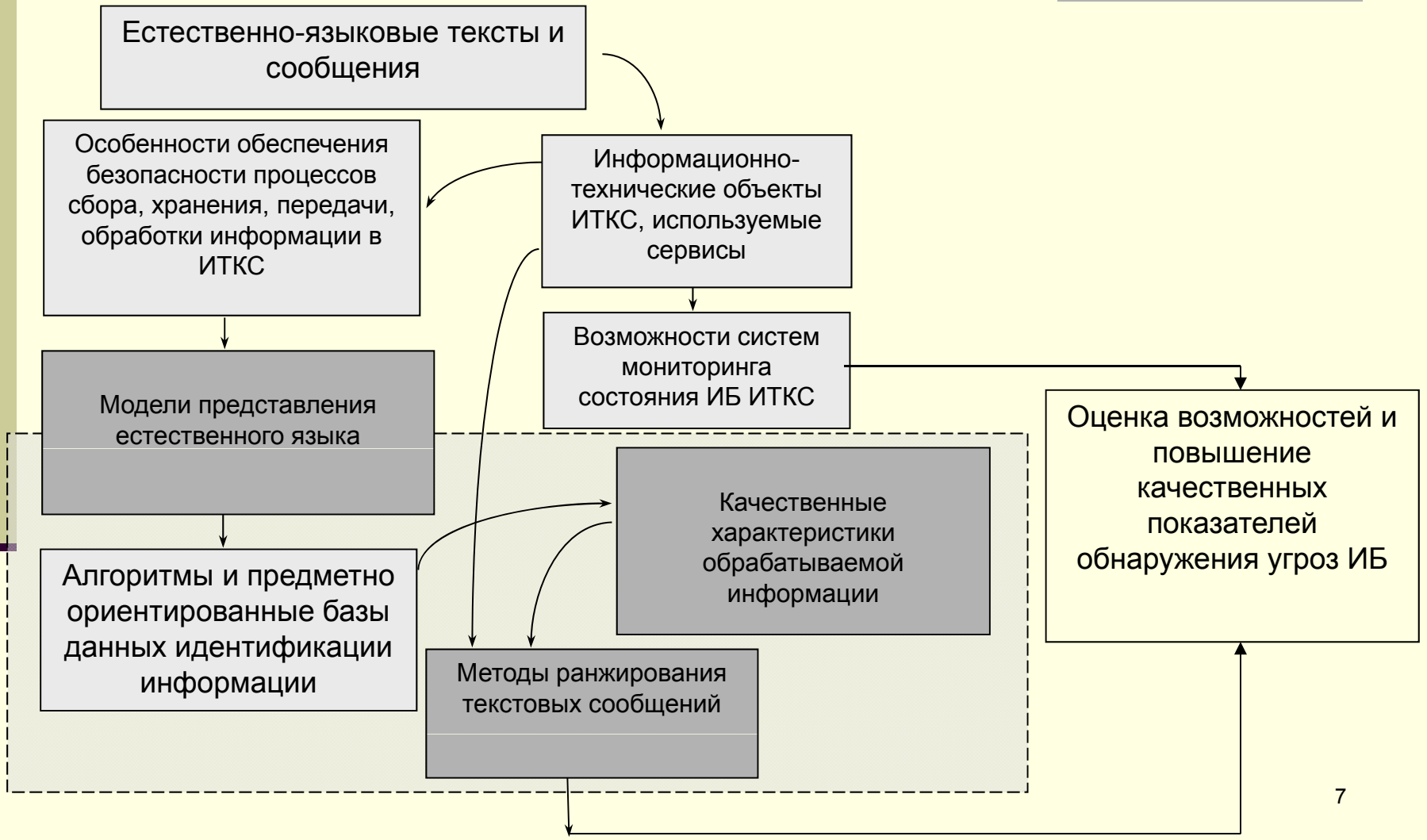
Обоснование и разработка теоретических основ математического и программного обеспечения СЗИ и мониторинга состояния ИБ ИТКС, выявляющих угрозы нарушения конфиденциальности, целостности, доступности, основанных на автоматизации процессов вычисления данных и фактов из текстов документов, с использованием проблемно ориентированной функциональной модели естественного языка

Цель работы

- **Теоретическая** - разработка, развитие аналитических методов, применяемых в системах мониторинга СЗИ, для обработки и вычисления информации ЕЯ текстов с целью обнаружения и противодействие угрозам нарушения информационной безопасности, отличающихся от известных использованием функциональности семантико-грамматических связей между словами, позволяющих осуществлять более качественный анализ конструкций естественного языка.

- **Прагматическая** - повышение показателей защищенности информации, вероятности обнаружения угроз ИБ за счет увеличения качественных характеристик идентифицируемых ЕЯ конструкций при автоматизации процессов вычисления информации текстов предметной области в системах мониторинга состояния ИБ ИТКС.

Сущность проблемы



Формальная запись научной проблемы:

Найти $\mathbf{M}_m : Q \to Q', D \to D'$

$$\forall q'\left(q' \in Q'\right) \quad \forall d'\left(d' \in D'\right)$$

такие, что

$$\exists\left(\widehat{I} = \widehat{I}\left\{\mathbf{M}, H, q, q', d, d', \Delta I\right\}\right)$$

при

$$\left\|I - \widehat{I}\right\| \Rightarrow \Delta I_{\min}$$

$$M : T \xrightarrow{F} O$$

Основные направления исследования (1)

Направление информационной безопасности: определяет основополагающие направления защиты информации и защиты от информации в ИТКС и глобальных вычислительных сетях, связанные с ними качественные показатели.

Направление контроля информационных потоков: нацелено на поддержку контроля технических каналов утечки конфиденциальной информации

Направление математической лингвистики: связано с разработкой моделей представления естественного языка, методов и алгоритмов обработки и вычисления естественно-языковых конструкций, направленных на достижение заданных качественных показателей СЗИ и систем мониторинга ИБ

Системное направление: позволяет повысить качественные характеристики систем мониторинга состояния ИБ ИТКС и СЗИ обнаружения и идентификации угроз ИБ на основе функциональной модели естественного языка,

Основные направления исследования (2)

Методика определения характеристик для СЗИ информационно-технических объектов, обрабатывающих текстовую информацию

Система моделей, методов, методик для обнаружения и предотвращения угроз нарушения информационной безопасности при контент анализе текстов открытых источников компьютерных сетей, основанная на применении модели естественного языка

Комплекс методов, определяющий состав морфологического уровня обработки ЕЯ сообщений СЗИ, позволяющих повысить устойчивость алгоритмов функциональных компонент анализа текстовой информации

Концепция построения методов и моделей мониторинга потоков текстовой информации ИТКС, основанная на идентификации информационных объектов текстовой информации.

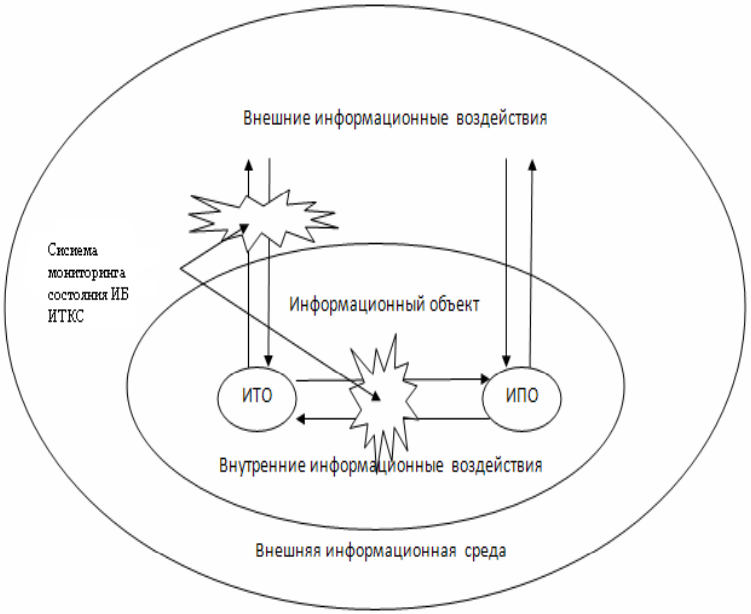
Комплекс методик и моделей активного аудита текстовых источников открытых компьютерных сетей, содержащих угрозы нарушения ИБ, основанный на построении специализированных объектов естественно-языковых конструкций

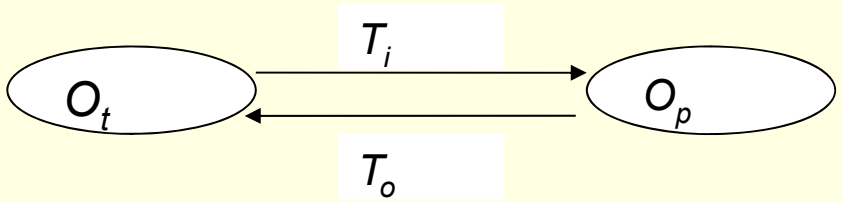
Методика определения характеристик для СЗИ ИТО (1)

Краткая характеристика:

- **Цель:**
  - Повышение точности определения наиболее уязвимых узлов ИТО
  - Обоснование ТТХ СЗИ и систем мониторинга состояния информационной безопасности
- **Подходы к решению:**
  - Моделирование поведения потенциального нарушителя
  - Вероятностные оценки информационного воздействия

Методика определения характеристик для СЗИ ИТО (2)





$$M=<O_t, O_p, T_i, T_o>$$

O_t – множество информационно-технических объектов(ИТО),

O_p – множество информационно-психологических объектов(ИПО),

T_i – входные информационные потоки текстовой информации

T_o – выходные информационные потоки текстовой информации.

$$O_t \rightarrow Z_o;\ Z_o \rightarrow Tz_o;$$
$$O_t \rightarrow I_o;$$
$$O_t \rightarrow S_o;$$
$$O_t \rightarrow < Tz_o, I_o, S_o >$$

Zo – система защиты информации

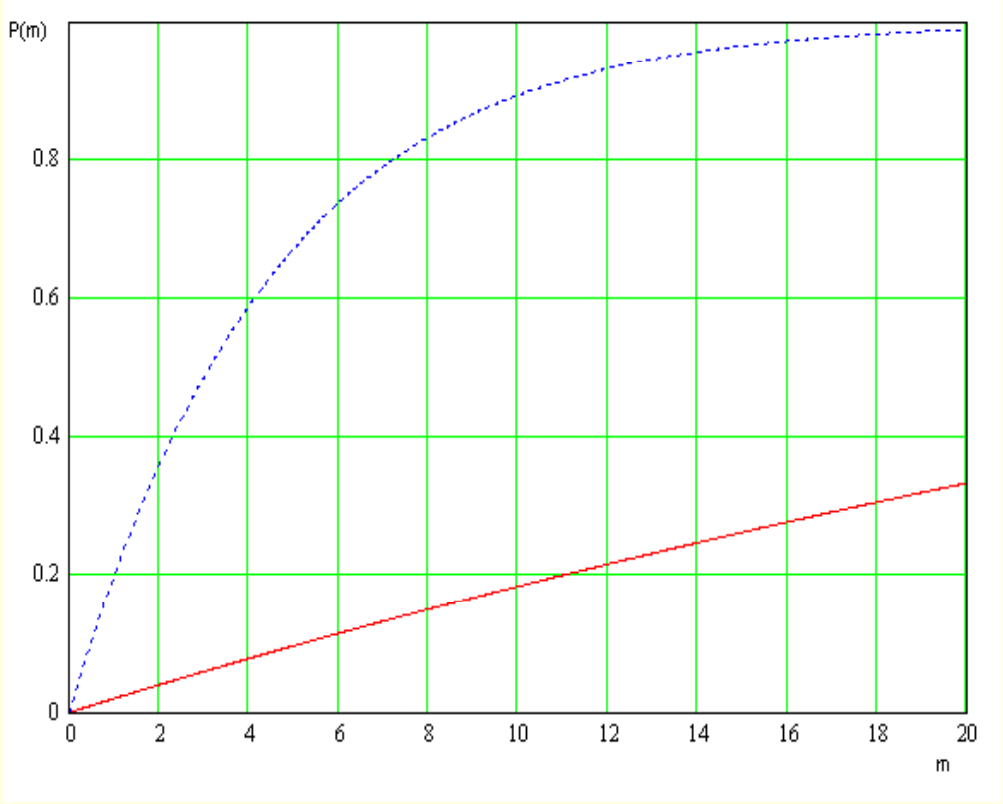
Tzo – характеристики системы защиты информации

Io - характеристики целевой аудитории

So – характеристики предоставляемых сервисов

Методика определения характеристик для СЗИ ИТО (3)

Вероятность возникновения события оказания влияния на ИПО



$$P = P(A)P(B \mid A)P(C \mid AB)$$

$$p_o = \prod_{i=1}^{n} p_i$$

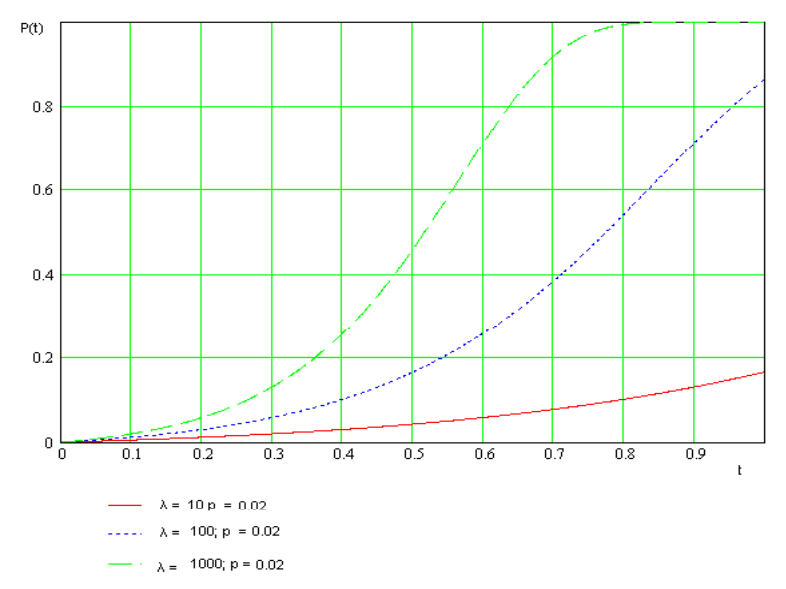
$$p = 1 - \prod_{j=1}^{m} (1 - \prod_{i=1}^{n} p_i)$$

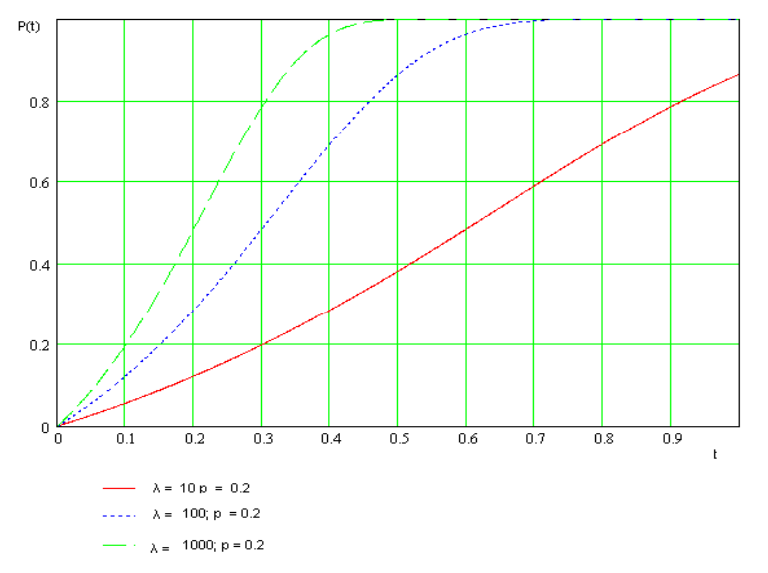
$$p = 1 - (1 - p_o)^m$$

Методика определения характеристик для СЗИ ИТО (4)

Зависимость вероятности информационного воздействия от интенсивности поступления потенциально опасных сообщений

$N = n(t)$ $\quad n(t) = \lambda^{t} - 1 \quad p(t) = 1 - (1 - p_0)^{\lambda^{t}-1}$





Методика позволяет:

- Обосновывать требуемые качественные показатели, определяющие характеристики обнаружения угроз ИБ СЗИ и системами мониторинга
  - *частота модерации ИТО ИТКС*
  - *уровень накапливаемых немодерируемых сообщений*
- Определять наиболее уязвимые сервисы и элементы ИТО ИТКС
- Вырабатывать рекомендации и определять комплекс мероприятий по достижению заданной вероятности устранения угрозы

Обнаружение угроз нарушения ИБ на основе на применении модели ЕЯ

Краткая характеристика:

- **Цель:**
  - Повышение вероятности обнаружения потенциально опасных сообщений
  - Повышение показателей качества СМПО СЗИ и систем мониторинга состояния ИБ
- **Подходы к решению:**
  - Адаптация к особенностям специфических текстовых конструкций
  - Повышение устойчивости алгоритмов СМПО СЗИ и систем мониторинга состояния ИБ

Обнаружение угроз нарушения ИБ на основе на применении модели ЕЯ

- Z_o – система защиты информации / система мониторинга состояния ИБ ИТКС
- Tz_o – характеристики системы защиты информации
- Uz_o - уязвимости функциональных характеристик СМПО

$$Z_o = <Tz_o , Uz_o >$$

Адаптированная модель естественного языка

Морфологический уровень

Синтаксический уровень

Семантический уровень

СГТ ППФ, где K_i =17
+
СГТ отдельных частей речи

Синтаксический предикат
Sint(A_1,…,A_n)
A_i - морфологическая информация
+
Система приоритетов для сборки конструкций

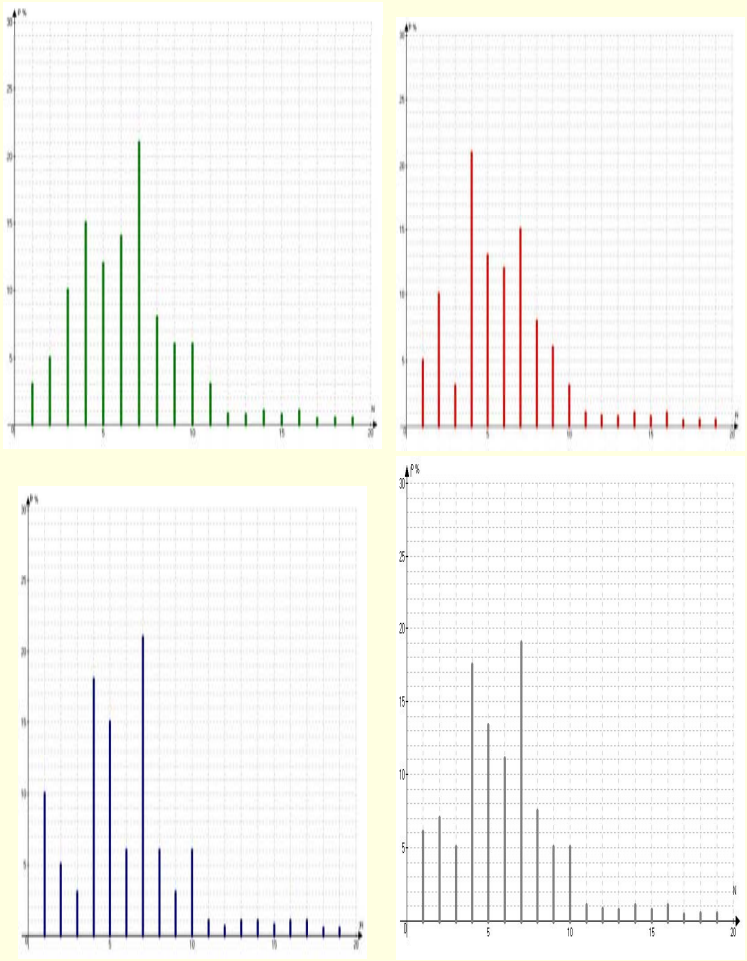
M=<W,Si,Ks>

W- множество словоформ

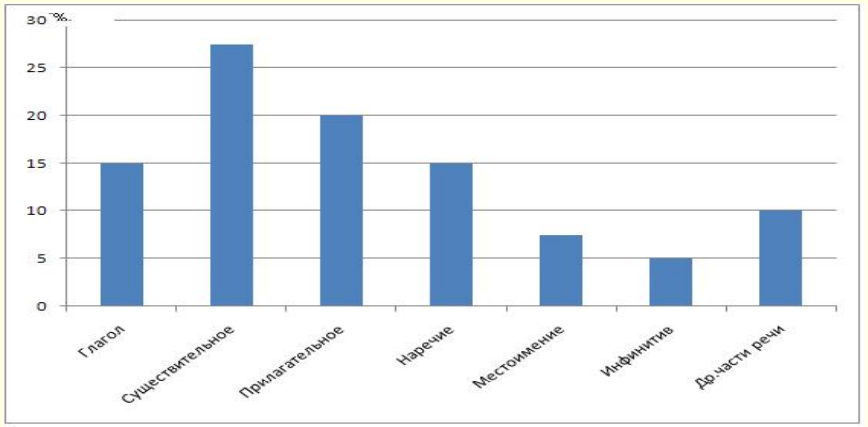
Si- множество синтаксических шаблонов

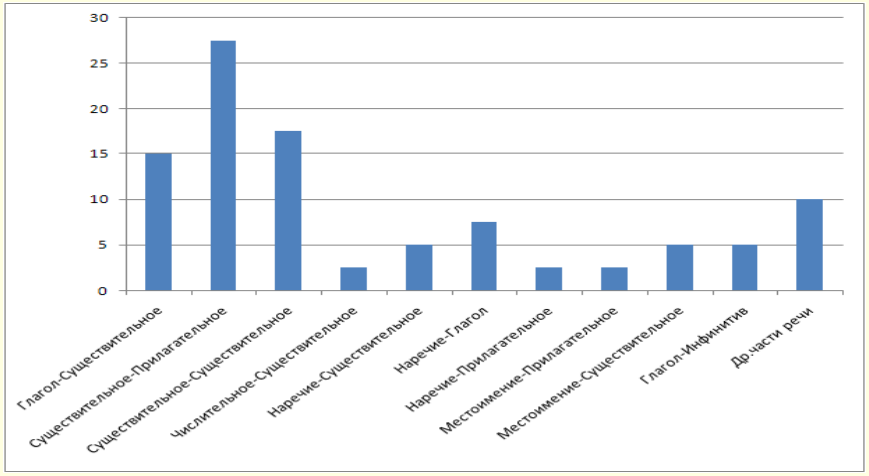
Ks- множество классов

Статистические особенности конструкций ЕЯ в комментариях



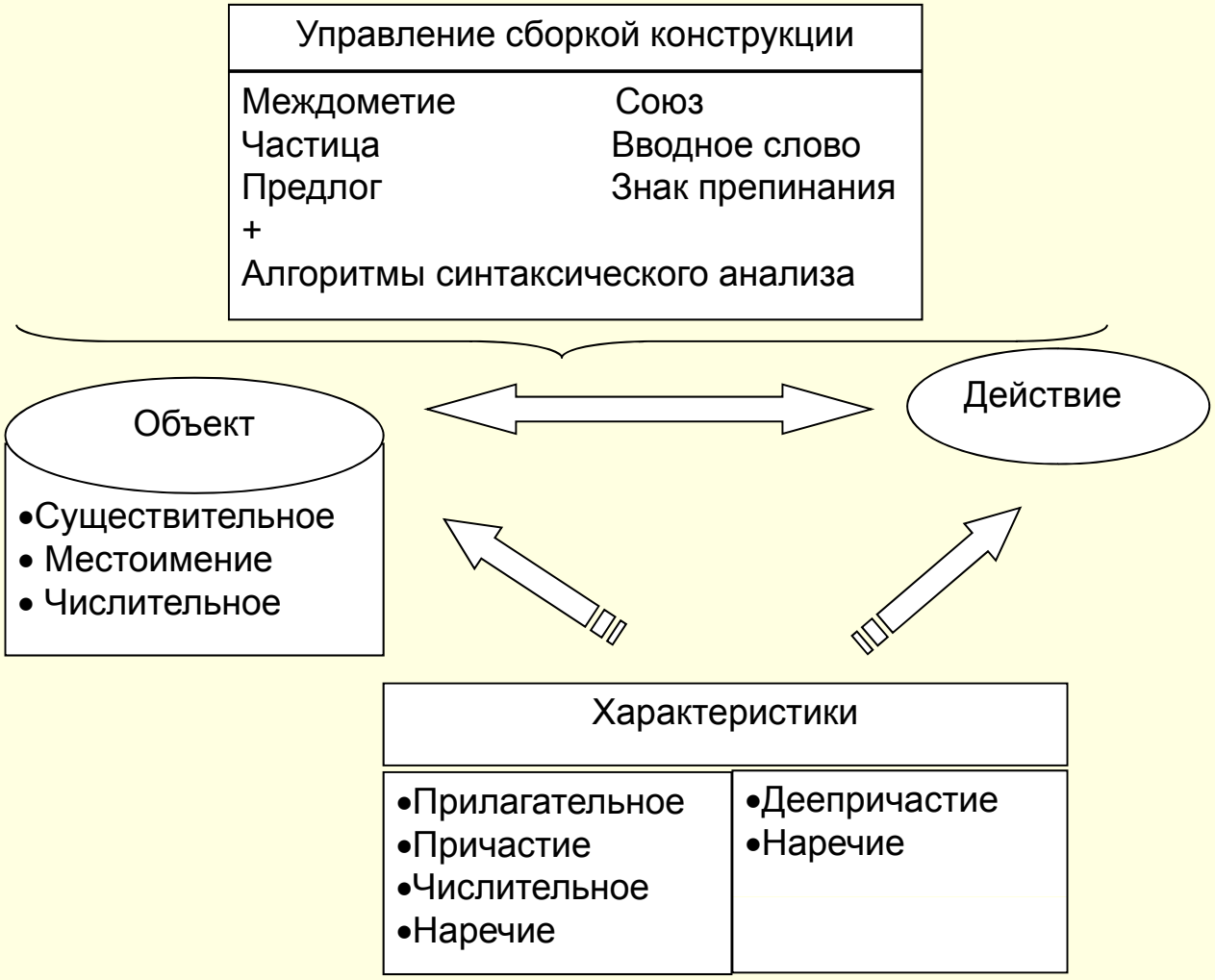
Распределение количества слов в предложениях комментариев пользователей





Распределение частей речи в предложениях комментариев пользователей

Универсальная структура представления естественного языка



M=<W,H>

где *W* - множество словоформ

H – характеристики

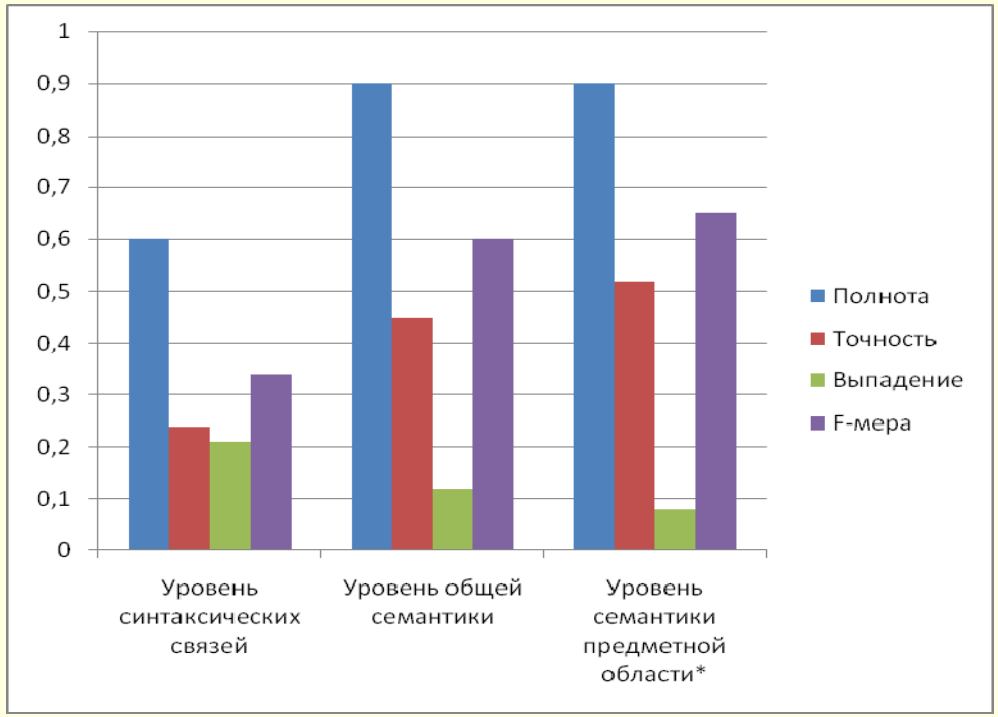
H={O|D|C}

O - объект

D - действие

C={Co,Cd} – характеристики объектов и действий

Результаты оценки показателей качества



$$R = \frac{H}{D} \qquad P = \frac{H}{N}$$

$$O = \frac{N - H}{N}$$

$$F = \frac{2PR}{P + R}$$

H - извлеченные релевантные документы,

D - общее число найденных документов,

N – общее число релевантных документов в выборке.

Применение моделей позволяет:

- Производить адаптацию систем мониторинга состояния ИБ ИТКС и СЗИ под особенности видов текстовых сообщений
- Уменьшать вычислительные затраты при обработке текстовой информации
- Повышать качественные характеристики обнаружения угроз СЗИ и системами мониторинга, анализирующими текстовую информацию
- Снижать трудоемкость создания предметно ориентированных баз данных
- Осуществлять настройку словарных БД, используемых при предметно-ориентированной обработке ЕЯ

Определение состава морфологического уровня обработки ЕЯ сообщений СЗИ(1)

Краткая характеристика:

- **Цель:**
  - Повышение качественных показателей защищенности исходя из специфических характеристик обрабатываемой СЗИ текстовой информации в условиях внешних ограничений
- **Подходы к решению:**
  - Определение влияния природы ЕЯ на реализацию уровней обработки в условиях внешних ограничений
  - Обоснование использования различных видов обработки
- **Результаты:**

Определение состава морфологического уровня обработки ЕЯ сообщений СЗИ(2)

Пусть a_i – коэффициент полезности (эффективности) элемента СЗИ,

b_i – требования элемента СЗИ к вычислительным ресурсам.

Тогда внутри уровня обработки ЕЯ

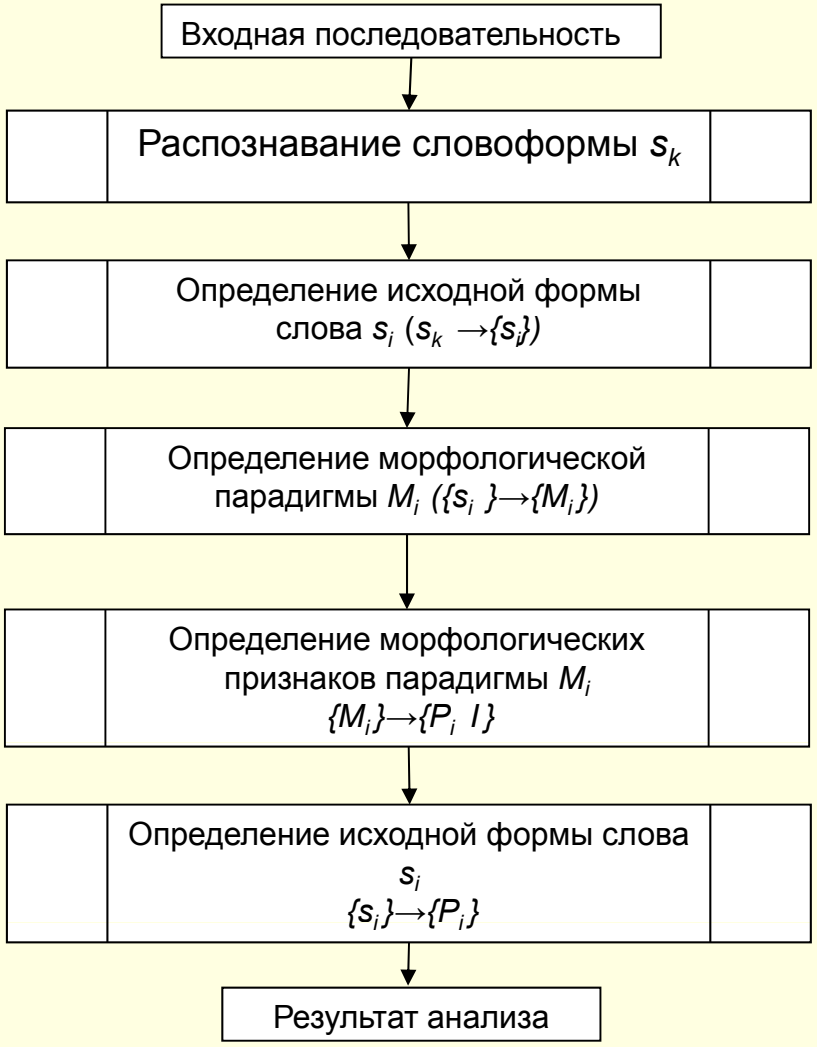
$$\begin{cases} \sum_{i=1}^{n} a_i x_i \rightarrow \max \\ \sum_{i=1}^{n} b_i x_i \le B \\ x_i = \{0;1\} \end{cases}$$

$$R(ma) = \sum_{A \in T} \sum_{B \in T} \lambda_{AB} P_A P_{AB}; \quad P_A = P_a + P_s.$$

$$R(ma) = \sum_{A \in T} \sum_{B \in T} \lambda_{AB} (P_a + P_s) P_{AB}$$

$$R(ma) = \sum_{A \in T} \sum_{B \in T} \lambda_{AB} P_s P_{AB}$$

Морфологический анализатор



$$S = \{S_i\},\ i = \overline{1,n} \qquad M = \{M_j\},\ j = \overline{1,t}$$

$$B = \{B_l\},\ l = \overline{1,p} \qquad c = \{c_r\},\ r = \overline{1,z}$$

$$S \xrightarrow{f} M \qquad M \xrightarrow{g} S$$

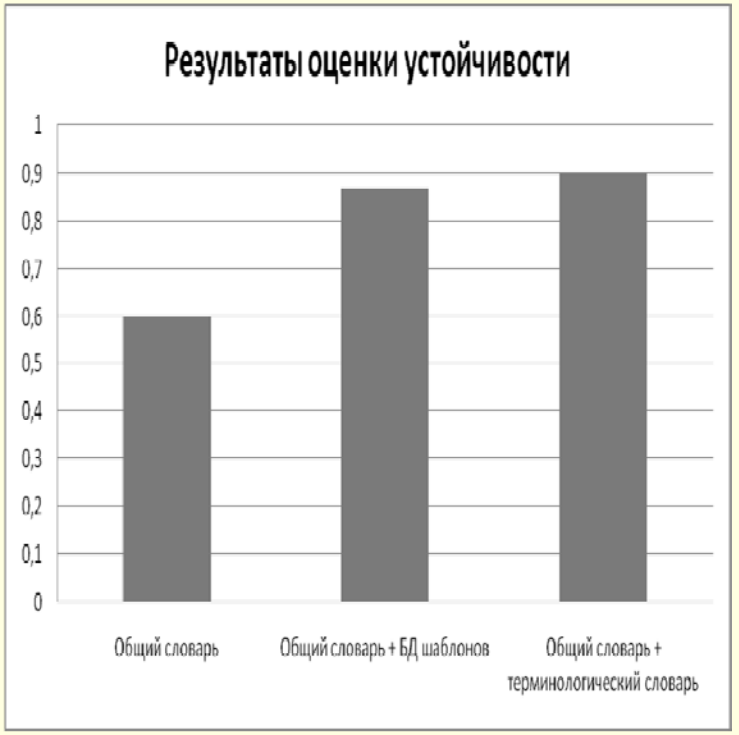
$$f_k : s_k \subset M_k = B_l + C_r$$

$$\{B_l\} = s_k - \{c_r\}$$

$$B_l \rightarrow S_k \qquad S_k \xrightarrow{f} M_k$$

$$g_k : M_k \rightarrow S_k$$

Устойчивость алгоритмов



Результаты

- Повышение устойчивости обработки текстовой информации за счет выявления специфических конструкций и их особенностей, направленных на использование уязвимостей СЗИ
- Повышение показателей качества обнаружения потенциально опасных сообщений потоков текстовой информации
- Обеспечение заданной надежности алгоритмов и СМПО СЗИ и систем мониторинга состояния ИБ ИТКС
- Оптимизация состава средств обнаружения угроз ИБ

Мониторинг потоков текстовой информации ИТКС(1)

Краткая характеристика:

- **Цель:**
  - Повышение качественных показателей систем мониторинга состояния ИБ при внешней обработке ЕЯ конструкций
  - Снижение вычислительной сложности обработки текстовой информации
- **Подходы к решению:**
  - Создание системы приоритетов обработки ОЕЯ
  - Использование масштабируемых предикатов

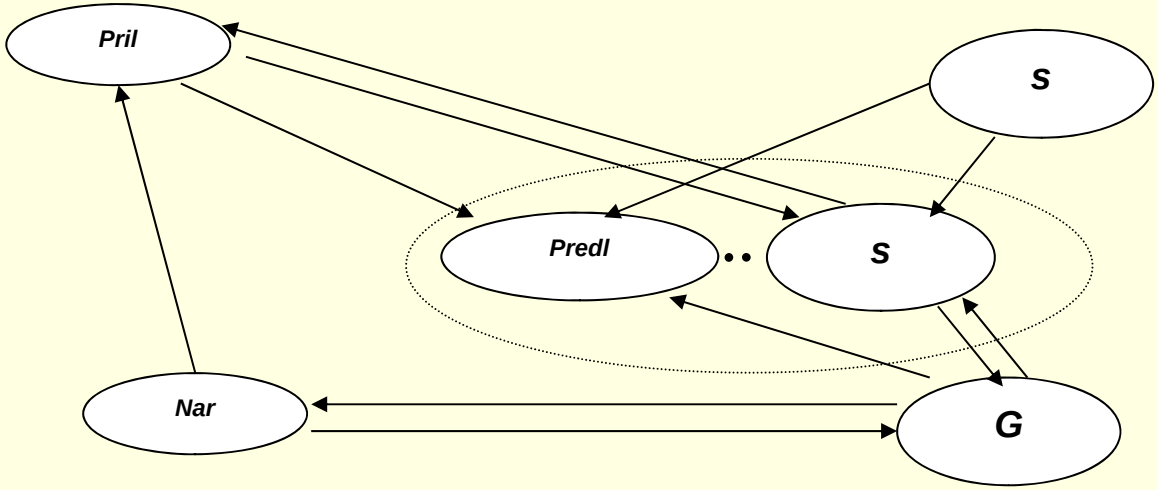
Мониторинг потоков текстовой информации ИТКС (2)

- Z_o – система мониторинга состояния ИБ ИТКС
- Tz_o – характеристики множества функциональных компонент систем мониторинга состояния ИБ ИТКС

$$Z_o \rightarrow <Tz_o>$$

$$Tz_o : R \rightarrow \{H_o, H_1\}$$

Связи конструкции словоформ сообщения

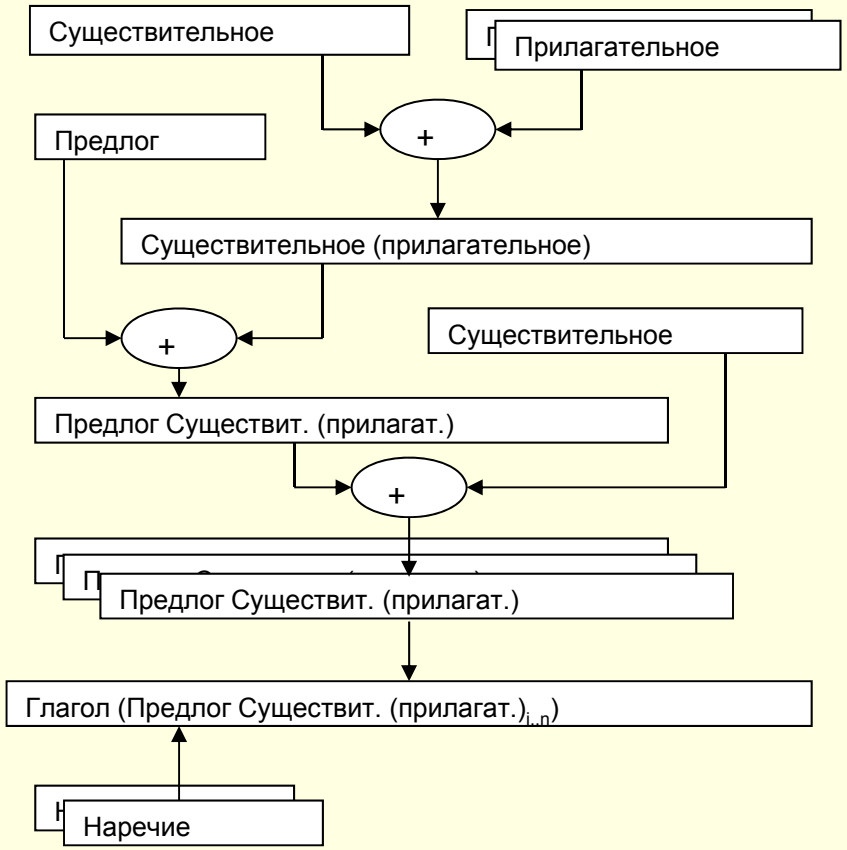


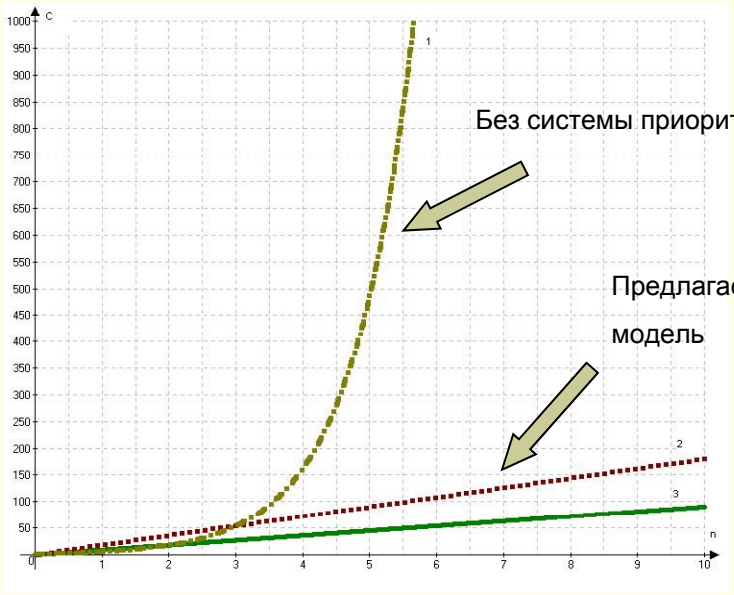
$W\ (a_i \rightarrow f_i)$

```
G(Z1:!Им {K1} g, Z2:!Род{K2} g, Z3:!Дат{K3} g,
  Z4:!Вин{K4} g, Z5:!Тв{K5}  g, Z6:!Пред{K6} g)

S(Z1:!Род, Z2:!Дат, Z3:!Вин, Z4:!Тв, Z5:!Пред)
```

Алгоритмическая последовательность свертки предложения ОЕЯ





Зависимость количества сравнений от числа слов сообщения:

1 – Семантическая модель без системы приоритетов.

2 – Семантическая модель с системой приоритетов.

3 – Синтаксическая модель.

Результаты

- Использование функциональных особенностей ЕЯ конструкций при вычислении семантики выражений для обнаружения потенциально опасных сообщений
- Создание специализированных БД для оценки эмоционального фона сообщения, находящегося на ИТО с целью анализа информационного воздействия
- Автоматизация вычисления пространственно-временных характеристик ЕЯ конструкций для построения предметно ориентированных БД
- Уменьшение вычислительной сложности алгоритмов обработки ЕЯ информации

Активный аудит текстовых источников открытых компьютерных сетей(1)

Краткая характеристика:

- **Цель:**
  - Повышение точности вычисления ИТО, требующих мониторинга состояния ИБ
- **Подходы к решению:**
  - Вероятностные оценки нахождения потенциально опасных сообщений
  - Использование структур информационных объектов для обучения системы

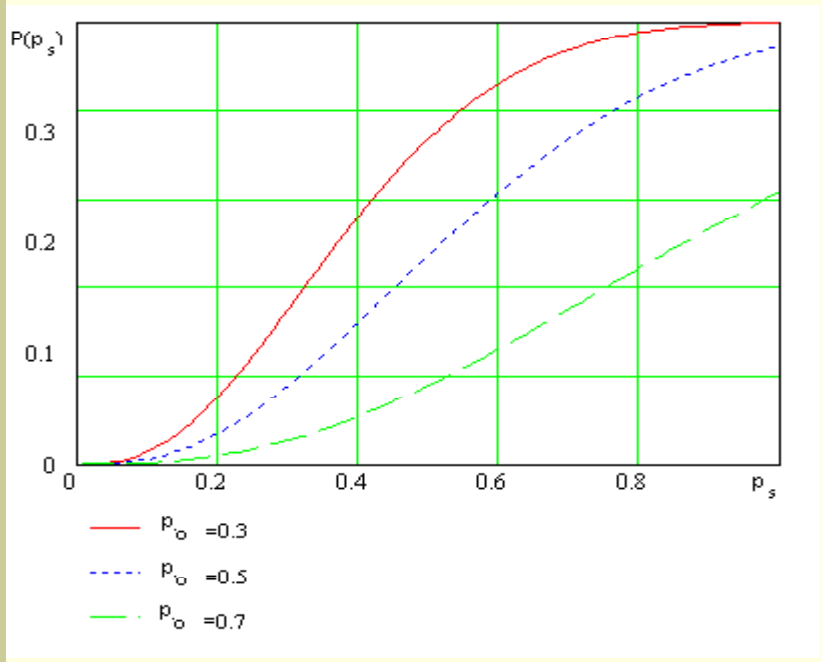
Активный аудит текстовых источников открытых компьютерных сетей(2)

$$R = G(p,Q)$$

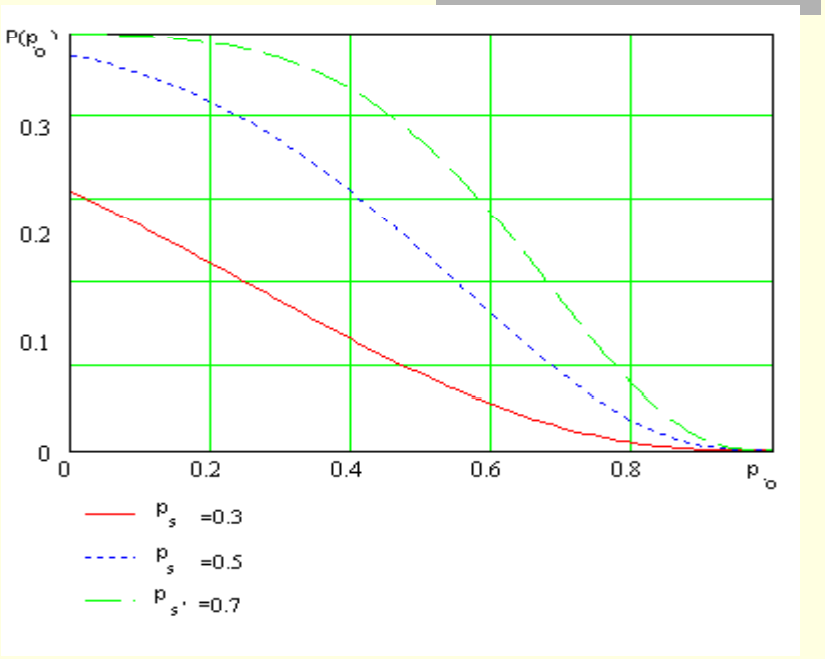
p – вероятностные характеристики

Q – обучение системы

Ранжирование ИТО



Вероятность содержания *m=3* и более потенциально опасных сообщений в ИТО, включающего в себя *n=10* ресурсов в зависимости от вероятности появления потенциально опасных сообщений, при вероятности обнаружения СЗИ 0.3,0.5,0.7



Вероятность содержания m=3 потенциально опасных сообщений в ИТО, включающего в себя n=10 ресурсов в зависимости от вероятности обнаружения СЗИ потенциально опасных сообщений, при вероятности

появления потенциально опасных сообщений 0.3,0.5,0.7

$$\mathrm{p_p} = p_s q_o \qquad \mathrm{p_p} = p_s(1-p_o)$$

$$\mathrm{p} = \sum_{m=k}^{n} \mathrm{C_n^m}\, p_p{}^m (1-p_p)^{n-m} \qquad \mathrm{p} = \sum_{m=k}^{n} \frac{n!(p_s(1-p_o))^m (1-p_s(1-p_o))^{n-m}}{(n-m)!m!}$$

Построение информационных объектов

$$O=\{I,Pr,Atr,Do,Du\};$$

где $I=H(Y)$; - идентификатор объекта

$s_m \rightarrow Pr$ - признак объекта

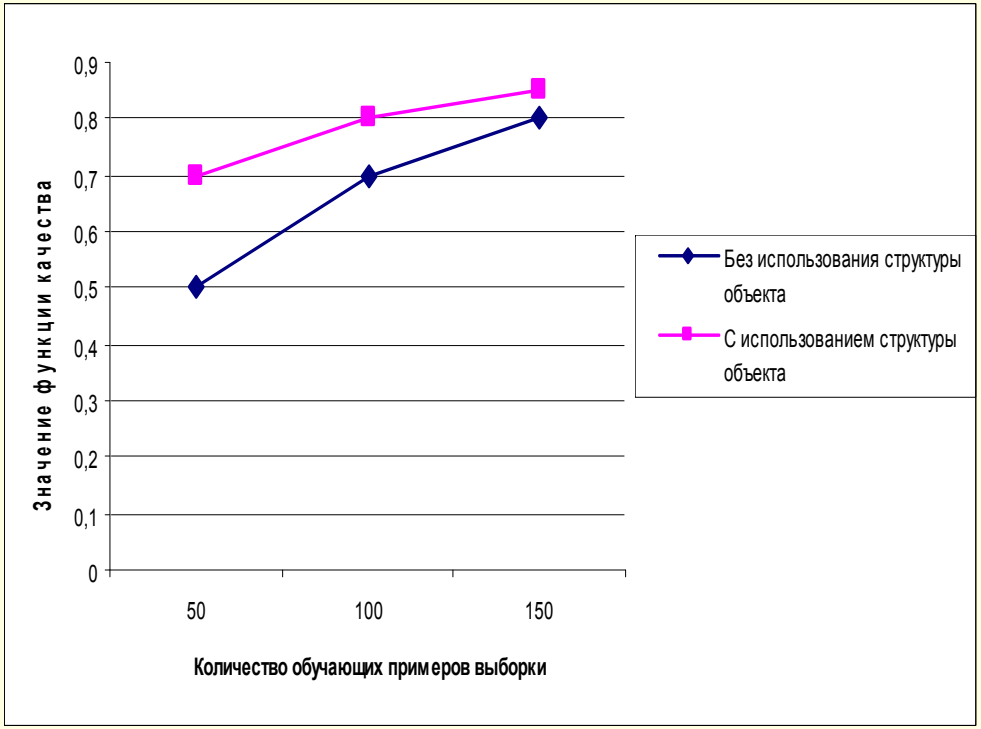
$s_p \rightarrow Atr$ - атрибут объекта

$s_f \rightarrow D_o, D_u$ – действия над объектом и объекта

объект может быть использован в моделях извлечения фактов и в моделях обучения.

Информация [ВЛАДЕЛЕЦ:] системы
Информация [ОБЪЕКТ:] о системе

Качественные показатели обучения системы



$$R_i = \frac{h_i}{d_i} \qquad P_i = \frac{h_i}{n_i} \qquad f_i = \frac{2h_i}{n_i + d_i}$$

$$F = \frac{1}{m} \sum_{i=1}^{m} \frac{2h_i}{n_i + d_i}$$

h – количество правильных извлечений

n – количество извлечений найденных системой

d – количество релевантных извлечений в выборке

Результаты

- Повышение вероятности обнаружения информационных объектов, подвергающихся информационным угрозам.
- Осуществление контроля за открытыми ресурсами ИТКС
- Исследование информации ресурсов сети с целью информационного противодействия различным видам утечек информации, корпоративному шпионажу и бизнес-разведке
- Распознавание компонентов текстовых сообщений ИТО, содержащих элементы возможных угроз ИБ

Основные результаты(1)

1.Методика определения характеристик для СЗИ информационно-технических объектов, обрабатывающих текстовую информацию, основанная на модели обеспечения ИБ потоков ИТКС **отличается от известных,** базирующихся на аналитических подходах, использованием вероятностных оценок информационного воздействия текстовых сообщений ресурсов открытых вычислительных сетей, что позволяет определить необходимые качественные показатели для систем мониторинга состояния ИБ и СЗИ ресурсов.

Основные результаты(2)

2. Система моделей, методов, методик для обнаружения и предотвращения угроз нарушения информационной безопасности при анализе текстов открытых источников компьютерных сетей, основанная на применении модели естественного языка, **отличается от известных,** базирующихся на аналитических подходах, использованием в описаниях словоформ масштабируемых предикатов связей, аргументы которых содержат информацию о морфологических характеристиках и семантико-грамматических типах присоединяемых слов, что позволяет увеличить вероятность обнаружения конфиденциальной информации системами анализа контента за счет унификации описания, упрощения структуры ЕЯ базы данных без существенных потерь показателей полноты и точности при вычислении объектов текстовой информации.

Основные результаты(3)

3. Комплекс методов, определяющий состав морфологического уровня обработки ЕЯ сообщений СЗИ, позволяющих повысить устойчивость алгоритмов функциональных компонент анализа текстовой информации, **отличается от известных**, использующих аналитические подходы, вычислением информации на основе характеристик, содержащихся в БД описаний словоформ для анализа возможностей соединения слов, что позволяет определять идентификаторы связей между словами, и, как следствие, повысить точность распознавания данных с целью уменьшения вероятности преодоления защиты.

Основные результаты(4)

4. Концепция построения методов и моделей мониторинга потоков текстовой информации ИТКС, основанная на идентификации структур текстовой информации, **отличается от известных**, базирующихся на алгоритмах вычисления связей между словами, использованием системы приоритетов, реализующей последовательность перебора формализованных описаний синтаксической информации словоформ, обусловленную стилистическими особенностями текстов предметной области, что позволяет увеличить вероятность обнаружения угроз при осуществлении мониторинга сообщений открытых источников текстовой информации вычислительных сетей, избегая лавинообразного роста вычислительной сложности при построении структур без существенного снижения устойчивости обработки.

.

Основные результаты(5)

5. Комплекс методик и моделей активного аудита текстовых источников открытых компьютерных сетей, содержащих угрозы нарушения ИБ, основанный на построении специализированных объектов естественно-языковых конструкций, **отличается от известных**, базирующихся на статистических подходах, использованием фреймовых структур, что позволяет уменьшить количество примеров для достижения заданного показателя качества функции обучения, увеличив вероятность обнаружения требуемой информации для систем мониторинга состояния ИБ.

.

Использование результатов

- ФЦП «Научные и научно-педагогические кадры инновационной России»
  - НИР - 4
- ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007—2013 годы»
  - НИР - 1, ОКР -1
- По заказу МО РФ
  - НИР– 6, ОКР -3