УДК 303.732.4

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПРОГНОЗИРОВАНИЯ ПОСЛЕДСТВИЙ ОШИБОЧНОГО КОНФИГУРИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ MS WINDOWS

Луценко Евгений Вениаминович
д. э. н., к. т. н., профессор
Кубанский государственный аграрный университет, Краснодар, Россия

Коржаков Валерий Евгеньевич
к. т. н., доцент
Адыгейский государственный университет
Адыгея, Россия

Дубянский Александр Александрович
Студент-дипломник
Кубанский государственный аграрный университет, Краснодар, Россия

В статье описана технология и некоторые результаты применения системно-когнитивного анализа для выявления знаний о последствиях ошибок в конфигурировании системы безопасности по отчету Microsoft Baseline Security Analyzer (MBSA) и использования этих знаний для прогнозирования последствий

Ключевые слова: СИСТЕМНО-КОГНИТИВНЫЙ АНАЛИЗ, СИСТЕМА «ЭЙДОС», ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ, ПРОГНОЗИРОВАНИЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОНФИГУРАЦИЯ СИСТЕМЫ БЕЗОПАСНОСТИ, MICROSOFT BASELINE SECURITY ANALYZER (MBSA)

UDC 303.732.4

INTELLECTUAL SYSTEM OF FORECASTING OF CONSEQUENCES OF ERRONEOUS CONFIGURATION OF SAFETY SYSTEMS OF MS WINDOWS

Lutsenko Evgeny Veniaminovich
Dr. Sci. Econ., Cand. Tech. Sci., Professor
Kuban State Agrarian University, Krasnodar, Russia

Korzhakov Valery Evgenievich
Cand. Tech. Sci., assistant professor
Adygeya State University, Adygeya, Russia

Dubyansky Alexander Aleksandrovich
diploma student
Kuban State Agrarian University, Krasnodar, Russia

In the article the technology and some results of application of systemic-cognitive analysis for revealing of knowledge of consequences of errors in configuration of safety systems under report of Microsoft Baseline Security Analyzer (MBSA) and uses of this knowledge for forecasting of consequences are described

Keywords: SYSTEMIC-COGNITIVE ANALYSIS, "EIDOS" SYSTEM, DECISION-MAKING SUPPORT, FORECASTING, INFORMATION SAFETY, CONFIGURATION OF SAFETY SYSTEM, MICROSOFT BASELINE SECURITY ANALYZER (MBSA)

Проблема обеспечения информационной безопасности является системной и далеко выходит за рамки чисто технической или инженерной проблемы. В частности вся серьезность возможных последствий ошибок в обеспечении информационной безопасности часто не вполне осознается не только системным администратором, но и руководством фирмы. Одной из причин этого, по-видимому, является то, что примеры, приводящиеся в специальной литературе[1], редко бывают убедительными, т.к. чаще всего описанные в них фирмы мало напоминают нашу конкретную небольшую фирму. В тоже время для обоснованного принятия решения о *целевом* финансировании работ по обеспечению информационной безопасности руководителю любой фирмы необходима информация как о стоимости этих ра-

[1] http://ru.wikipedia.org/wiki/Information_security

бот, так и о возможных финансовых и иных последствиях отказа от их проведения.

Однако проблема состоит в том, что получить подобную информацию в настоящее время весьма затруднительно, т.к. на Российском рынке программного обеспечения отсутствуют доступные небольшим фирмам и понятные рядовому системному администратору и его руководителю методики оценки последствий ошибок в конфигурировании системы безопасности их компьютеров.

К методу решения поставленной проблемы предъявляются определенные требования, в частности метод должен:

– обеспечивать решение сформулированной проблемы на основе информации системного администратора об ошибках конфигурации системы безопасности компьютеров и фактических последствиях этого в данной конкретной фирме;

– быть недорогим в приобретении и использовании, т.е. для этого должно быть достаточно недорогого лицензионного программного обеспечения и системного администратора, причем курс его дополнительного обучения должен быть несложным, т.е. не предъявлять к нему каких-то сверхжестких нереалистичных требований;

– быть адаптивным, т.е. оперативно учитывать изменения во всех компонентах моделируемой системы.

Для определенности ограничимся рассмотрением системы безопасности операционной системы MS Windows.

Одним из стандартных средств централизованной проверки компьютеров под управлением MS Windows, которое традиционно применяется для выявления типичных ошибок конфигурации системы безопасности и создания отдельного отчета по результатам проверки каждого компьютера под управлением операционной системы MS Windows, является Microsoft Baseline Security Analyzer (MBSA).[2]

Однако, данное средство не содержит какого-либо аппарата прогнозирования возможных последствий фактически имеющейся конфигурации системы безопасности.

Поэтому целью данной работы является решение поставленной проблемы путем разработки адаптивной методики *прогнозирования* возможных финансовых и иных последствий ошибок в настройках системы безопасности.

[2] http://yandex.ru/yandsearch?text=MICROSOFT%20BASELINE%20SECURITY%20ANALYZER%20(MBSA)%20&lr=213

Для достижения поставленной цели выбран метод системно-когнитивного анализа (СК-анализ). Этот выбор был обусловлен тем, что данный метод является непараметрическим, позволяет корректно и сопоставимо обрабатывать тысячи градаций факторов и будущих состояний объекта управления при неполных (фрагментированных), зашумленных данных различной природы, т.е. измеряемых в различных единицах измерения. Для метода СК-анализа разработаны и методика численных расчетов, и соответствующий программный инструментарий, а также технология и методика их применения. Они прошли успешную апробацию при решении ряда задач в различных предметных областях [1-16]. Наличие инструментария СК-анализа (базовая система "Эйдос") [1] позволяет не только осуществить синтез семантической информационной модели (СИМ), но и периодически проводить адаптацию и синтез ее новых версий, обеспечивая тем самым отслеживание динамики предметной области и сохраняя высокую адекватность модели в изменяющихся условиях. Важной особенностью СК-анализа является возможность единообразной числовой обработки разнотипных по смыслу и единицам измерения числовых и нечисловых данных. Это обеспечивается тем, что нечисловым величинам тем же методом, что и числовым, приписываются сопоставимые в пространстве и времени, а также между собой, количественные значения, позволяющие обрабатывать их как числовые: на первых двух этапах СК-анализа числовые величины сводятся к интервальным оценкам, как и информация об объектах нечисловой природы (фактах, событиях) (этот этап реализуется и в методах интервальной статистики); на третьем этапе СК-анализа всем этим величинам по единой методике, основанной на системном обобщении семантической теории информации А.Харкевича, сопоставляются количественные величины (имеющие смысл количества информации в признаке о принадлежности объекта к классу), с которыми в дальнейшем и производятся все операции моделирования (этот этап является уникальным для СК-анализа).

В работах [2-14] приведен перечень этапов системно-когнитивного анализа, которые необходимо выполнить, чтобы осуществить синтез модели объекта управления, решить с ее применением задачи прогнозирования и поддержки принятия решений, а также провести исследование объекта моделирования путем исследования его модели. Учитывая эти этапы СК-анализа выполним декомпозицию цели работы в последовательность задач, решение которых обеспечит ее поэтапное достижение:

1. Когнитивная структуризация предметной области и формальная постановка задачи, проектирование структуры и состава исходных данных.

2. Формализация предметной области.

2.1. Получение исходных данных запланированного состава в той форме, в которой они накапливаются в поставляющей их организации (обычно в форме базы данных какого-либо стандарта или Excel-формы).

2.2. Разработка стандартной Excel-формы для представления исходных данных.

2.3. Преобразование исходных данных из исходных баз данных в стандартную электронную Excel-форму.

2.4. Контроль достоверности исходных данных и исправление ошибок.

2.5. Использование стандартного программного интерфейса системы «Эйдос» для преобразования исходных данных из стандартной Excel-формы в базы данных системы "Эйдос" (импорт данных).

3. Синтез семантической информационной модели (СИМ), т.е. решение **задачи 1:** "***Многокритериальная типизация*** различных вариантов финансовых и иных последствий ошибок в настройках системы безопасности операционной системы".

4. Измерение адекватности СИМ.

5. Повышение эффективности СИМ.

6. Решение с помощью СИМ задач прогнозирования и поддержки принятия решений, а также исследования предметной области.

6.1. **Задача 2:** "Разработка методики ***прогнозирования*** влияния ошибок в настройках системы безопасности операционной системы на вид проблемы с безопасностью, а также способ, трудоемкость и стоимость ее устранения".

6.2. **Задача 3:** "Разработка методики ***поддержки принятия решений*** о выборе таких настроек системы безопасности операционной системы, которые по опыту фактически минимизируют проблемы безопасности".

6.3. **Задача 4:** «Исследование предметной области»

7. Разработка принципов оценки экономической эффективности разработанных технологий при их применении в торговой фирме.

8. Исследование ограничений разработанной технологии и перспектив ее развития.

Кратко рассмотрим решение этих задач.

1. Когнитивная структуризация предметной области это 1-й этап формальной постановки задачи, на котором решается, какие параметры будут рассматриваться в качестве причин, а какие – следствий. На этом этапе было решено рассматривать

в качестве следствий, т.е. *классов:*

1. Вид проблемы с безопасностью.
2. Способ устранения проблемы.
3. Трудоемкость устранения проблемы.
4. Стоимость устранения проблемы.

в качестве причин (факторов): – настройки конфигурации системы безопасности операционной системы:

1. Трудозатраты на устранение проблемы (Чел/часов).
2. Стоимость устранения проблемы (Руб.).
3. Система автоматического обновления.
4. Кол-во неустановленных обновл.безопасности MS Windows.
5. Кол-во неустановленных обновл.безопасности MS Office.
6. Количество слабых либо пустых паролей.
7. Количество паролей с неограниченным сроком действия.
8. Наличие более двух учетных записей администратора.
9. Включена учетная запись гость.
10. Минимальная длина пароля.
11. Максимальный срок действия пароля.
12. Пароль должен отвечать требованиям сложности.
13. Пороговое значение блокировки.
14. Разрешить доступ к FDD только локальным пользователям.
15. Разрешить доступ к CD только локальным пользователям.
16. Тип файловой системы.

На этапе формализации предметной области (постановки задачи), исходя из результатов когнитивной структуризации, было осуществлено проектирование структуры и состава исходных данных.

2.1. Исходные данные запланированного состава *были получены* в той форме, в которой они накапливаются в поставляющей их организации. В нашем случае этой организацией выступила фирма, название которой мы не приводим в связи с конфиденциальностью предоставленной ей информации. В полученной базе данных представлены данные по настройкам системы безопасности компьютеров фирмы, полученные с применением Microsoft Baseline Security Analyzer (MBSA), дополненные информацией об их фактических последствиях за календарный год, всего 323 записи по различным внутренним IP-адресам. Этого достаточно для целей данной работы, за что авторы благодарны руководству данной фирмы.

2.2. Была разработана стандартная Excel-форма для представления исходных данных (таблица 1), в которой и были получены данные

Таблица 1 – ИСХОДНЫЕ ДАННЫЕ (ФРАГМЕНТ)

Ip-адрес	Вид проблемы	Способ устранения проблемы	Трудозатраты на устранение проблемы (Челчасов)	Стоимость устранения проблемы (Руб.)	Система автоматического обновления	Кол-во неустановленных обновл.безопасности MS Windows	Кол-во неустановленных обновл.безопасности MS Office	Количество слабых либо пустых паролей	Количество паролей с неограниченным сроком действия	Наличие более двух учетных записей администратора	Включена учетная запись гость	Минимальная длина пароля	Максимальный срок действия пароля	Пароль должен отвечать требованиям сложности	Пороговое значение блокировки	Разрешить доступ к FDD только локальным пользователям	Разрешить доступ к CD только локальным пользователям	Тип файловой системы
192.168.1.12	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	1	0	0	0	Да	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.13	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	26	12	1	1	Нет	Да	0	0	Отключено	5	Да	Да	NTFS
192.168.1.14	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	1	6	0	0	Нет	Да	6	45	Включено	5	Да	Да	NTFS
192.168.1.15	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	5	15	1	1	Нет	Да	0	0	Отключено	3	Да	Да	NTFS
192.168.1.16	Сбой в работе	Устранение	3	3000	Отключено	64	23	3	3	Нет	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.17	Критический сбой в работе ОС	Переустановка ОС	5	5000	Отключено	124	19	2	2	Нет	Да	0	0	Отключено	0	Нет	Нет	NTFS
192.168.1.18	Сбой в работе прикладного ПО	Восстановление, настройка ПО	2	2000	Отключено	19	41	3	3	Нет	Да	0	30	Отключено	3	Да	Да	NTFS
192.168.1.19	Критический сбой в работе ПО	Переустановка и настройка ПО	4	4000	Отключено	19	68	0	0	Да	Нет	0	0	Отключено	3	Нет	Нет	NTFS
192.168.1.20	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	6	2	0	0	Да	Да	0	45	Отключено	0	Нет	Нет	NTFS
192.168.1.21	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	4	11	0	0	Да	Да	0	30	Включено	3	Да	Да	NTFS
192.168.1.22	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	0	6	0	0	Нет	Да	8	30	Включено	5	Нет	Нет	NTFS
192.168.1.23	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	7	10	0	2	Нет	Да	8	0	Отключено	5	Нет	Нет	NTFS
192.168.1.24	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	15	28	1	1	Нет	Да	0	5	Отключено	5	Да	Да	NTFS
192.168.1.25	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	48	40	1	1	Нет	Да	4	0	Отключено	5	Да	Да	NTFS
192.168.1.26	Сбой в работе	Устранение	3	3000	Отключено	77	15	3	3	Нет	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.27	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	2	0	0	0	Нет	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.28	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	0	0	0	0	Нет	Да	8	30	Включено	0	Да	Да	NTFS
192.168.1.29	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	1	1	0	0	Нет	Нет	0	0	Отключено	5	Да	Да	NTFS
192.168.1.30	Сбой в работе прикладного ПО	Восстановление, настройка ПО	2	2000	Включено	0	12	0	0	Нет	Нет	0	0	Отключено	0	Да	Да	FAT
192.168.1.31	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	18	11	3	3	Нет	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.32	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	5	2	1	3	Нет	Нет	0	0	Отключено	0	Да	Да	NTFS
192.168.1.33	Сбой в работе	Устранение	3	3000	Отключено	114	47	2	2	Да	Да	0	0	Отключено	0	Да	Да	FAT
192.168.1.34	Критический сбой в работе ПО	Переустановка и настройка ПО	4	4000	Отключено	86	20	2	2	Да	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.35	Сбой в работе прикладного ПО	Восстановление, настройка ПО	2	2000	Отключено	25	44	2	0	Нет	Да	0	0	Отключено	0	Да	Да	NTFS
192.168.1.36	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	0	3	0	0	Нет	Да	8	30	Включено	0	Нет	Нет	NTFS
192.168.1.37	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	35	17	1	1	Да	Да	4	0	Отключено	0	Да	Да	NTFS
192.168.1.38	Сбой в работе	Устранение	3	3000	Отключено	79	30	2	2	Да	Да	4	0	Отключено	0	Да	Да	NTFS
192.168.1.39	Критический сбой в работе ОС	Переустановка ОС	5	5000	Отключено	87	39	3	3	Нет	Да	0	0	Отключено	0	Нет	Нет	FAT
192.168.1.40	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	20	23	0	2	Нет	Да	8	0	Отключено	0	Нет	Нет	NTFS
192.168.1.41	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Отключено	21	5	0	1	Да	Да	4	0	Отключено	0	Да	Да	NTFS
192.168.1.42	Сбой в работе прикладного ПО	Восстановление, настройка ПО	2	2000	Отключено	66	51	1	1	Нет	Да	0	0	Отключено	0	Да	Да	FAT
192.168.1.43	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	0	10	0	0	Да	Да	0	0	Отключено	0	Нет	Нет	NTFS
192.168.1.44	Проблемы отсутствуют	Проблемы отсутствуют	0	0	Включено	2	8	0	0	Нет	Да	6	30	Включено	0	Нет	Нет	NTFS
192.168.1.45	Сбой в работе прикладного ПО	Восстановление, настройка ПО	2	2000	Включено	1	9	0	0	Да	Да	0	0	Отключено	0	Да	Да	FAT

2.3. Исходные данные из Excel-формы, представленной в таблице 1, были преобразованы средствами Excel в стандартную для программного интерфейса _152 системы "Эйдос" электронную Excel-форму, которая от-

личается от приведенной в таблице 1 отсутствием горизонтальной шапки и обратным порядком строк.

2.4. На этапе контроля достоверности исходных данных ошибок обнаружено не было.

2.5. Затем Excel-форма, приведенная на таблице 1 с применением sCalc из пакета OpenOffice была записана в стандарте DBF MS DOS-кириллица с именем Inp_data.dbf. Информация ее шапки была представлена в виде отдельного текстового файла стандарта MS DOS с именем: Inp_name.txt. Для этого шапка была скопирована из Excel в MS Word, затем таблица преобразована в текст с концом абзаца после каждого заголовка столбца, текст был выровнен по левому краю и 1-е буквы сделаны большими, как в предложениях.

Все это сделано в соответствии с требованиями стандартного интерфейса системы «Эйдос» с внешними базами данных: режим _152. Экранная форма меню вызова данного программного интерфейса приведена на рисунке 1, help режима приведен на рисунке 2, экранные формы самого программного интерфейса _152 приведены на рисунках 3 и 4.

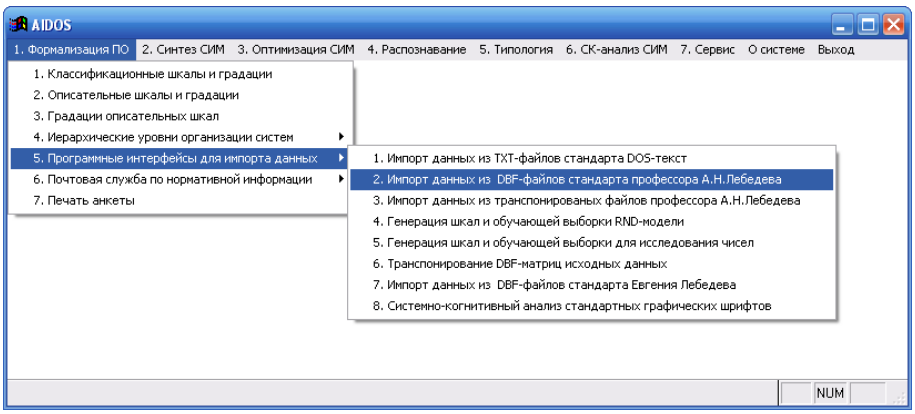


Рисунок 1. Экранная форма вызова режима _152 системы «Эйдос».

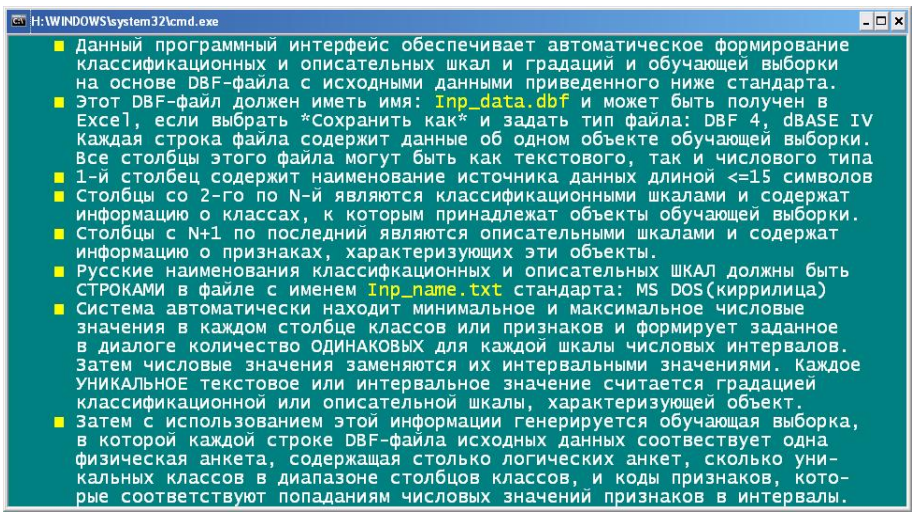


Рисунок 2. Требования стандартного интерфейса системы «Эйдос» с внешними базами данных: режим _152.

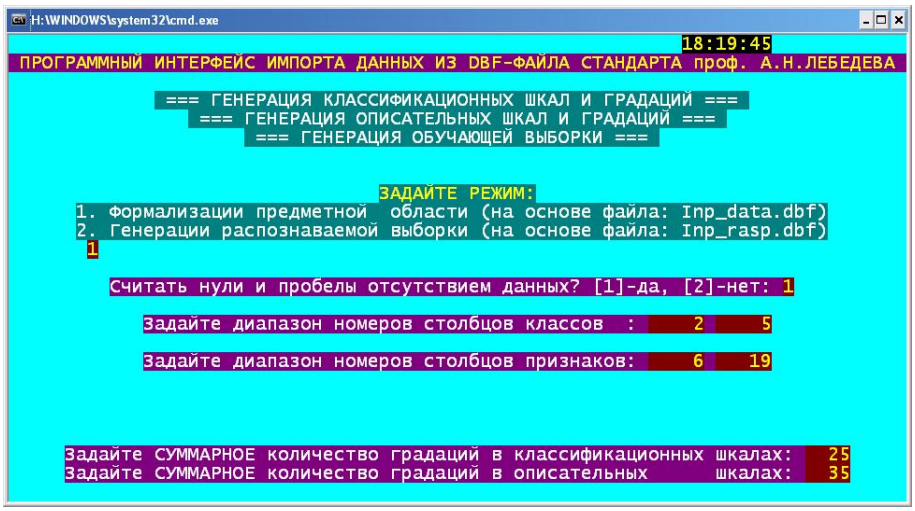


Рисунок 3. Первая экранная форма режима _152 системы «Эйдос».

Рисунок 4. Вторая экранная форма режима _152 системы «Эйдос».

В результате работы данного программного интерфейса ***автоматически*** получаются исходный справочник классов распознавания, справочник признаков, а также обучающая выборка, представляющая собой закодированные в соответствии с этими справочниками строки из таблицы 1 (таблица 2 – таблица 5):

Таблица 2 – СПРАВОЧНИК КЛАССОВ (ИНТЕРВАЛЬНЫХ ЗНАЧЕНИЙ КЛАССИФИКАЦИОННЫХ ШКАЛ)

KOD	NAME
1	ВИД ПРОБЛЕМЫ-Критический сбой в аппаратной части
2	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС
3	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО
4	ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечка данных
5	ВИД ПРОБЛЕМЫ-Потеря данных
6	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют
7	ВИД ПРОБЛЕМЫ-Сбой в аппаратной части
8	ВИД ПРОБЛЕМЫ-Сбой в работе ОС
9	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО
10	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части
11	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных

12	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО
13	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части
14	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС
15	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС
16	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО
17	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности
18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют
19	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев
20	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {2.00, 3.00}
21	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00}
22	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00}
23	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {2000.00, 3000.00}
24	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {3000.00, 4000.00}
25	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {4000.00, 5000.00}

Таблица 3 – СПРАВОЧНИК НАИМЕНОВАНИЙ ФАКТОРОВ (ОПИСАТЕЛЬНЫХ ШКАЛ)

KOD	NAME
1	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ
2	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS
3	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE
4	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ
5	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ
6	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА
7	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ
8	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ
9	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ
10	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ
11	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ
12	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ
13	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ
14	ТИП ФАЙЛОВОЙ СИСТЕМЫ

Таблица 4 – СПРАВОЧНИК НАИМЕНОВАНИЙ ИНТЕРВАЛЬНЫХ ЗНАЧЕНИЙ ФАКТОРОВ (ГРАДАЦИЙ ОПИСАТЕЛЬНЫХ ШКАЛ)

KOD	NAME
1	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Включено
2	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Отключено
3	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {1.00, 55.67}
4	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {55.67, 110.34}
5	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {110.34, 165.01}
6	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {1.00, 38.00}
7	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {38.00, 75.00}
8	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {75.00, 112.00}
9	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.00, 1.67}
10	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.67, 2.34}
11	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {2.34, 3.01}
12	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.00, 1.67}
13	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.67, 2.34}
14	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {2.34, 3.01}
15	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Да
16	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Нет
17	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Да
18	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Нет
19	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {4.00, 5.33}
20	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {5.33, 6.66}
21	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {6.66, 7.99}
22	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {5.00, 36.33}
23	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {36.33, 67.66}
24	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {67.66, 98.99}
25	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Включено

26	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Отключено
27	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {3.00, 3.67}
28	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {3.67, 4.34}
29	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {4.34, 5.01}
30	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да
31	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет
32	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да
33	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет
34	ТИП ФАЙЛОВОЙ СИСТЕМЫ-FAT
35	ТИП ФАЙЛОВОЙ СИСТЕМЫ-NTFS

Таблица 5 – АНКЕТА обучающей выборки N° 1

02-05-10 18:28:27 г.Краснодар

Код	Наименования классов распознавания
6	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют
18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют

К о д ы п е р в и ч н ы х п р и з н а к о в
1 3 15 17 26 30 32 35

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

Таким образом, данным программным интерфейсом ***полностью автоматизируется*** этап СК-анализа, называемый "Формализация предметной области".

3. В результате синтеза семантической информационной модели решена **задача 1:** "***Многокритериальная типизация*** различных вариантов финансовых и иных последствий ошибок в настройках системы безопасности операционной системы". Решение этой задачи осуществлялось в ряд этапов:

Этап-1. Расчет матрицы сопряженности (матрицы абсолютных частот), связывающей частоты ***фактов*** совместного наблюдения в исходной выборке интервальных значений классов и факторов. Всего этих фактов исследовано **9010**, что и составляет объем выборки. По своей форме матрица абсолютных частот является *базой данных*, т.к. в ней содержится способа содержательной смысловой интерпретации данных.

Этап-2. На основе базы данных абсолютных частот рассчитываются информационные базы условных и безусловных процентных распределений или частостей, которые при увеличении объема исходной выборки стремятся к предельным значениям: вероятностям. Имея это в виду несколько упрощая считается допустимым, как это принято в литературе, называть их условными и безусловными вероятностями. По своей форме матрицы условных и безусловных вероятностей является *информационными базами*, т.к. в них содержится способ содержательной смысловой интерпретации данных, т.е. уже по сути информации [15].

Этап-3. На основе информационной базы условных и безусловных вероятностей рассчитывается *база знаний.* Есть все основания так называть ее, т.к. в ней не только содержится результат содержательной смысловой интерпретации данных, но и оценка их *полезности* для достижения *целевых* состояний объекта управления и избегания нежелательных (нецелевых), т.е. по сути *знания*, которые можно непосредственно использовать для управления моделируемым объектом [15] (таблица 6).

Таблица 6 – БАЗА ЗНАНИЙ О СИЛЕ И НАПРАВЛЕНИИ ВЛИЯНИЯ ЗНАЧЕНИЙ ФАКТОРОВ НА ПЕРЕХОД МОДЕЛИРУЕМОГО ОБЪЕКТА В СОСТОЯНИЯ, СООТВЕТСТВУЮЩИЕ КЛАССАМ (Бит × 100)

KOD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1						23	-26		-30	-26		-38						23	-105	-55	-107	-115	-55	-107	-115
2	33	28	28	28	31	-30	17	29	17	17	31	19	33	28	28	28	28	-30	26	22	25	25	22	25	25
3			-34	-40		9	-1	-6	5	-1		3				-34	-40	9	-3	-3	-18	-33	-3	-18	-33
4		48	36	57	19	-41	40	34	10	40	19	13			55	36	57	-41	31	19	32	33	19	32	33
5	116	97	70		129			4			129		116	147	84	70			1	-5	45	73	-5	45	73
6	-9	-49	-9	-14	-32	7	10	-5	-32	10	-32	-30	-9	21	-78	-9	-14	7	-8	-16	-5	-8	-16	-5	-8
7	37	45	12	33	15	-34	1	16	50	1	15	49	37		51	12	33	-34	21	36	11	12	36	11	12
8		119	77			-54									126	77		-54			41	69		41	69
9		-18	31		34	-12	20	0	17	20	34	19			-11	31		-12	-3	6	16	23	6	16	23
10		36	9	15		-9	19	25	-11	19		-8		86	23	9	15	-9	22	5	14	12	5	14	12
11	90	15	20	50	32	-26	18	33	-11	18	32	-9	90		22	20	50	-26	31	20	24	21	20	24	21
12		-35	-20	0		6	4	-2	0	4		3			-28	-20	0	6	-5	-4	-7	-14	-4	-7	-14
13		41	23	29	12	-5	-2	4	-52	-2	12	-50		65	37	23	29	-5	1	-16	16	21	-16	16	21
14	61	-14	15	21	39	1		-16	-26		39	-23	61		-7	15	21	1	-19	-14	-1	18	-14	-1	18
15	53	-22	-7	13	66	-11	73	12	23	73	66	25	53		-15	-7	13	-11	9	19	-0	-16	19	-0	-16
16	-21	3	-0	-6	-44	2	-58	-3	-5	-58	-44	-6	-21	9	2	-0	-6	2	-2	-5	-1	1	-5	-1	1
17	30	19	0	11	8	-6	29	17	-0	29	8	2	30	26	18	0	11	-6	14	8	6	1	8	6	1
18		-62	-5	-27	-9	8		-43	3		-9	-0			-55	-5	-27	8	-32	-13	-13	-6	-13	-13	-6
19			9			-10		13	39			42				9		-10	10	25	8	1	25	8	1
20						28												28							
21																									
22			-91			19		-87	-5			-12				-91		19	-55	-25	-57	-64	-25	-57	-64
23						28												28							
24						28												28							
25			-38	-18	0	17		-90	-18		0	-26				-38	-18	17	-58	-35	-39	-32	-35	-39	-32
26	25	21	11	5	2	-11	24	18	9	24	2	11	25	20	21	11	5	-11	15	13	11	9	13	11	9
27		-47	-18	-12	6	12		-85	-3		6	-9			-40	-18	-12	12	-52	-23	-26	-15	-23	-26	-15
28																									
29		44	2			-3		41							51	2		-3	38	-3	21	-6	-3	21	-6
30	33	-7	-7	13	10	-7	31	19	13	31	10	16	33		0	-7	13	-7	16	16	4	-16	16	4	-16
31		6	5	-30	-12	8		-47	-21		-12	-27		41	-2	5	-30	8	-35	-29	-9	12	-29	-9	12
32	34	-6	-6	14	11	-7	33	20	11	33	11	14	34		1	-6	14	-7	17	15	5	-14	15	5	-14

В этой матрице столбцы соответствуют классам распознавания, строки – градациям факторов, а в клетках на их пересечении приведено ***количество знаний*** в битах × 100, которое содержится в определенной градации фактора о том, что этот случай относится к определенному классу.

Отметим, что в настоящее время общепринятыми терминами являются: «База данных» и «База знаний», а термин «Информационные базы» считается «незагостированным», т.е. неофициальным, или даже ошибочным, когда под ним, по сути, понимаются базы данных. Предлагается придать термину «Информационные базы» полноценный статус в качестве официального термина, т.к. вполне понятно и обоснованно [15] как его содержание соотносится с содержанием терминов «База данных» и «База знаний»:

– Базы данных (БД) – информация записанная на носителях (или находящаяся в каналах связи) на определенном языке (системе кодирования), безотносительно к ее смыслу.

– Информационная база (ИБ) – это БД вместе с тезаурусом, т.е. способом их смысловой интерпретации.

– База знаний (БЗ) – это ИБ вместе с информацией о том, насколько какая информация полезна для достижения различных целей.

4. Измерение адекватности СИМ осуществляется последовательным выполнением режимов _21 (копирование обучающей выборки в распознаваемую), _41 (пакетное распознавание) и _62 (измерение адекватности СИМ) системы «Эйдос».

Пункты 3 и 4 удобно выполнить также с помощью режима _25 системы "Эйдос", который последовательно выполняет все вышеперечисленные операции, т.е. сначала выполняет синтез семантической информационной модели (СИМ), а затем копирует обучающую выборку в распознаваемую выборку), проводит пакетное распознавание и проверку ее адекватности, которая оказалась неплохой: более 71% (таблица 7).

Таблица 7 – ВЫХОДНАЯ ФОРМА ПО РЕЗУЛЬТАТАМ ИЗМЕРЕНИЯ АДЕКВАТНОСТИ ИСХОДНОЙ МОДЕЛИ (ФРАГМЕНТ)

ИЗМЕРЕНИЕ АДЕКВАТНОСТИ (ДИФФЕРЕНЦИАЛЬНОЙ И ИНТЕГРАЛЬНОЙ ВАЛИДНОСТИ) СЕМАНТИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ

Всего физических анкет: 323 (100% для п.15)
Всего логических анкет: 844

4. Средняя достоверность идентификации логических анкет с учетом сходства : 17.096%
5. Среднее сходство логических анкет, правильно отнесенных к классу : 9.824%
6. Среднее сходство логических анкет, ошибочно не отнесенных к классу : 2.091%
7. Среднее сходство логических анкет, ошибочно отнесенных к классу : 2.602%
8. Среднее сходство логических анкет, правильно не отнесенных к классу : 11.966%

9. Средняя достоверность идентификации логических анкет с учетом кол-ва : 43.517%
10. Среднее количество физич-х анкет, действительно относящихся к классу: 154.408 (100% для п.11 и п.12)
Среднее количество физич-х анкет, действительно не относящихся к классу: 168.592 (100% для п.13 и п.14)
Всего физических анкет: 323.000 (100% для п.15)
11. Среднее количество и % лог-их анкет, правильно отнесенных к классу: 109.639, т.е. 71.006%
12. Среднее количество и % лог-их анкет, ошибочно не отнесенных к классу: 44.769, т.е. 28.994% (Ошибка 1-го рода)
13. Среднее количество и % лог-их анкет, ошибочно отнесенных к классу: 46.451, т.е. 27.552% (Ошибка 2-го рода)
14. Среднее количество и % лог-их анкет, правильно не отнесенных к классу: 122.141, т.е. 72.448%

15. Средневзвешенная вероятность случайного угадывания принадлежности объекта к классу (%): 47.804
16. Средневзвешенная эффективность применения модели по сравнению со случ. угадыванием (раз): 7.947
17. Обобщенная достоверность модели (Д1+Д2)/2: 71.727%. Обобщенная ошибка (Е1+Е2)/2: 28.273%

03-05-10 09:00:52 г.Краснодар

N п/п	Код класса	Наименование класса	Достов. идентиф. лог.анк. с уч.количества эвр.крит	Кол-во лог.анк. дейст-но относящихся к классу	Количество логических анкет правильно или ошибочно отнесенных или не отнесенных к классу				Вероятн. случайного угадывания (%) =NLA/NPA	Эффектив модели по срав. со случ. угадыв. (раз)
					Правиль. отнесен.	Ошибочно не отнес	Ошибочно отнесен.	Правиль. не отнес		
1	2	3	9	10	11	12	13	14	15	16
1	1	ВИД ПРОБЛЕМЫ-Критический сбой в аппаратной части	51.7	2	2	0	78	243	0.619	161.551
2	2	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС	70.9	8	7	1	46	269	2.477	35.325
3	3	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО	59.1	18	14	4	62	243	5.573	13.956
4	4	ВИД ПРОБЛЕМЫ-Потеря данных	83.9	3	2	1	25	295	0.929	71.762
5	5	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют	48.0	246	173	73	11	66	76.161	0.923
6	6	ВИД ПРОБЛЕМЫ-Сбой в аппаратной части	49.2	4	4	0	82	237	1.238	80.775
7	7	ВИД ПРОБЛЕМЫ-Сбой в работе ОС	-1.5	17	16	1	163	143	5.263	17.883
8	8	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО	40.6	21	15	6	90	212	6.502	10.986
9	9	ВИД ПРОБЛЕМЫ-Утечка данных	38.7	4	3	1	98	221	1.238	60.582
10	10	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части	49.2	4	4	0	82	237	1.238	80.775
11	11	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных	83.9	3	2	1	25	295	0.929	71.762
12	12	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО	33.1	20	15	5	103	200	6.192	12.112
13	13	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части	51.7	2	2	0	78	243	0.619	161.551
14	14	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС	18.9	1	1	0	131	191	0.310	322.581
15	15	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС	73.4	7	7	0	43	273	2.167	46.147
16	16	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО	59.1	18	14	4	62	243	5.573	13.956
17	17	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности	38.7	4	3	1	98	221	1.238	60.582
18	18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют	48.0	246	173	73	11	66	76.161	0.923
19	19	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев	9.0	18	16	2	145	160	5.573	15.950
20	20	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00)	28.8	41	32	9	106	176	12.693	6.149
21	21	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00)	30.7	37	30	7	105	181	11.455	7.078
22	22	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00)	52.3	21	17	4	73	229	6.502	12.450
23	23	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00)	28.8	41	32	9	106	176	12.693	6.149
24	24	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00)	30.7	37	30	7	105	181	11.455	7.078
25	25	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00)	52.3	21	17	4	73	229	6.502	12.450
		Средневзвешенные значения	43.5	154.4	109.6	44.8	46.5	122.1	47.804	7.947

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

5. В системе "Эйдос" реализовано несколько различных методов повышения адекватности модели:

– исключение из модели статистически малопредставленных классов и факторов (артефактов);

– исключение незначимых факторов, т.е. факторов имеющих низкую селективную силу или дифференцирующую способность;

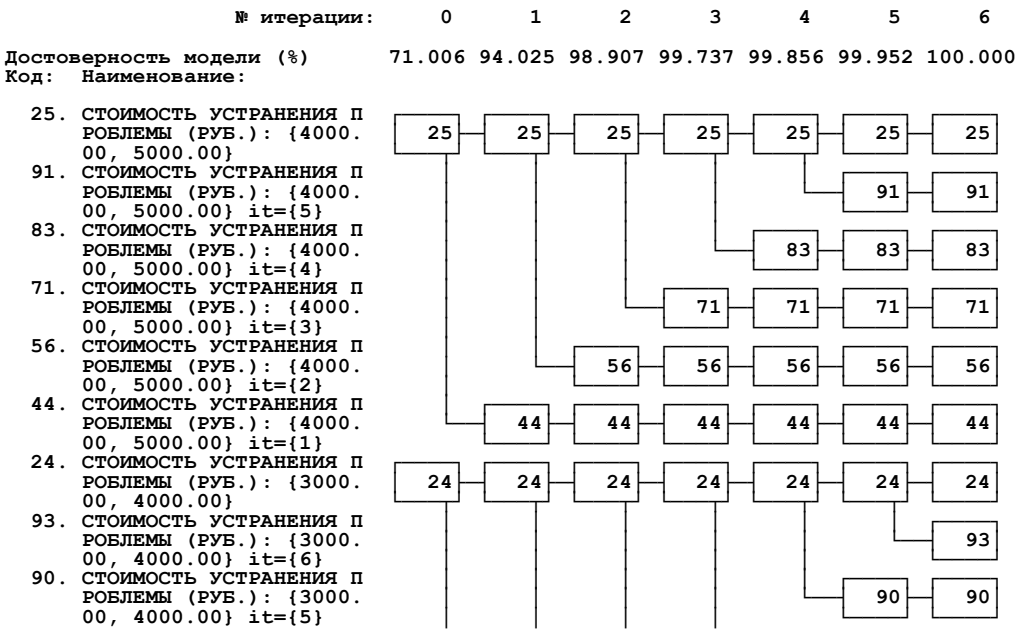
– ремонт (взвешивание) данных, что обеспечивает не только классическую, но и структурную репрезентативность исследуемой выборки по отношению к генеральной совокупности;

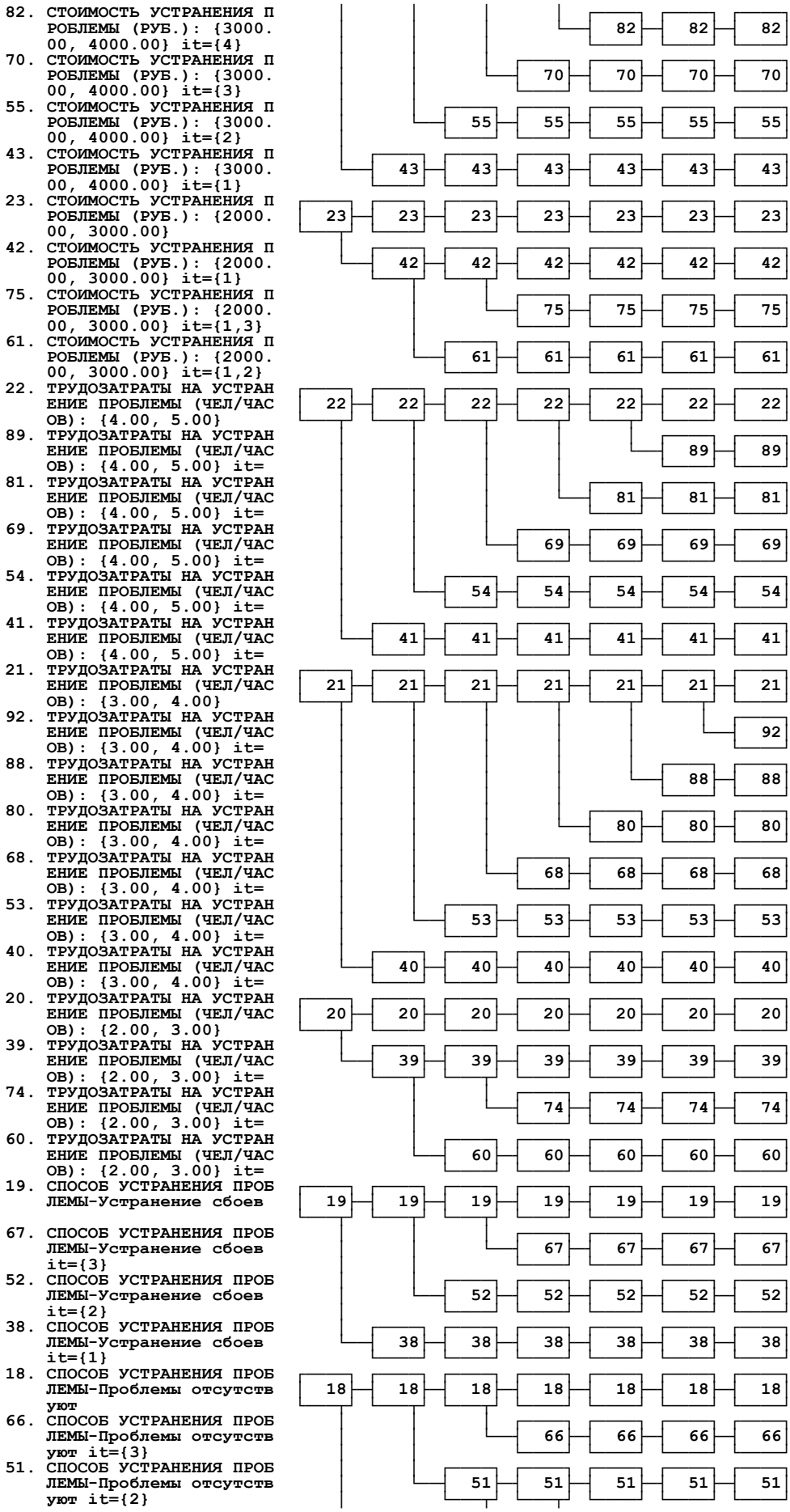
– итерационное разделение классов на типичную и нетипичную части (дивизивная, т.е. разделяющая, в отличие от агломеративной, древовидная кластеризация);

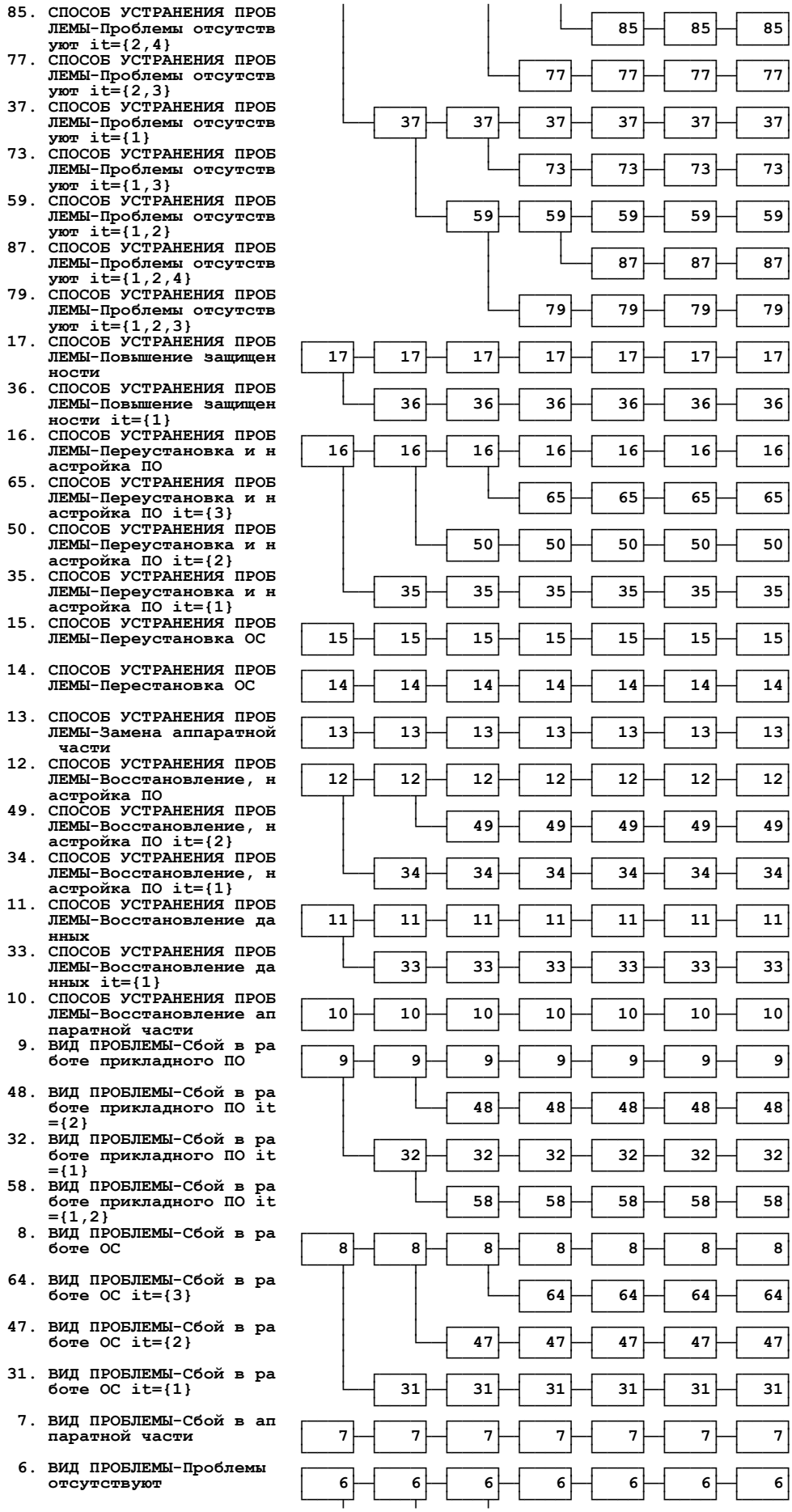
– генерация сочетанных признаков, дополнение справочников классов и признаков и перекодирование исходной выборки.

Проверка адекватности модели, проведенная в режиме _25 после ее синтеза, показала, что имеет смысл *повысить адекватность модели*. Для этой цели был применен метод повышения адекватности модели, путем итерационного разделение классов на типичную и нетипичную части (дивизивная, т.е. разделяющая, в отличие от агломеративной, древовидная кластеризация). В результате было получено следующее дерево классов (рисунок 5):

ДЕРЕВО РАЗДЕЛЕНИЯ КЛАССОВ НА ТИПИЧНЫЕ И НЕТИПИЧНЫЕ




82. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {3000.00, 4000.00} it={4}
70. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {3000.00, 4000.00} it={3}
55. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {3000.00, 4000.00} it={2}
43. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {3000.00, 4000.00} it={1}
23. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {2000.00, 3000.00}
42. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {2000.00, 3000.00} it={1}
75. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {2000.00, 3000.00} it={1,3}
61. СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {2000.00, 3000.00} it={1,2}
22. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00}
89. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00} it=
81. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00} it=
69. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00} it=
54. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00} it=
41. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {4.00, 5.00} it=
21. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00}
92. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
88. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
80. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
68. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
53. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
40. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {3.00, 4.00} it=
20. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {2.00, 3.00}
39. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {2.00, 3.00} it=
74. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {2.00, 3.00} it=
60. ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): {2.00, 3.00} it=
19. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев
67. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it={3}
52. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it={2}
38. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it={1}
18. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют
66. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={3}
51. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={2}


85. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={2,4}
77. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={2,3}
37. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={1}
73. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={1,3}
59. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={1,2}
87. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={1,2,4}
79. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it={1,2,3}
17. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности
36. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности it={1}
16. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО
65. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it={3}
50. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it={2}
35. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it={1}
15. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС
14. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС
13. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части
12. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО
49. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО it={2}
34. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО it={1}
11. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных
33. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных it={1}
10. СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части
9. ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО
48. ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it={2}
32. ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it={1}
58. ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it={1,2}
8. ВИД ПРОБЛЕМЫ-Сбой в работе ОС
64. ВИД ПРОБЛЕМЫ-Сбой в работе ОС it={3}
47. ВИД ПРОБЛЕМЫ-Сбой в работе ОС it={2}
31. ВИД ПРОБЛЕМЫ-Сбой в работе ОС it={1}
7. ВИД ПРОБЛЕМЫ-Сбой в аппаратной части
6. ВИД ПРОБЛЕМЫ-Проблемы отсутствуют

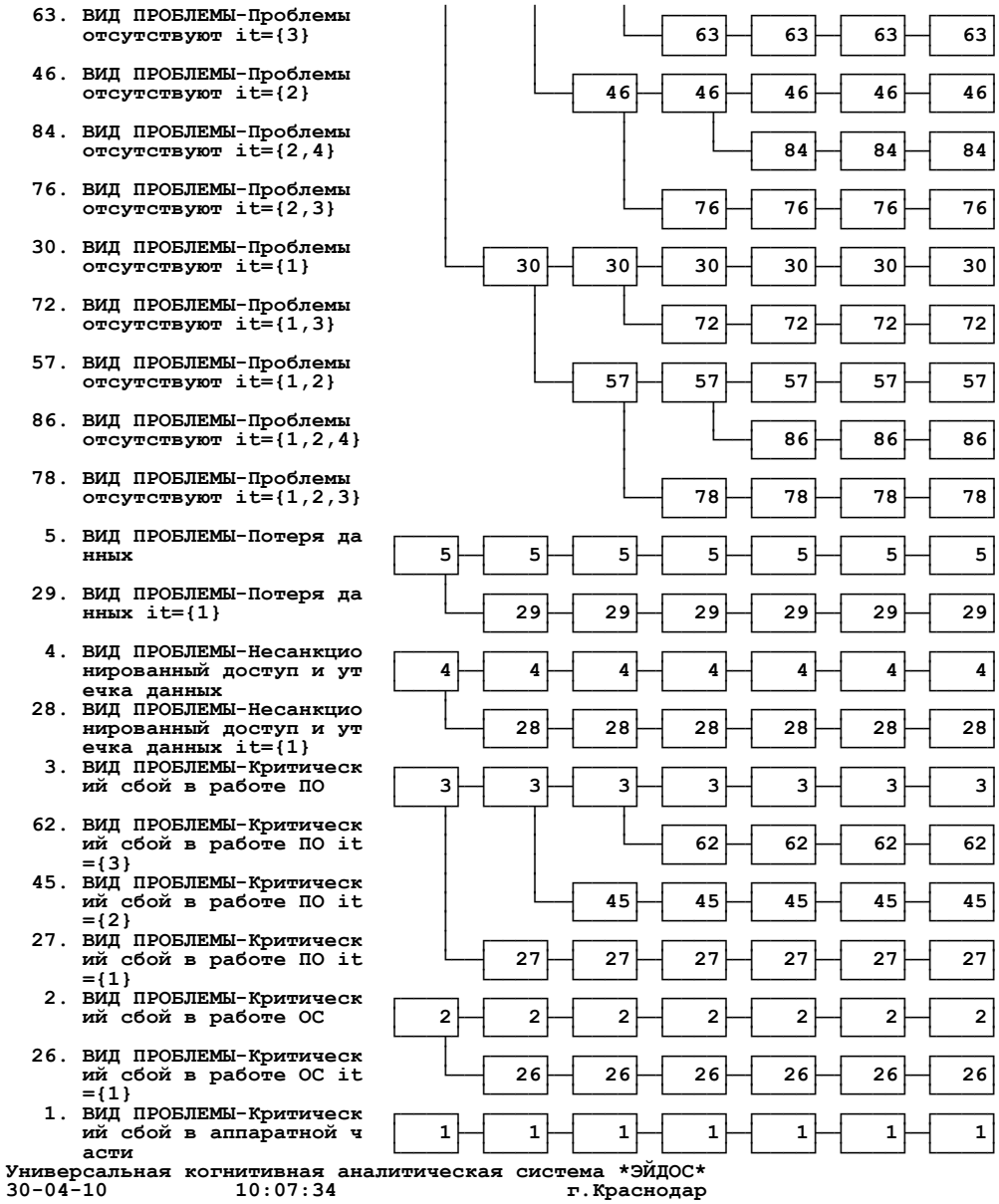


Рисунок 5 – Дерево разделения классов на типичную и нетипичную части (дивизивная кластеризация)

По результатам кластеризации можно сделать вывод о том, что различные классы обладают различной степенью вариабельности обусловливающих их факторов, т.е. одни классы являются жестко детерминированными, тогда как другие вызываются различными сочетаниями действующих факторов, что затрудняет и делает менее достоверной их прогнозирование и осуществление.

В результате проведения данной процедуры степень достоверности модели повысилась (таблица 8):

Таблица 8 – ВЫХОДНАЯ ФОРМА ПО РЕЗУЛЬТАТАМ ИЗМЕРЕНИЯ АДЕКВАТНОСТИ МОДЕЛИ, УЛУЧШЕННОЙ МЕТОДОМ ДИВИЗИВНОЙ КЛАСТЕРИЗАЦИИ

ИЗМЕРЕНИЕ АДЕКВАТНОСТИ (ДИФФЕРЕНЦИАЛЬНОЙ И ИНТЕГРАЛЬНОЙ ВАЛИДНОСТИ) СЕМАНТИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ

Всего физических анкет: 323 (100% для п.15)
Всего логических анкет: 844

4. Средняя достоверность идентификации логических анкет с учетом сходства : 17.799%
5. Среднее сходство логических анкет, правильно отнесенных к классу : 6.808%
6. Среднее сходство логических анкет, ошибочно не отнесенных к классу : 0.000%
7. Среднее сходство логических анкет, ошибочно отнесенных к классу : 4.415%
8. Среднее сходство логических анкет, правильно не отнесенных к классу : 15.406%

9. Средняя достоверность идентификации логических анкет с учетом кол-ва : 55.511%
10. Среднее количество физич-х анкет, действительно относящихся к классу: 78.756 (100% для п.11 и п.12)
Среднее количество физич-х анкет, действительно не относящихся к классу: 244.244 (100% для п.13 и п.14)
Всего физических анкет: 323.000 (100% для п.15)
11. Среднее количество и % лог-их анкет, правильно отнесенных к классу: 78.756, т.е. 100.000%
12. Среднее количество и % лог-их анкет, ошибочно не отнесенных к классу: 0.000, т.е. 0.000% (Ошибка 1-го рода)
13. Среднее количество и % лог-их анкет, ошибочно отнесенных к классу: 71.850, т.е. 29.417% (Ошибка 2-го рода)
14. Среднее количество и % лог-их анкет, правильно не отнесенных к классу: 172.395, т.е. 70.583%

15. Средневзвешенная вероятность случайного угадывания принадлежности объекта к классу (%): 24.382
16. Средневзвешенная эффективность применения модели по сравнению со случ. угадыванием (раз): 35.578
17. Обобщенная достоверность модели (Д1+Д2)/2: 85.292%. Обобщенная ошибка (Е1+Е2)/2: 14.709%

02-05-10 19:01:56 г.Краснодар

N п/п	Код класса	Наименование класса	Достов. идентиф. лог.анк. с уч.ко-личества эвр.крит	Кол-во лог.анк. дейст-но относя-щихся к классу	Количество логических анкет правильно или ошибочно отнесенных или не отнесенных к классу				Вероятн. случай-ного угадыва-ния (%) =NLA/NFA	Эффектив модели по срав. со случ. угадыв. (раз)
					Правиль. отнесен.	Ошибочно не отнес	Ощибочно отнесен.	Правиль. не отнес		
1	2	3	9	10	11	12	13	14	15	16
1	1	ВИД ПРОБЛЕМЫ-Критический сбой в аппаратной части	51.7	2	2	0	78	243	0.619	161.551
2	2	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС	81.4	7	7	0	30	286	2.167	46.147
3	3	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО	74.0	7	7	0	42	274	2.167	46.147
4	4	ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечка данных	33.7	3	3	0	107	213	0.929	107.643
5	5	ВИД ПРОБЛЕМЫ-Потеря данных	86.4	2	2	0	22	299	0.619	161.551
6	6	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют	92.6	163	163	0	12	148	50.464	1.982
7	7	ВИД ПРОБЛЕМЫ-Сбой в аппаратной части	49.2	4	4	0	82	237	1.238	80.775
8	8	ВИД ПРОБЛЕМЫ-Сбой в работе ОС	8.4	13	13	0	148	162	4.025	24.845
9	9	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО	39.3	13	13	0	98	212	4.025	24.845
10	10	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части	49.2	4	4	0	82	237	1.238	80.775
11	11	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных	86.4	2	2	0	22	299	0.619	161.551
12	12	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО	39.3	13	13	0	98	212	4.025	24.845
13	13	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части	51.7	2	2	0	78	243	0.619	161.551
14	14	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС	18.9	1	1	0	131	191	0.310	322.581
15	15	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС	73.4	7	7	0	43	273	2.167	46.147
16	16	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО	74.0	7	7	0	42	274	2.167	46.147
17	17	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности	33.7	3	3	0	107	213	0.929	107.643
18	18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют	92.6	163	163	0	12	148	50.464	1.982
19	19	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев	8.4	13	13	0	148	162	4.025	24.845
20	20	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00)	23.8	32	32	0	123	168	9.907	10.094
21	21	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00)	72.1	15	15	0	45	263	4.644	21.533
22	22	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00)	80.8	11	11	0	31	281	3.406	29.360
23	23	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00)	23.8	32	32	0	123	168	9.907	10.094
24	24	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00)	72.1	15	15	0	45	263	4.644	21.533
25	25	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00)	80.8	11	11	0	31	281	3.406	29.360
26	26	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС it=(1)	15.8	1	1	0	136	186	0.310	322.581
27	27	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО it=(1)	17.6	4	4	0	133	186	1.238	80.775
28	28	ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечка данных it=(1)	-5.9	1	1	0	171	151	0.310	322.581
29	29	ВИД ПРОБЛЕМЫ-Потеря данных it=(1)	-2.2	1	1	0	165	157	0.310	322.581
30	30	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(1)	36.8	67	67	0	102	154	20.743	4.821
31	31	ВИД ПРОБЛЕМЫ-Сбой в работе ОС it=(1)	-9.6	1	1	0	177	145	0.310	322.581
32	32	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it=(1)	4.0	5	5	0	155	163	1.548	64.599
33	33	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных it=(1)	-2.2	1	1	0	165	157	0.310	322.581
34	34	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО it=(1)	18.3	5	5	0	132	186	1.548	64.599
35	35	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it=(1)	17.6	4	4	0	133	186	1.238	80.775
36	36	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности it=(1)	-5.9	1	1	0	171	151	0.310	322.581
37	37	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(1)	36.8	67	67	0	102	154	20.743	4.821
38	38	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it=(1)	-0.9	2	2	0	163	158	0.619	161.551
39	39	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00) it=	7.7	7	7	0	149	167	2.167	46.147
40	40	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	18.9	7	7	0	131	185	2.167	46.147
41	41	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00) it=	13.3	4	4	0	140	179	1.238	80.775
42	42	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00) it=(1)	7.7	7	7	0	149	167	2.167	46.147
43	43	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(1)	18.9	7	7	0	131	185	2.167	46.147
44	44	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00) it=(1)	13.3	4	4	0	140	179	1.238	80.775
45	45	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО it=(2)	62.2	4	4	0	61	258	1.238	80.775
46	46	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(2)	23.2	7	7	0	124	192	2.167	46.147
47	47	ВИД ПРОБЛЕМЫ-Сбой в работе ОС it=(2)	-32.5	2	2	0	214	107	0.619	161.551
48	48	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it=(2)	62.2	2	2	0	61	260	0.619	161.551
49	49	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО it=(2)	62.2	2	2	0	61	260	0.619	161.551
50	50	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it=(2)	62.2	4	4	0	61	258	1.238	80.775
51	51	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(2)	23.2	7	7	0	124	192	2.167	46.147
52	52	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it=(2)	-32.5	2	2	0	214	107	0.619	161.551
53	53	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	9.0	7	7	0	147	169	2.167	46.147
54	54	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00) it=	2.8	2	2	0	157	164	0.619	161.551
55	55	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(2)	9.0	7	7	0	147	169	2.167	46.147
56	56	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00) it=(2)	2.8	2	2	0	157	164	0.619	161.551
57	57	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2)	-34.4	3	3	0	217	103	0.929	107.643
58	58	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО it=(1,2)	-29.4	1	1	0	209	113	0.310	322.581
59	59	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2)	-34.4	3	3	0	217	103	0.929	107.643
60	60	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00) it=	-62.8	1	1	0	263	59	0.310	322.581
61	61	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00) it=(1,2)	-62.8	1	1	0	263	59	0.310	322.581
62	62	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО it=(3)	56.7	3	3	0	70	250	0.929	107.643
63	63	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(3)	-52.9	1	1	0	247	75	0.310	322.581
64	64	ВИД ПРОБЛЕМЫ-Сбой в работе ОС it=(3)	-56.7	1	1	0	253	69	0.310	322.581
65	65	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО it=(3)	56.7	3	3	0	70	250	0.929	107.643
66	66	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(3)	-52.9	1	1	0	247	75	0.310	322.581
67	67	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев it=(3)	-56.7	1	1	0	253	69	0.310	322.581
68	68	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	41.2	2	2	0	95	226	0.619	161.551
69	69	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00) it=	44.3	2	2	0	90	231	0.619	161.551
70	70	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(3)	41.2	2	2	0	95	226	0.619	161.551
71	71	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00) it=(3)	44.3	2	2	0	90	231	0.619	161.551
72	72	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,3)	25.7	1	1	0	120	202	0.310	322.581
73	73	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,3)	25.7	1	1	0	120	202	0.310	322.581
74	74	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00) it=	-29.4	1	1	0	209	113	0.310	322.581
75	75	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00) it=(1,3)	-29.4	1	1	0	209	113	0.310	322.581
76	76	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(2,3)	-2.8	1	1	0	166	156	0.310	322.581
77	77	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(2,3)	-2.8	1	1	0	166	156	0.310	322.581
78	78	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2,3)	-1.5	1	1	0	164	158	0.310	322.581
79	79	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2,3)	-1.5	1	1	0	164	158	0.310	322.581
80	80	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	1.5	3	3	0	159	161	0.929	107.643
81	81	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00) it=	4.0	1	1	0	155	167	0.310	322.581
82	82	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(4)	1.5	3	3	0	159	161	0.929	107.643
83	83	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00) it=(4)	4.0	1	1	0	155	167	0.310	322.581
84	84	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(2,4)	-7.1	1	1	0	173	149	0.310	322.581
85	85	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(2,4)	-7.1	1	1	0	173	149	0.310	322.581
86	86	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2,4)	-30.7	1	1	0	211	111	0.310	322.581
87	87	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют it=(1,2,4)	-30.7	1	1	0	211	111	0.310	322.581
88	88	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	-30.0	2	2	0	210	111	0.619	161.551
89	89	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00) it=	35.0	1	1	0	105	217	0.310	322.581
90	90	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(5)	-30.0	2	2	0	210	111	0.619	161.551
91	91	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00) it=(5)	35.0	1	1	0	105	217	0.310	322.581
92	92	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00) it=	-16.4	1	1	0	188	134	0.310	322.581
93	93	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00) it=(6)	-16.4	1	1	0	188	134	0.310	322.581
		Средневзвешенные значения	55.5	78.8	78.8	0.0	71.8	172.4	24.382	35.578

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

Аналогичная информация приведена в скриншотах экранных форм (рисунок 6):

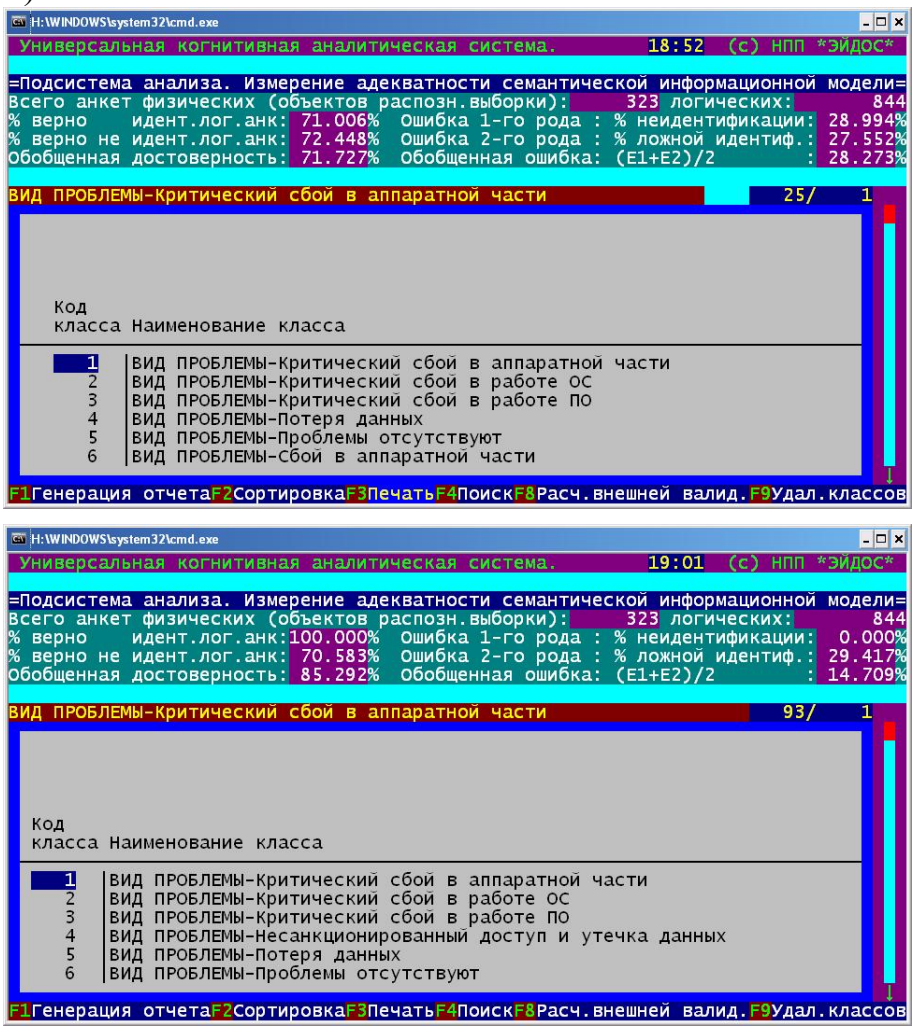


Рисунок 6. Экранные формы режима _62 системы «Эйдос»

Из сопоставительного анализа таблиц 7 и 8, а также рисунка 6 можно сделать следующие выводы:

– в результате разделения классов на типичную и нетипичную части достоверность верной идентификации повысилась на **29**%, достоверность верной неидентификации при этом немного понизилась, но общая (средняя) достоверность модели возросла на **13,6**%;

– при прогнозировании и принятии решений целесообразно учитывать дифференциальную достоверность идентификации по классам, связанную со степенью их детерминированности;

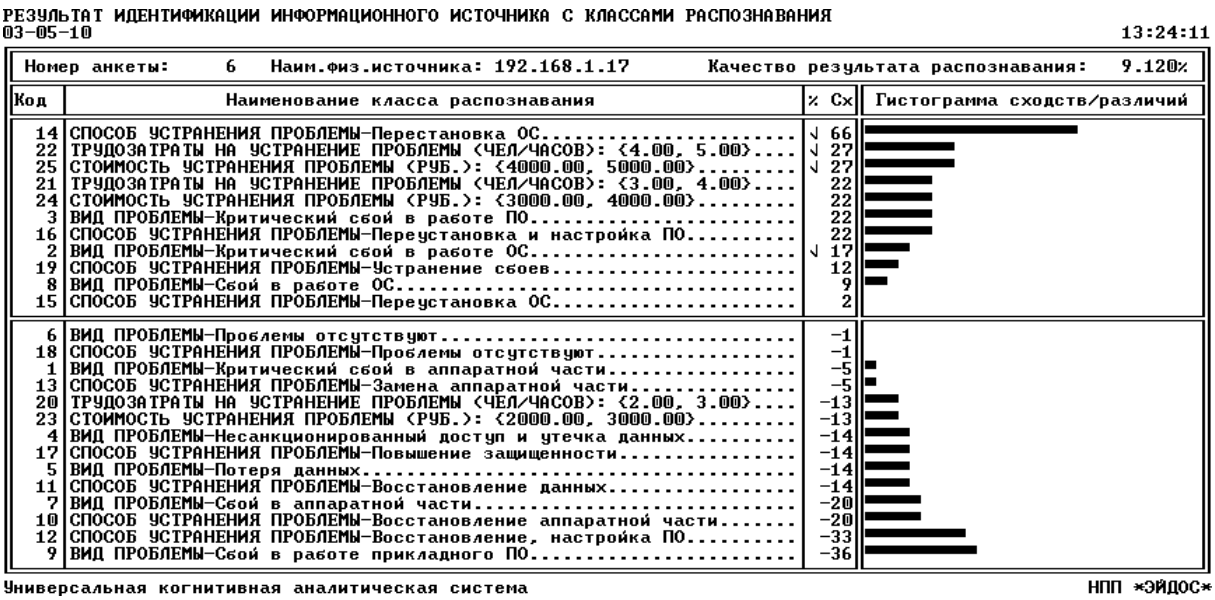
– применение модели чаще всего обеспечивает во много раз более высокую достоверность, чем случайное угадывание или не использование модели, однако по слабодетерминированным классам это не так и их неце-

лесообразно учитывать при прогнозировании и рассматривать при анализе модели.

6. Решение с помощью СИМ задач прогнозирования и поддержки принятия решений, а также исследования предметной области.

6.1. **Задача 2:** "Разработка методики ***прогнозирования*** влияния ошибок в настройках системы безопасности операционной системы на вид проблемы с безопасностью, а также способ, трудоемкость и стоимость ее устранения".

В системе "Эйдос" есть стандартный режим _42, обеспечивающий подсчет для каждого состояния системы информационной безопасности фирмы, представленного в *распознаваемой* выборке, суммарного количества знаний, которое содержится в интервальных значениях факторов, отражающих настройки системы безопасности, о принадлежности данного состояния к каждому из классов. Затем в режиме _431 все классы сортируются (ранжируются) в порядке убывания суммарного количества информации, содержащегося в описании примера, о принадлежности к ним. Эта информация представляется в виде экранных форм и файлов (рисунки 7, 8).


РЕЗУЛЬТАТ ИДЕНТИФИКАЦИИ ИНФОРМАЦИОННОГО ИСТОЧНИКА С КЛАССАМИ РАСПОЗНАВАНИЯ
03-05-10 13:24:11

Номер анкеты: 6 Наим.физ.источника: 192.168.1.17 Качество результата распознавания: 9.120%

Код	Наименование класса распознавания	% Сх	Гистограмма сходств/различий
14	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС	↓ 66	
22	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00)	↓ 27	
25	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00)	↓ 27	
21	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00)	22	
24	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00)	22	
3	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО	22	
16	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО	22	
2	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС	↓ 17	
19	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев	12	
8	ВИД ПРОБЛЕМЫ-Сбой в работе ОС	9	
15	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС	2	
6	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют	-1	
18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют	-1	
1	ВИД ПРОБЛЕМЫ-Критический сбой в аппаратной части	-5	
13	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части	-5	
20	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00)	-13	
23	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00)	-13	
4	ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечка данных	-14	
17	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности	-14	
5	ВИД ПРОБЛЕМЫ-Потеря данных	-14	
11	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных	-14	
7	ВИД ПРОБЛЕМЫ-Сбой в аппаратной части	-20	
10	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части	-20	
12	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО	-33	
9	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО	-36	

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

Рисунок 7. Пример выходной формы с результатами прогнозирования последствий ошибок в настройках системы безопасности операционной системы

РЕЗУЛЬТАТ ИДЕНТИФИКАЦИИ ИНФОРМАЦИОННОГО ИСТОЧНИКА С КЛАССАМИ РАСПОЗНАВАНИЯ
03-05-10 13:24:11

Номер анкеты: 7 Наим.физ.источника: 192.168.1.18 Качество результата распознавания: 7.210%

Код	Наименование класса распознавания	% Сх	Гистограмма сходств/различий
20	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (2.00, 3.00)....	√ 18	
23	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (2000.00, 3000.00).....	√ 18	
1	ВИД ПРОБЛЕМЫ-Критический сбой в аппаратной части.....	13	
13	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Замена аппаратной части.....	13	
9	ВИД ПРОБЛЕМЫ-Сбой в работе прикладного ПО.....	√ 11	
19	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Устранение сбоев.....	11	
12	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление, настройка ПО.....	√ 11	
4	ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечка данных.....	10	
17	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Повышение защищенности.....	10	
8	ВИД ПРОБЛЕМЫ-Сбой в работе ОС.....	-1	
21	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (3.00, 4.00)....	-3	
24	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (3000.00, 4000.00).....	-3	
15	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка ОС.....	-5	
2	ВИД ПРОБЛЕМЫ-Критический сбой в работе ОС.....	-9	
22	ТРУДОЗАТРАТЫ НА УСТРАНЕНИЕ ПРОБЛЕМЫ (ЧЕЛ/ЧАСОВ): (4.00, 5.00)....	-10	
25	СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): (4000.00, 5000.00).....	-10	
6	ВИД ПРОБЛЕМЫ-Проблемы отсутствуют.....	-10	
18	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Проблемы отсутствуют.....	-10	
5	ВИД ПРОБЛЕМЫ-Потеря данных.....	-13	
11	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление данных.....	-13	
14	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Перестановка ОС.....	-16	
7	ВИД ПРОБЛЕМЫ-Сбой в аппаратной части.....	-16	
10	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Восстановление аппаратной части.....	-16	
3	ВИД ПРОБЛЕМЫ-Критический сбой в работе ПО.....	-23	
16	СПОСОБ УСТРАНЕНИЯ ПРОБЛЕМЫ-Переустановка и настройка ПО.....	-23	

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

Рисунок 8. Пример выходной формы с результатами прогнозирования последствий ошибок в настройках системы безопасности операционной системы

В качестве примеров для прогнозирования последствий ошибок в настройках системы безопасности операционной системы использованы примеры из исходной обучающей выборки. Птичками "√" в формах на рисунках 7, 8 отмечены классы соответствующие реально наступившим последствиям.

Если в распознаваемой выборке представлено сразу несколько примеров настроек системы безопасности операционной системы на различных компьютерах, то может представлять интерес другая форма вывода информации о результатах прогнозирования по ним, т.е. по степени сходства с определенным классом (рисунок 9).

В верхней части этой формы приведены IP-адреса компьютеров, для которых возникновение этой проблема вероятно, если судить по настройкам их системы безопасности, а в нижней – для которых это маловероятно. Видно, что для компьютера с IP-адресом 192.168.0.106 на эту проблему следует обратить внимание, хотя на нем она еще не зафиксирована (хотя, возможно, уже и имела место). И наоборот, на компьютере с IP-адресом 192.168.2.52 эта проблема уже имела место, хотя по своим настройкам он является нетипичным для компьютеров с подобной проблемой.

РЕЗУЛЬТАТ ИДЕНТИФИКАЦИИ ИНФОРМАЦИОННЫХ ИСТОЧНИКОВ С КЛАССОМ РАСПОЗНАВАНИЯ
03-05-10 13:54:13

Класс: 4 ВИД ПРОБЛЕМЫ-Несанкционированный доступ и утечк Качество: 17.86%

Код	Информационный источник	% Сход	Гистограмма сходств/различий
36	192.168.1.47	↓ 63	
231	192.168.0.106	57	
242	10.10.10.13	↓ 23	
284	10.10.200.17	↓ 19	
103	192.168.2.52	↓ -19	
67	192.168.2.16	-57	
84	192.168.2.33	-57	
93	192.168.2.42	-57	
97	192.168.2.46	-57	
98	192.168.2.47	-57	
108	192.168.2.57	-57	
113	192.168.2.62	-57	
116	192.168.2.65	-57	
124	192.168.2.73	-57	
144	192.168.2.93	-57	
61	192.168.2.10	-57	
133	192.168.2.82	-57	
66	192.168.2.15	-61	
115	192.168.2.64	-61	
127	192.168.2.76	-61	
69	192.168.2.18	-61	
122	192.168.2.71	-61	
57	192.168.2.6	-64	
64	192.168.2.13	-64	
71	192.168.2.20	-64	
90	192.168.2.39	-64	
94	192.168.2.43	-64	
95	192.168.2.44	-64	
100	192.168.2.49	-64	
106	192.168.2.55	-64	
117	192.168.2.66	-64	
119	192.168.2.68	-64	
120	192.168.2.69	-64	
128	192.168.2.77	-64	
52	192.168.2.1	-65	
59	192.168.2.8	-65	
60	192.168.2.9	-65	
63	192.168.2.12	-65	
77	192.168.2.26	-65	
91	192.168.2.40	-65	
104	192.168.2.53	-65	
105	192.168.2.54	-65	
110	192.168.2.59	-65	
111	192.168.2.60	-65	
118	192.168.2.67	-65	
121	192.168.2.70	-65	

Универсальная когнитивная аналитическая система НПП *ЭЙДОС*

Рисунок 9. Пример карточки идентификации примеров с классом: «Несанкционированный доступ и утечка данных»

6.2. **Задача 3:** "Разработка методики ***поддержки принятия решений*** о выборе таких настроек системы безопасности операционной системы, которые по опыту фактически минимизируют проблемы безопасности".

Данная задача является обратной по отношению к задаче прогнозирования. Если при прогнозировании по заданным настройкам системы безопасности операционной системы определяется, какие проблемы с информационной безопасностью ими обусловливаются, то в задаче принятия

решений, наоборот: по заданному виду проблемы или ее отсутствию определяется, какие настройки системы безопасности способствуют возникновению этой проблемы, а какие препятствуют этому.

Данная задача решается во многих режимах системы "Эйдос", в частности в режиме _511, который выдает следующие формы (таблицы 9 и 10), содержащие ***знания*** о настройках системы безопасности операционной системы в различной степени способствующих и препятствующих (красным) возникновению данной проблемы.

Таблица 9 – ИНФОРМАЦИОННЫЙ ПОРТРЕТ КЛАССА: СТОИМОСТЬ УСТРАНЕНИЯ ПРОБЛЕМЫ (РУБ.): {4000.00, 5000.00} (МАКСИМАЛЬНАЯ)

NUM	KOD	NAME	BIT	%
1	5	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {110.34, 1	0,73444	15,82
2	8	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {75.00, 112	0,69191	14,90
3	4	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {55.67, 11	0,33335	7,18
4	2	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Отключено	0,24972	5,38
5	9	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.00, 1.67}	0,23148	4,98
6	34	ТИП ФАЙЛОВОЙ СИСТЕМЫ-FAT	0,23148	4,98
7	13	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.67, 2.34}	0,21342	4,60
8	11	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {2.34, 3.01}	0,21121	4,55
9	14	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {2.34, 3.01}	0,18162	3,91
10	10	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.67, 2.34}	0,12490	2,69
11	31	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет	0,11768	2,53
12	33	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет	0,11768	2,53
13	7	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {38.00, 75.	0,11729	2,53
14	26	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Отключено	0,08945	1,93
15	19	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {4.00, 5.33}	0,01110	0,24
16	16	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Нет	0,00961	0,21
17	17	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Да	0,00904	0,19
18	35	ТИП ФАЙЛОВОЙ СИСТЕМЫ-NTFS	-0,04930	-1,06
19	18	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Нет	-0,05783	-1,25
20	29	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {4.34, 5.01}	-0,06366	-1,37
21	6	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {1.00, 38.0	-0,07701	-1,66
22	12	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.00, 1.67}	-0,13895	-2,99
23	32	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да	-0,14448	-3,11
24	27	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {3.00, 3.67}	-0,14886	-3,21
25	15	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Да	-0,15535	-3,35
26	30	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да	-0,15535	-3,35
27	25	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Включено	-0,31834	-6,86
28	3	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {1.00, 55.	-0,33108	-7,13
29	22	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {5.00, 36.33}	-0,63915	-13,76
30	1	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Включено	-1,14679	-24,69

Таблица 10 – ИНФОРМАЦИОННЫЙ ПОРТРЕТ КЛАССА: ВИД ПРОБЛЕМЫ-Проблемы отсутствуют

NUM	KOD	NAME	BIT	%
1	20	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {5.33, 6.66}	0,27719	5,97
2	23	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {36.33, 67.66}	0,27719	5,97
3	24	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {67.66, 98.99}	0,27719	5,97
4	1	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Включено	0,23382	5,04
5	22	МАКСИМАЛЬНЫЙ СРОК ДЕЙСТВИЯ ПАРОЛЯ: {5.00, 36.33}	0,18720	4,03
6	25	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Включено	0,16777	3,61
7	27	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {3.00, 3.67}	0,12257	2,64
8	3	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {1.00, 55.	0,09169	1,97
9	18	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Нет	0,08344	1,80
10	31	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет	0,07726	1,66
11	33	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Нет	0,07726	1,66
12	6	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {1.00, 38.0	0,07416	1,60
13	12	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.00, 1.67}	0,05519	1,19
14	35	ТИП ФАЙЛОВОЙ СИСТЕМЫ-NTFS	0,02760	0,59
15	16	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Нет	0,02455	0,53
16	14	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {2.34, 3.01}	0,00659	0,14
17	29	ПОРОГОВОЕ ЗНАЧЕНИЕ БЛОКИРОВКИ: {4.34, 5.01}	-0,03192	-0,69
18	13	КОЛИЧЕСТВО ПАРОЛЕЙ С НЕОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ: {1.67, 2.34}	-0,05459	-1,18
19	17	ВКЛЮЧЕНА УЧЕТНАЯ ЗАПИСЬ ГОСТЬ-Да	-0,06410	-1,38
20	30	РАЗРЕШИТЬ ДОСТУП К FDD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да	-0,06565	-1,41
21	32	РАЗРЕШИТЬ ДОСТУП К CD ТОЛЬКО ЛОКАЛЬНЫМ ПОЛЬЗОВАТЕЛЯМ-Да	-0,06758	-1,46
22	10	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.67, 2.34}	-0,08989	-1,94
23	19	МИНИМАЛЬНАЯ ДЛИНА ПАРОЛЯ: {4.00, 5.33}	-0,10387	-2,24
24	15	НАЛИЧИЕ БОЛЕЕ ДВУХ УЧЕТНЫХ ЗАПИСЕЙ АДМИНИСТРАТОРА-Да	-0,10964	-2,36
25	26	ПАРОЛЬ ДОЛЖЕН ОТВЕЧАТЬ ТРЕБОВАНИЯМ СЛОЖНОСТИ-Отключено	-0,11253	-2,42
26	9	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {1.00, 1.67}	-0,11942	-2,57
27	11	КОЛИЧЕСТВО СЛАБЫХ ЛИБО ПУСТЫХ ПАРОЛЕЙ: {2.34, 3.01}	-0,25724	-5,54
28	2	СИСТЕМА АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ-Отключено	-0,29830	-6,42
29	7	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {38.00, 75.	-0,34314	-7,39
30	34	ТИП ФАЙЛОВОЙ СИСТЕМЫ-FAT	-0,39002	-8,40
31	4	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS WINDOWS: {55.67, 11	-0,41485	-8,93
32	8	КОЛ-ВО НЕУСТАНОВЛЕННЫХ ОБНОВЛ.БЕЗОПАСНОСТИ MS OFFICE: {75.00, 112	-0,54358	-11,71

Необходимо отметить, что задача выявления фактически имеющихся зависимостей, и задача содержательного объяснения причин существования именно обнаруженных зависимостей, а не каких-либо других, т.е. задача ***содержательной интерпретации обнаруженных зависимостей***, – это совершенно разные задачи. По мнению авторов, задача интерпретации должна решаться специалистами в моделируемой предметной области, однако сама возможность применения обнаруженных зависимостей в практике прогнозирования и принятия решений не связано с наличием или отсутствием такой содержательной интерпретации или со степенью ее адекватности.

6.3. **Задача 4:** «Исследование предметной области» решается применением режимов системы «Эйдос», предназначенных для этих целей, которые приведены в работе [1]. Подробные примеры применения этих режимов приведены в работах [2-14]. Классификация исследовательских задач, которые могут решаться с применением системы «Эйдос», приведена в работе [17]. Здесь же отметим лишь, что задачи проблемы, связанные с информационной безопасностью (как впрочем, и другие) обычно возникают не по одной, а сразу несколько, т.к. одни и те же погрешности системы защиты приводят не к одной, а ко многим проблемам. Это наглядно видно

из семантической сети классов, построенной на основе матрицы сходства обобщенных образов классов по их системам детерминации (рисунок 10).

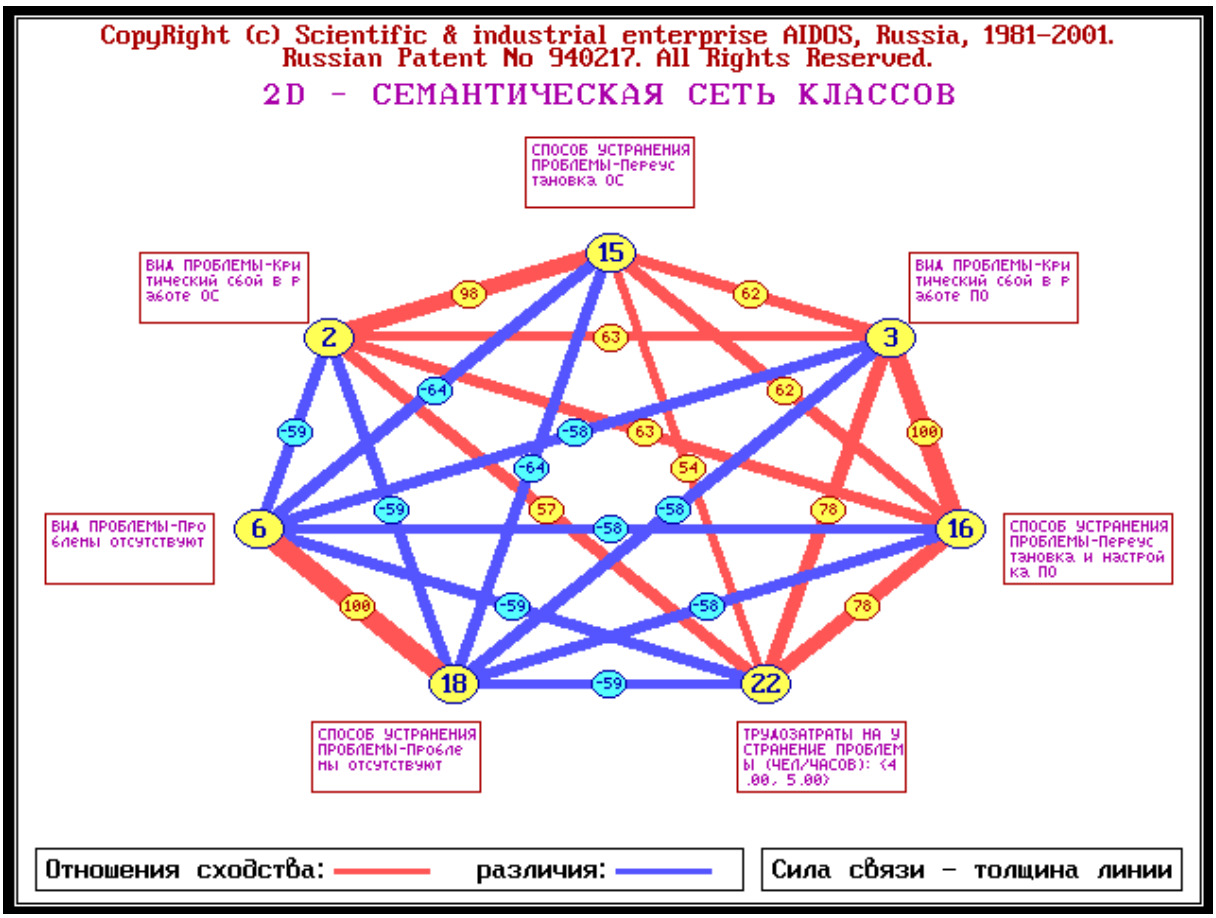


Рисунок 10. Семантическая сеть классов

7. Основной принцип оценки экономической эффективности разработанной методики (при условии ее применения в деятельности реальной фирмы) состоит в том, что данная методика позволяет создать научно обоснованный *образ желательных настроек системы безопасности* (как и образ нежелательных), за счет чего минимизируются затраты на устранение проблем, связанных с нарушением информационной безопасность компьютеров, а значит рентабельность и прибыль компании повысится. Экономическая эффективность применения данной методики может оцениваться как разница между прибылью, полученной в условиях ее применения и прибылью без нее, причем прибыль, полученная в условиях применения методики учитывает и затраты на ее приобретение и применение.

8. При планировании данного исследования авторы ставили цель лишь оценить возможность применения технологии СК-анализа для прогнозирования последствий ошибочного конфигурирования системы безопасности MS Windows. Данное исследование показало, что это возможно и перспективно. Представленный в работе вариант исследования имеет ряд

ограничений и недостатков, в преодолении которых и состоит перспектива его развития. В частности можно было бы увеличить объем исследуемой выборки за счет увеличения количества компьютеров и периода времени, за который исследуется деятельность фирмы. Кроме того известно, что Microsoft Baseline Security Analyzer (MBSA) является лишь базовым средством обеспечения информационной безопасности MS Windows, позволяющим выявлять лишь наиболее явные ошибки в застройках системы безопасности, и, следовательно, перспективным является развитие предлагаемой методики с использованием и специальных профессиональных средств.

Выводы.

В статье описана технология и некоторые результаты применения системно-когнитивного анализа для выявления знаний о последствиях ошибок в конфигурировании системы безопасности по отчету Microsoft Baseline Security Analyzer (MBSA) и использования этих знаний для прогнозирования последствий.

Литература[3]

1. Луценко Е.В. 30 лет системе «Эйдос» – одной из старейших отечественных универсальных систем искусственного интеллекта, широко применяемых и развивающихся и в настоящее время / Е.В. Луценко // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2009. – №10(54). – Шифр Информрегистра: 0420900012\0110. – Режим доступа: http://ej.kubagro.ru/2009/10/pdf/04.pdf
2. Луценко Е.В. Универсальная автоматизированная система распознавания образов "Эйдос" (версия 4.1): Монография (научное издание). – Краснодар: КЮИ МВД РФ, 1995. –76с.
3. Луценко Е.В. Теоретические основы и технология адаптивного семантического анализа в поддержке принятия решений (на примере универсальной автоматизированной системы распознавания образов "ЭЙДОС-5.1"): Монография (научное издание). – Краснодар: КЮИ МВД РФ, 1996. –280с.
4. Симанков В.С., Луценко Е.В. Адаптивное управление сложными системами на основе теории распознавания образов: Монография (научное издание). – Краснодар: ТУ КубГТУ, 1999. –318с.
5. Симанков В.С., Луценко Е.В., Лаптев В.Н. Системный анализ в адаптивном управлении: Монография (научное издание). /Под науч. ред. В.С.Симанкова. – Краснодар: ИСТЭК КубГТУ, 2001. –258с.
6. Луценко Е.В. Автоматизированный системно-когнитивный анализ в управлении активными объектами (системная теория информации и ее применение в исследовании экономических, социально-психологических, технологических и организационно-технических систем): Монография (научное издание). – Краснодар: КубГАУ. 2002. – 605с.
7. Луценко Е.В. Интеллектуальные информационные системы: Учебное пособие с грифом УМО для студентов специальности 351400 "Прикладная информатика (по отраслям)". – Краснодар: КубГАУ. 2004. – 633с.

[3] Для удобства читателей эти работы размещены на его сайтах: http://lc.kubagro.ru и http://lc.narod.ru

8. Луценко Е.В., Лойко В.И., Семантические информационные модели управления агропромышленным комплексом: Монография (научное издание). – Краснодар: КубГАУ. 2005. –480с.
9. Луценко Е.В. Интеллектуальные информационные системы: Учебное пособие с грифом министерства для студентов специальности "Прикладная информатика (по областям)" и другим экономическим специальностям. 2-е изд., перераб. и доп.– Краснодар: КубГАУ, 2006. –615с.
10. Луценко Е.В. Лабораторный практикум по интеллектуальным информационным системам: Учебное пособие с грифом министерства для студентов специальности "Прикладная информатика (по областям)" и другим экономическим специальностям. 2-е изд., перераб. и доп. – Краснодар: КубГАУ, 2006. – 318с.
11. Наприев И.Л., Луценко Е.В., Чистилин А.Н. Образ-Я и стилевые особенности деятельности сотрудников органов внутренних дел в экстремальных условиях: Монография (научное издание). – Краснодар: КубГАУ. 2008. –262с.
12. Луценко Е. В., Лойко В.И., Великанова Л.О. Прогнозирование и принятие решений в растениеводстве с применением технологий искусственного интеллекта: Монография (научное издание). – Краснодар: КубГАУ, 2008. –257с.
13. Трунев А.П., Луценко Е.В. Астросоциотипология: Монография (научное издание). – Краснодар: КубГАУ, 2008. –264с.
14. Луценко Е.В., Коржаков В.Е., Лаптев В.Н. Теоретические основы и технология применения системно-когнитивного анализа в автоматизированных системах обработки информации и управления (АСОИУ) (на примере АСУ вузом): Под науч. ред. д.э.н., проф. Е.В.Луценко. Монография (научное издание). – Майкоп: АГУ. 2009. – 536 с.
15. Луценко Е.В. Системно-когнитивный анализ как развитие концепции смысла Шенка – Абельсона / Е.В. Луценко // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2004. – №03(5). – Режим доступа: http://ej.kubagro.ru/2004/03/pdf/04.pdf
16. Луценко Е.В. Расчет эластичности объектов информационной безопасности на основе системной теории информации. //Ж-л "Безопасность информационных технологий". – М.: МИФИ, 2003. – №2. – С. 82-90.[4]
17. Луценко Е.В. Исследование двухуровневой семантической информационной модели агропромышленного холдинга / Е.В. Луценко, В.И. Лойко, О.А. Макаревич // Научный журнал КубГАУ [Электронный ресурс]. – Краснодар: КубГАУ, 2008. – №08(42). – Шифр Информрегистра: 0420800012\0118. – Режим доступа: http://ej.kubagro.ru/2008/08/pdf/03.pdf

[4] http://ej.kubagro.ru/2003/01/05/p05.asp