Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет математики и информационных технологий

Кафедра вычислительной техники и защиты информации

Разработка метода контроля поведения пользователя на основе ассоциативной модели

ОГУ 10.03.01.62.5318.014 ПЗ

Руководитель
д.т.н., профессор
Т.З. Аралбаев
Исполнитель
студент гр. 14ИБ(б)КЗОИ
М.Д. Хатеев

Оренбург 2018

Постановка задачи:

Цель работы: снижение риска от несанкционированных действий пользователя в компьютерной системе.

Для достижения поставленной цели необходимо решить следующие задачи:

1 Обосновать актуальность темы исследования;

2 Провести аналитический обзор патентной и периодической литературы по теме работы;

3 Разработать классификацию пользователей компьютерной системы;

4 Разработать модель нарушителя и модель угроз информационной безопасности компьютерной системы на примере «Межрайонной ИФНС России №6 по Оренбургской области»;

5 Разработать концепцию контроля поведения пользователя в компьютерной системе;

6 Разработать технико-экономическое обоснование на разработку метода контроля поведения пользователя в компьютерной системе;

7 Разработать математическую модель контроля поведения пользователя в компьютерной системе;

8 Разработать структурную схему устройства для контроля поведения пользователя;

9 Разработать схему алгоритма программы «Эмулятор устройства для контроля поведения пользователя»;

10 Разработать прикладную программу «Эмулятор устройства для контроля поведения пользователя»

11 Рассчитать экономические показатели проекта.

Задача 3. Разработать классификацию пользователей компьютерной системы

Классификация пользователей компьютерной системы по уровням их квалификации представлена на рисунке 2.

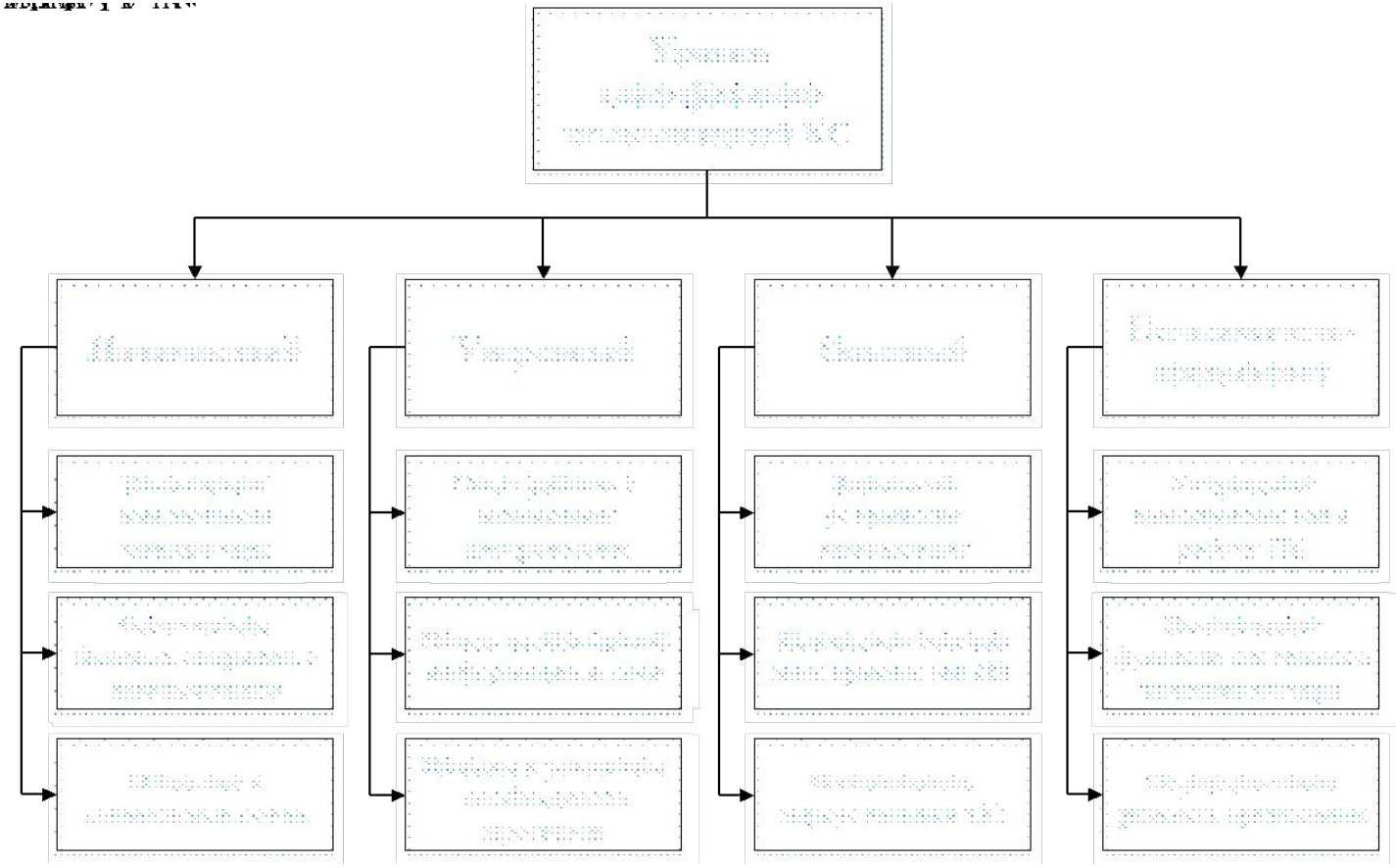


Рисунок 2 - Классификация пользователей компьютерной системы по уровням их квалификации

Задача 5. Разработать концепцию контроля поведения пользователя в компьютерной системе

На рисунке 3 представлена концептуальная модель контроля поведения пользователя.

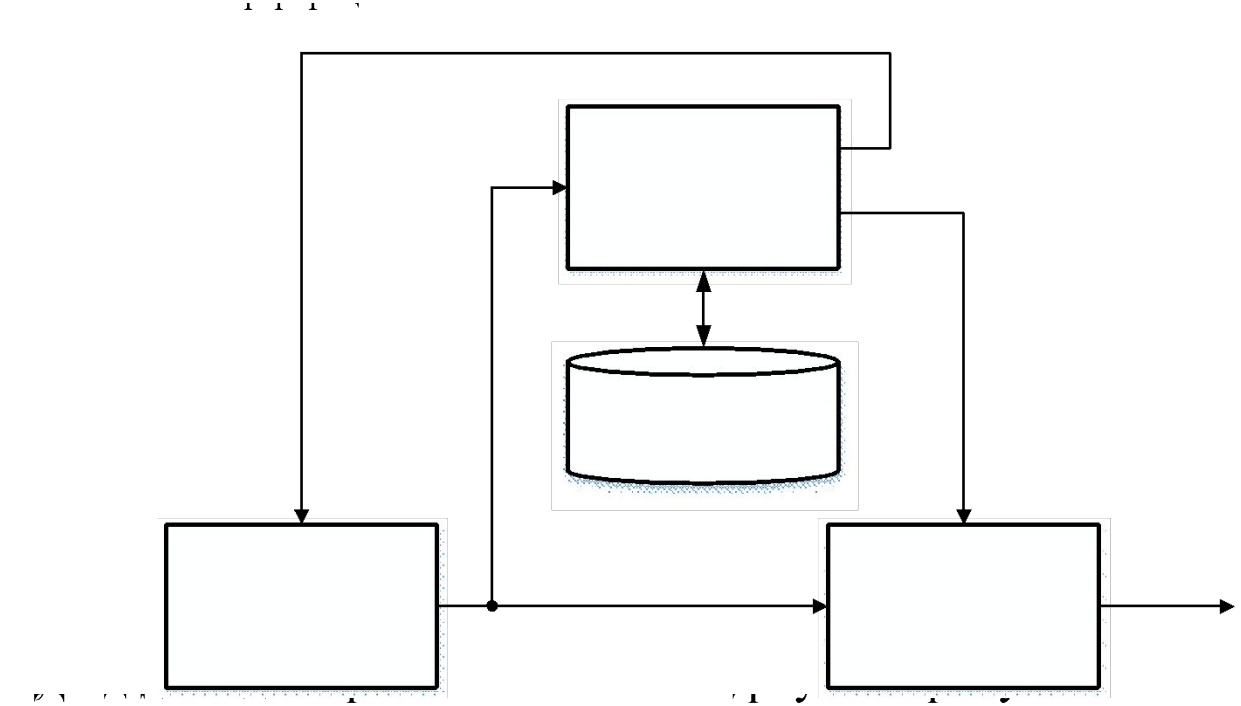


Рисунок 3 – Концептуальная модель контроля поведения пользователя

Задача 7. Разработать математическую модель контроля поведения пользователя в компьютерной системе

К исходным данным задачи контроля поведения пользователя относятся:

$\boldsymbol{Q = \{q_1, q_2, \ldots, q_j, \ldots q_N\}}$ - множество контролируемых транзакций, выполняемых пользователем;

$\boldsymbol{P = \{p_1, p_2, \ldots, p_i, \ldots p_M\}}$ - множество информативных признаков, в частности:

K - код транзакции,

NO - номер операции в транзакции,

KOT - код операции транзакции.

Математическая модель мониторинга поведения пользователя описывает модель контроля набираемых пользователем признаков: ***K***, ***NO***, ***KOT*** в конкретный момент времени ***t***.

Совокупный признак ***P(t)*** имеет следующий вид:

$$\boldsymbol{P(t)=(K\_NO\_KOT)_t}.$$

В каждый момент времени ***t*** совокупный признак ассоциируется (≡) с кодом соответствующей легитимной (правомерной) операции $\boldsymbol{<KOT>_t}$, хранящейся в блоке ассоциативной памяти:

$$\boldsymbol{(K\_NO\_KOT)_t \equiv <KOT>_t}$$

В случае отсутствия ассоциации производится запрет на ввод следующей операции.

Задача 8. Разработать структурную схему устройства для контроля поведения пользователя

На рисунке 4 представлена структурная схема устройства для контроля поведения пользователя.

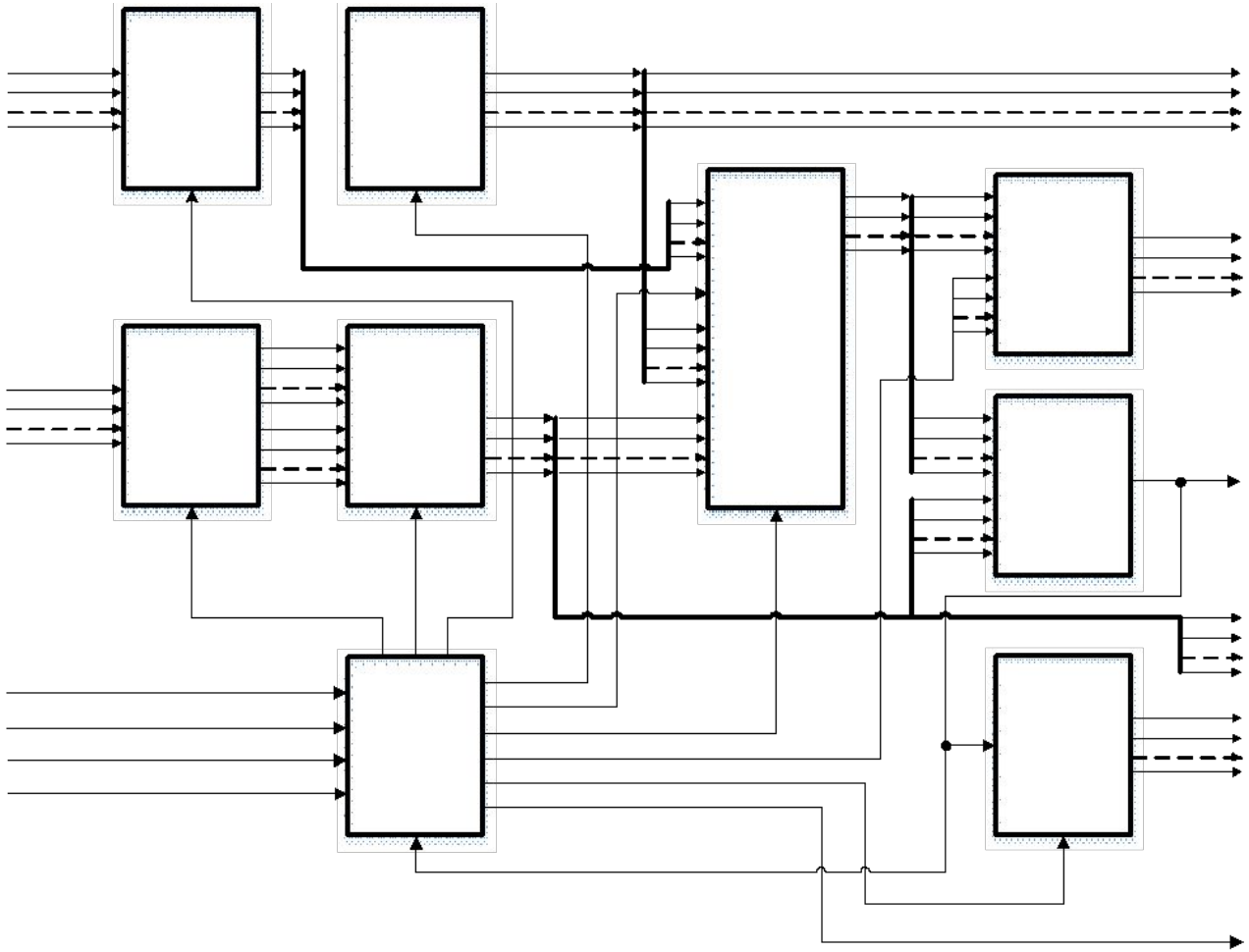


Рисунок 4 – Структурная схема устройства для контроля поведения пользователя

Задача 8. Разработать структурную схему устройства для контроля поведения пользователя (Продолжение)

В таблице 5 представлено содержимое блока памяти в режиме контроля.

Таблица 5 - Содержимое блока памяти в режиме контроля

№	Адресная часть										Данные			Корректность	Команда
	A			B	C			D			E			F	G
0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	не исп.
1	0	0	1	1	0	0	1	1	0	0	1	0	0	0	К
2	0	0	1	1	0	1	0	1	0	1	1	0	1	0	О
3	0	0	1	1	0	1	1	0	1	0	0	1	0	0	Ж
4	0	0	1	1	1	0	0	0	1	1	0	1	1	0	З
5	0	0	1	1	1	0	1	0	0	1	0	0	1	0	Г
6	0	0	1	1	1	1	0	1	1	0	1	1	0	0	С
7	0	0	1	1	1	1	1	1	1	1	1	1	1	0	Ф

A - код транзакции;
B - режим работы устройства;
C - код адреса;
D - код команды.

Задача 9. Разработать схему алгоритма программы «Эмулятор устройства для контроля поведения пользователя»

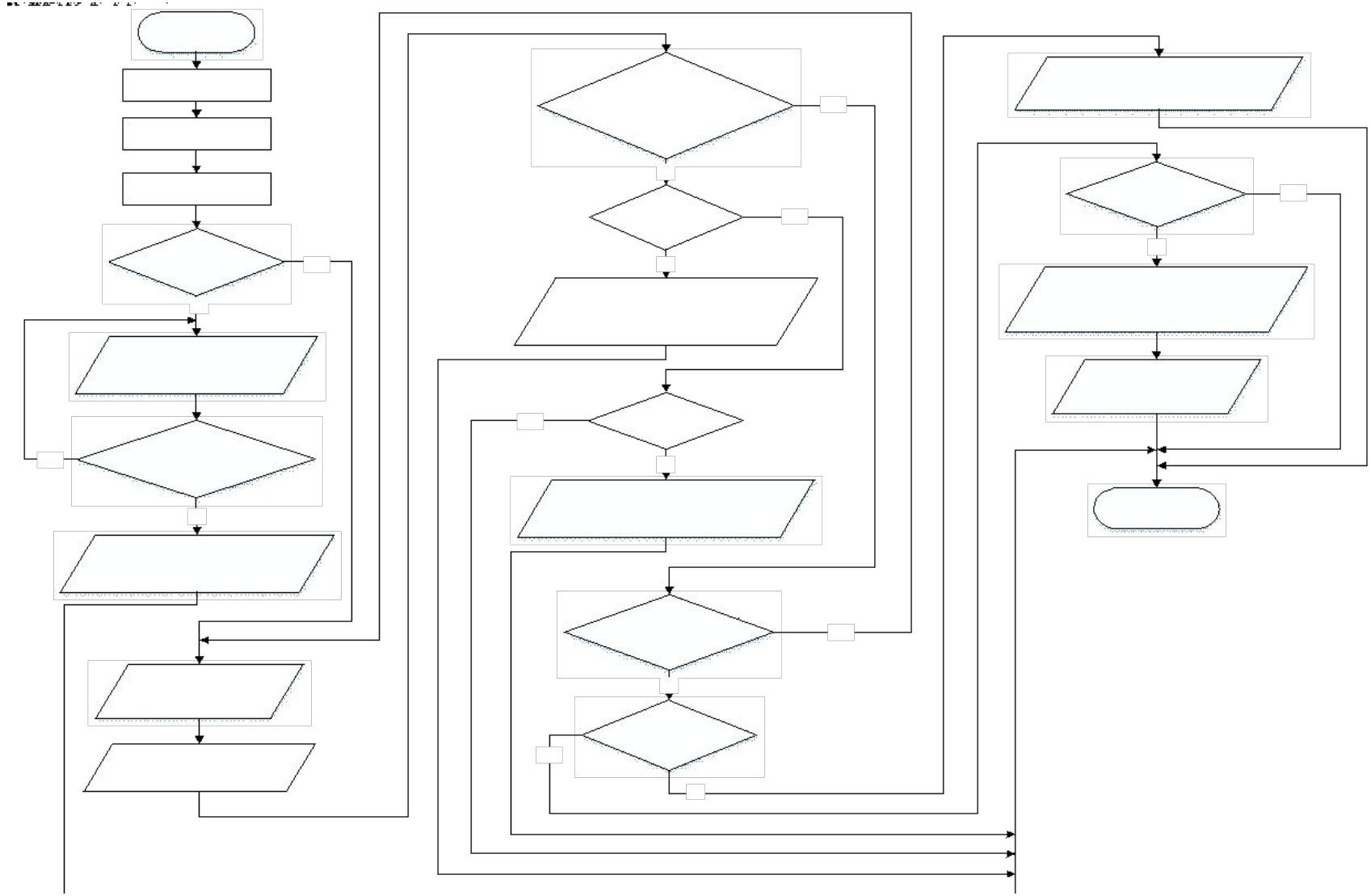


Рисунок 5 – Схема алгоритма программы «Эмулятор устройства для контроля поведения пользователя»

Задача 10. Разработать прикладную программу «Эмулятор устройства для контроля поведения пользователя»

На рисунке 6 представлена экранная форма главного окна программы «Эмулятор устройства для контроля поведения пользователя»

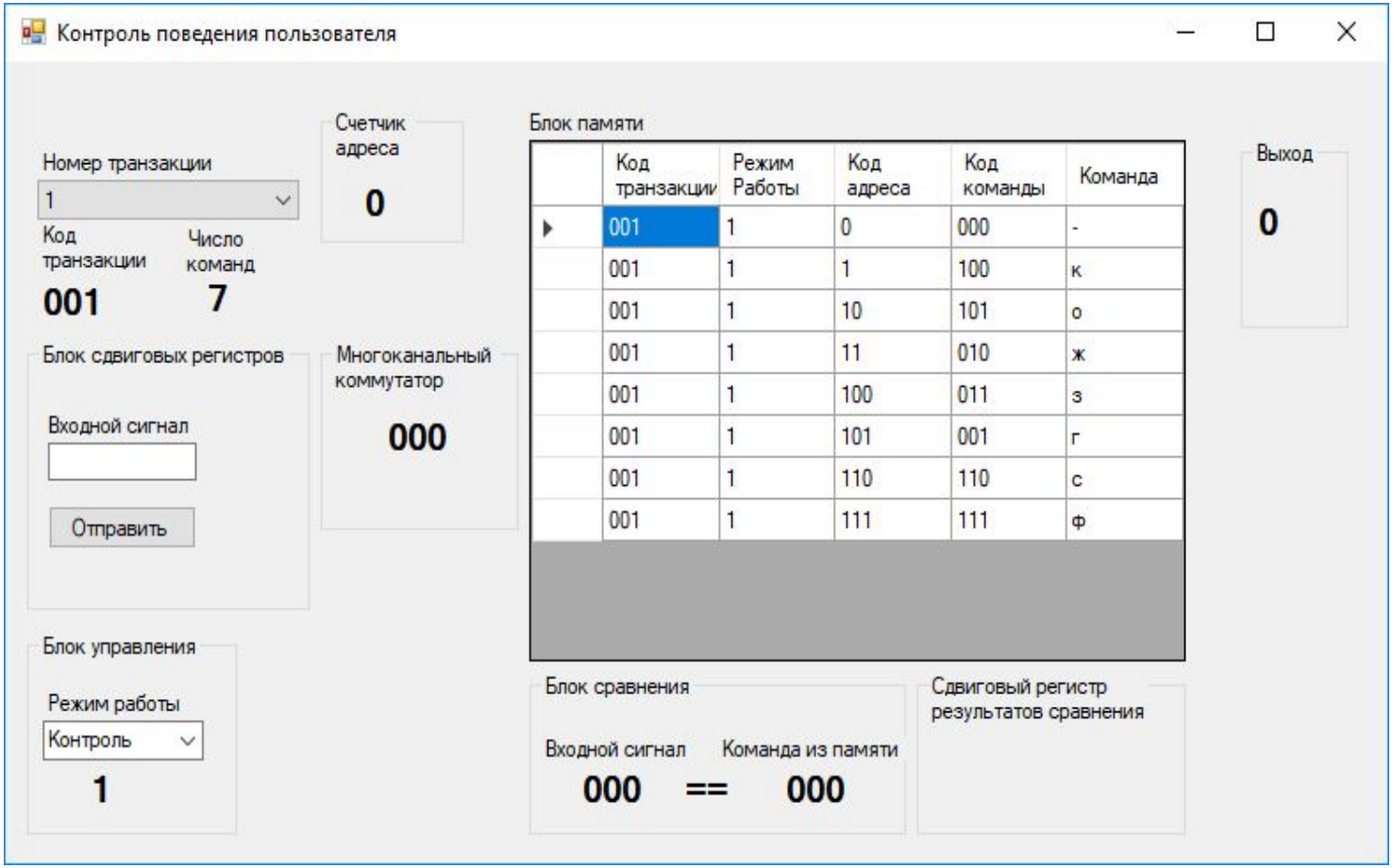


Рисунок 6 – Экранная форма главного окна программы «Эмулятор устройства для контроля поведения пользователя»

Задача 10. Разработать прикладную программу «Эмулятор устройства для контроля поведения пользователя» (Продолжение)

На рисунке 7 представлен пример работы программы «Эмулятор устройства для контроля поведения пользователя» в режиме контроля.

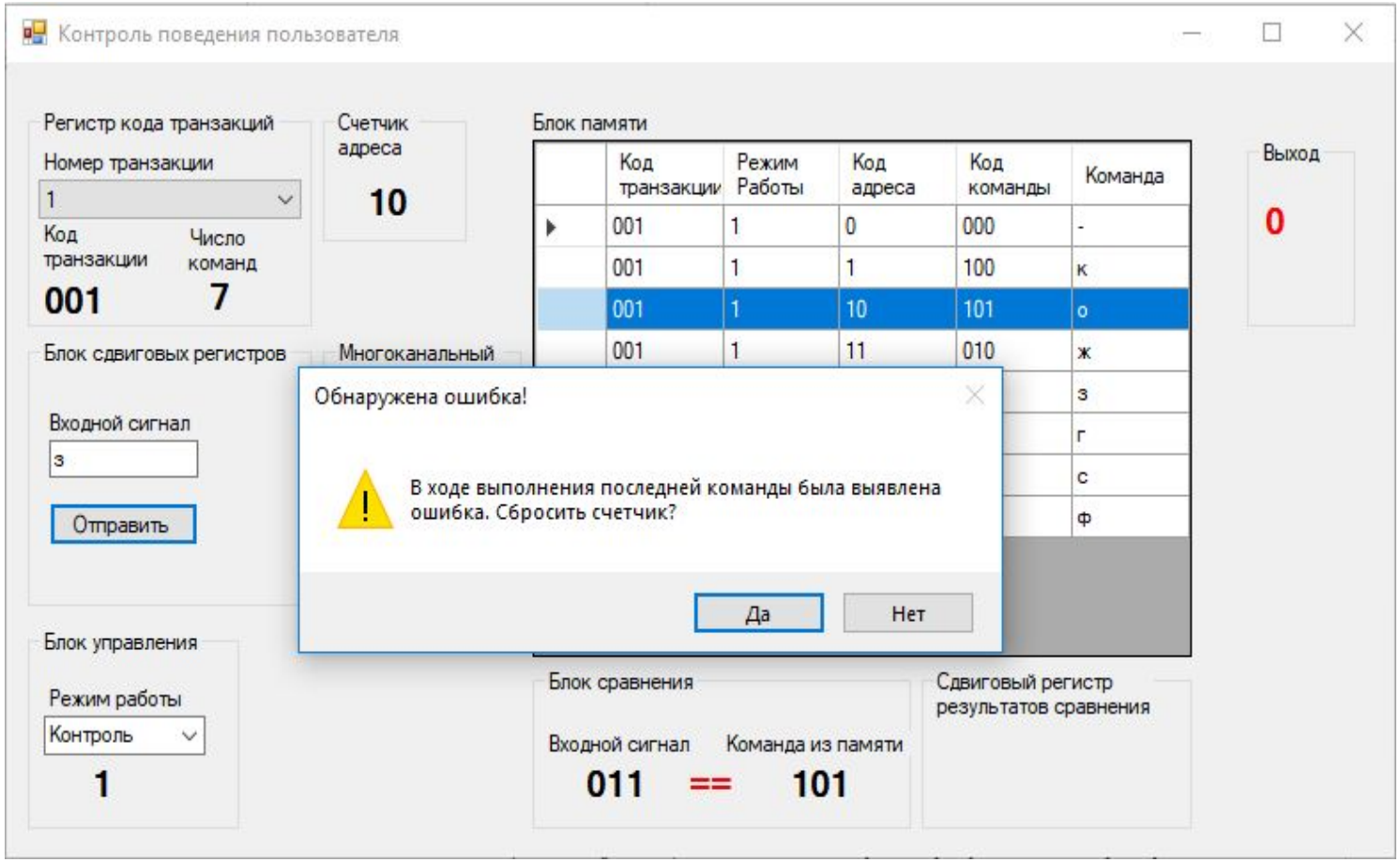
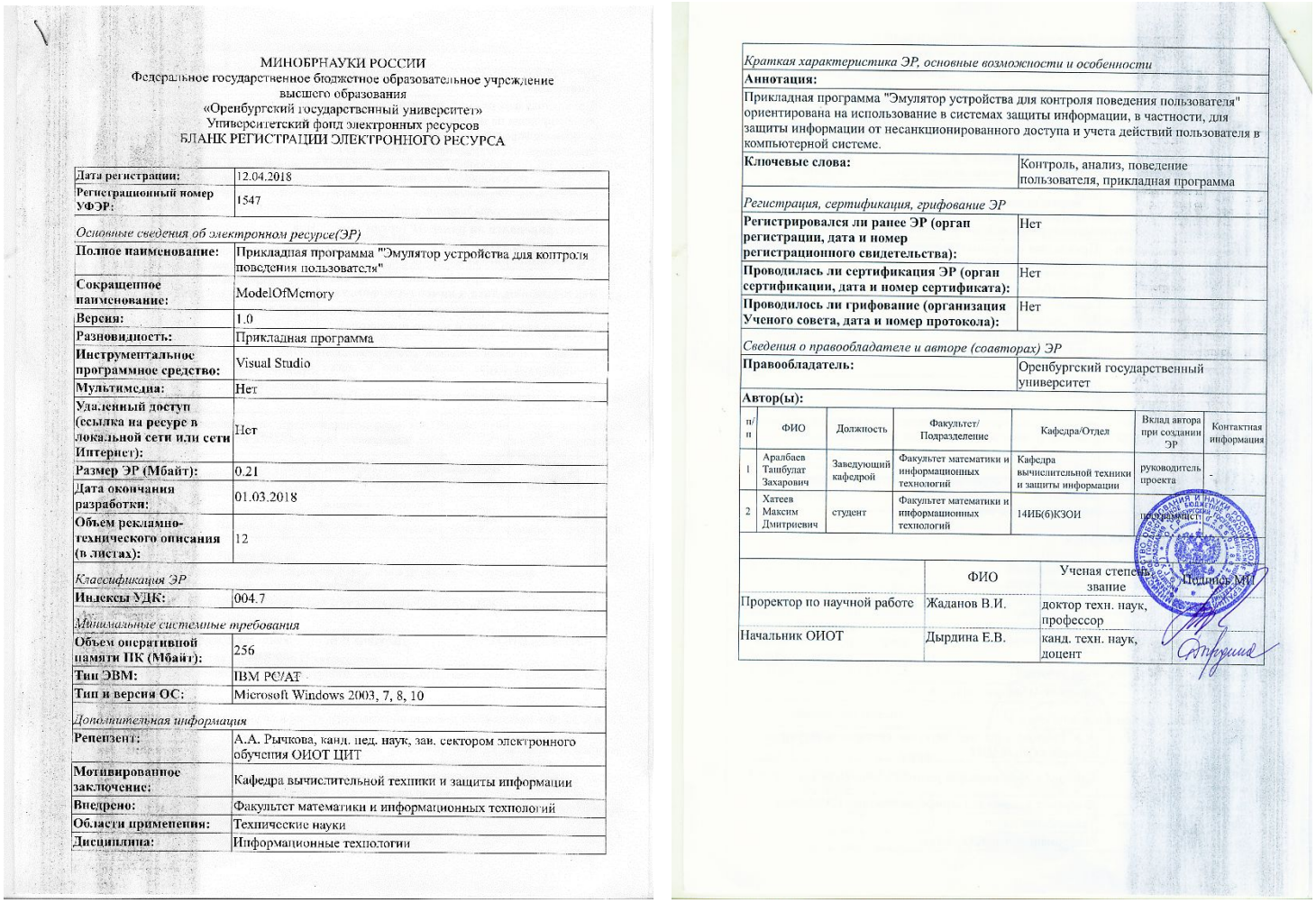


Рисунок 7 – Пример работы программы в режиме «Контроль»

Задача 10. Разработать прикладную программу «Эмулятор устройства для контроля поведения пользователя» (Продолжение)

На рисунке 8 представлен бланк регистрации программы в университетском фонде электронных ресурсов.



МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»
Университетский фонд электронных ресурсов
БЛАНК РЕГИСТРАЦИИ ЭЛЕКТРОННОГО РЕСУРСА

Дата регистрации:	12.04.2018
Регистрационный номер УФЭР:	1547
Основные сведения об электронном ресурсе(ЭР)	
Полное наименование:	Прикладная программа "Эмулятор устройства для контроля поведения пользователя"
Сокращенное наименование:	ModelOfMemory
Версия:	1.0
Разновидность:	Прикладная программа
Инструментальное программное средство:	Visual Studio
Мультимедиа:	Нет
Удаленный доступ (ссылка на ресурс в локальной сети или сети Интернет):	Нет
Размер ЭР (Мбайт):	0.21
Дата окончания разработки:	01.03.2018
Объем рекламно-технического описания (в листах):	12
Классификация ЭР	
Индексы УДК:	004.7
Минимальные системные требования	
Объем оперативной памяти ПК (Мбайт):	256
Тип ЭВМ:	IBM PC/AT
Тип и версия ОС:	Microsoft Windows 2003, 7, 8, 10
Дополнительная информация	
Репензент:	А.А. Рычкова, канд. пед. наук, зав. сектором электронного обучения ОИОТ ЦИТ
Мотивированное заключение:	Кафедра вычислительной техники и защиты информации
Внедрено:	Факультет математики и информационных технологий
Область применения:	Технические науки
Дисциплина:	Информационные технологии

Краткая характеристика ЭР, основные возможности и особенности

Аннотация:

Прикладная программа "Эмулятор устройства для контроля поведения пользователя" ориентирована на использование в системах защиты информации, в частности, для защиты информации от несанкционированного доступа и учета действий пользователя в компьютерной системе.

Ключевые слова:	Контроль, анализ, поведение пользователя, прикладная программа
Регистрация, сертификация, грифование ЭР	
Регистрировался ли ранее ЭР (орган регистрации, дата и номер регистрационного свидетельства):	Нет
Проводилась ли сертификация ЭР (орган сертификации, дата и номер сертификата):	Нет
Проводилось ли грифование (организация Ученого совета, дата и номер протокола):	Нет
Сведения о правообладателе и авторе (соавторах) ЭР	
Правообладатель:	Оренбургский государственный университет

Автор(ы):

п/п	ФИО	Должность	Факультет/ Подразделение	Кафедра/Отдел	Вклад автора при создании ЭР	Контактная информация
1	Аралбаев Ташбулат Захарович	Заведующий кафедрой	Факультет математики и информационных технологий	Кафедра вычислительной техники и защиты информации	руководитель проекта	-
2	Хатеев Максим Дмитриевич	студент	Факультет математики и информационных технологий	14ИБ(б)КЗОИ	программист	

	ФИО	Ученая степень, звание	Подпись МП
Проректор по научной работе	Жаданов В.И.	доктор техн. наук, профессор	
Начальник ОИОТ	Дырдина Е.В.	канд. техн. наук, доцент	

Рисунок 8 – Бланк регистрации электронного ресурса

Заключение

В ходе выполнения курсового проекта была достигнута цель, а именно: снижение риска от несанкционированных действий пользователя в компьютерной системе, а также выполнены следующие задачи:

1 Обоснована актуальность темы исследования, в результате чего было выявлено, что угроза несанкционированного доступа со стороны пользователей компьютерной системы занимает первое место среди угроз информационной безопасности компьютерной системы;

2 Проведен аналитический обзор патентной и периодической литературы, посвященной методам контроля поведения пользователя;

3 Разработана классификация пользователей компьютерной системы. По уровням квалификации различают следующих пользователей: начинающий пользователь, уверенный пользователь, опытный пользователь, пользователь-специалист;

4 Разработана модель нарушителя и модель угроз информационной безопасности компьютерной системы на примере «Межрайонной России ИФНС №6 по Оренбургской области»;

5 Разработана концепция контроля поведения пользователя в компьютерной системе;

6 Разработано технико-экономическое обоснование на разработку метода контроля поведения пользователя в компьютерной системе;

7 Разработана математическая модель контроля поведения пользователя в компьютерной системе;

8 Разработана структурная схема устройства для контроля поведения пользователя;

9 Разработана схема алгоритма программы «Эмулятор устройства для контроля поведения пользователя»;

10 Разработана прикладная программа «Эмулятор устройства для контроля поведения пользователя»;

11 Рассчитаны экономические показатели проекта.