# КОНЦЕПЦИЯ РАЗРАБОТКИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА СОТРУДНИКА СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Евдокимов Д. А., Файзуллин Р. Т.,***
*ГОУ ВПО Омский государственный университет им. Ф. М. Достоевского (Российская Федерация)*

В настоящей работе представляется концепция автоматизированного рабочего места (АРМ) сотрудника службы информационной безопасности (ИБ) предприятия. Для выполнения своих функциональных обязанностей сотрудник службы ИБ должен обладать широкими знаниями в области международных и отечественных стандартов в области ИБ для построения эффективной системы информационной безопасности. Сотрудник должен постоянно поддерживать систему ИБ на должном уровне, чтобы она отвечала актуальным угрозам безопасности, для этого необходимо регулярно проводить аудит системы ИБ с целью ее оценки и минимизации рисков.

Применение автоматизированных систем при проведении аудита ИБ способствует улучшению качества исследования, уменьшает влияние человеческого фактора, позволяет специалисту использовать более широкий арсенал критериев оценки ИБ. Модель проведения оценки защищенности объект информатизации (ОИ) предприятия при помощи автоматизированного рабочего места (АРМ) основана на формировании опросов для специалистов по информационной безопасности, производящих аудит. Процесс заполнения опроса основан на информации, которая не всегда может быть точной, например, в случае самооценки. Учитывая возможные неточности в исходной информации, в представляемой концепции для обработки результатов аудита применяется модель оценки, основанная на теории нечетких множеств (ТНМ).

Одной из задач разработки АРМа является разработка опросной анкеты по определенным критериям и стандартам информационной безопасности, а это влечет необходимость проведения исследования по актуальным, для специфики исследуемой

информационной системы, требованиям в данной области. Предлагаемая концепция предусматривает наделение АРМа свойством масштабируемости, которое достигается путем применения метода лексического анализа текстовых документов с целью получения опросной анкеты, которая изначально не закладывается в код программы на этапе разработки.

На рисунке 1 представлена концептуальная схема алгоритма работы программы на этапе формирования анкеты и проведения классификации.

**Лексический анализ** - процесс аналитического разбора входной последовательности символов с целью получения на выходе последовательности символов, называемых «токенами». При этом, в процессе лексического анализа производится распознавание и выделение лексем из входной последовательности символов [1].

Традиционно принято организовывать процесс лексического анализа, рассматривая входную последовательность символов, как поток символов. При такой организации, процесс самостоятельно управляет выборкой отдельных символов из входного потока[2]. Входной поток формируется из библиотеки документов, содержащих методики и критерии оценки информационной безопасности предприятия. При добавлении документа в библиотеку ему присваивается метка ***T***, определяющая его принадлежность к тому или иному разделу исследования, если ранее существовал данный раздел, иначе создается новый раздел. В качестве метки ***T*** принадлежности к определенному критерию ***K*** используется заголовок документа, в котором прописывается номер ***K***-го критерия из списка.

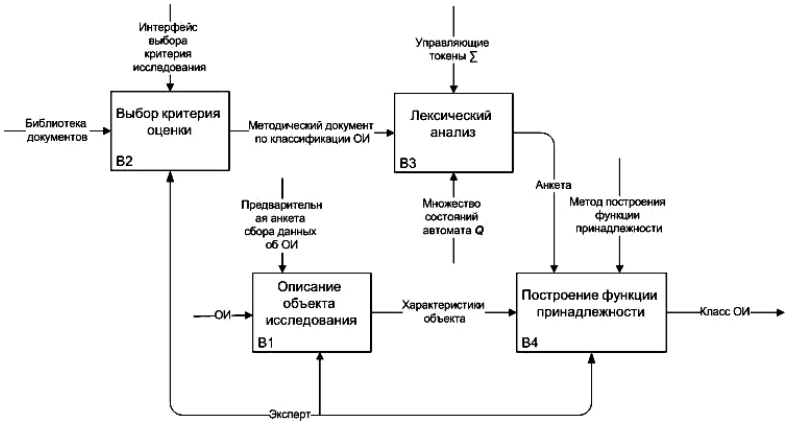


***Рисунок 1*** **- Алгоритм формирования опросных анкет проведения оценки защищенности ОИ предприятия.**

Для достижения масштабируемости АРМ по использованию критериев оценки, применяется метод лексического анализа библиотеки документов. Выбор критерия исследования $\boldsymbol{K_i}$ пользователем программы определяет перечень документов таких, что $\boldsymbol{T_j = K_i}$. Для любого исследования будет два и более документов. Лексический анализ первого документа формирует опросную анкету для определения класса в рамках выбранного критерия, второго - анкету оценки выполнения требований. Структура анкеты и содержание формируется в результате распознавания лексем конечным автоматом

$$\boldsymbol{M = (Q, \Sigma, \delta, q_0, F),} \qquad (1)$$

где $Q$ - конечное множество состояний автомата; $q_0$ - начальное состояние автомата $q_0 \in Q$; $F$ - множество заключительных (или допускающих) состояний, таких что $F \subset \sum Q$; $\sum$ — допустимый входной алфавит (конечное множество допустимых входных символов), из которого формируются строки, считываемые автоматом; $\delta$ — заданное отображение множества $Q \times \sum$ во множество $P(Q)$ подмножеств $Q$:

$$\boldsymbol{\delta : Q \times \sum \rightarrow P(Q)} \qquad (2)$$

На выходе алгоритма автомат выдает анкету для классификации либо оценки ОИ в зависимости от выбранного входного документа. Анкета формируется отображением $\delta$ множества $Q \times \Sigma$ во множество $P(Q)$ подмножеств Q.

Следующие этапы исследования – классификация и/или оценка исследуемой системы по выбранной методике с применением математического аппарата ТНМ. Пользователь АРМ проводящий оценку защищенности ОИ определяет метод оценки, на выбор предлагается два метода ТНМ: на основе балльной шкалы и на основе лингвистической шкалы[3].

**Литература**

1. Джон Хопкрофт, Раджив Мотвани, Джеффри Ульман Введение в теорию автоматов, языков и вычислений = Introduction to Automata Theory, Languages, and Computation. — М.: «Вильямс», 2002. — С. 528.
2. Касьянов В.Н. Лекции по теории формальных языков, автоматов и сложности вычислений. - Новосибирск: НГУ, 1995. - С. 112.
3. Батыршин И.З., Недосекин А.О., Стецко А.А., Тарасов В.Б., Язенин А.В., Ярушкина Н.Г. Теория и практика нечетких гибридных систем. Под ред. Н.Г. Ярушкиной. М.: Физматлит, 2007.