МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Автоматизированные системы управления»

# ТЕХНОЛОГИИ ПОИСКА, ПЕРЕДАЧИ И ЗАЩИТЫ ДАННЫХ

***Методические рекомендации к лабораторным работам для студентов специальности 1-40 80 02 «Системный анализ, управление и обработка информации» дневной и заочной форм обучения***


Могилев 2020

УДК 004.4
ББК 32.973.2
Т38

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Автоматизированные системы управления» «14» апреля 2020 г., протокол № 9

Составители: канд. физ.-мат. наук, доц. В. А. Ливинская;
канд. техн. наук, доц. В. М. Ковальчук

Рецензент С. В. Болотов

Методические рекомендации предназначены для студентов специальности 1-40 80 02 «Системный анализ, управление и обработка информации» дневной и заочной форм обучения

Учебно-методическое издание

# ТЕХНОЛОГИИ ПОИСКА, ПЕРЕДАЧИ И ЗАЩИТЫ ДАННЫХ

| | |
|---|---|
| Ответственный за выпуск | А. И. Якимов |
| Корректор | А. А. Подошевко |
| Компьютерная верстка | Н. П. Полевничая |

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 16 экз. Заказ №

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, Могилев.

# Содержание

# Введение

Цель методических рекомендаций к лабораторным работам по дисциплине «Технологии поиска, передачи и защиты данных» заключается в овладении студентами практическими навыками результативного применения существующих и новых информационных технологий, формирование у студентов представления о роли информационных технологий в цифровой экономике.

Дисциплина «Технологии поиска, передачи и защиты информации» является неотъемлемой частью современных знаний и связана с рядом других дисциплин: «Информатика», «Системы аналитического программирования». Выполнение заданий позволит студентам выработать практические навыки работы с основными программными средствами технологий поиска, передачи и управления информационной безопасностью.

В процессе выполнения лабораторной работы студенты знакомятся с теоретическим материалом, методами решения задач, выполняют индивидуальное задание и оформляют отчет.

Отчет содержит: название и цель лабораторной работы, структуру и листинг электронных документов и анализ полученных результатов и выводы. В отчете можно привести также ответы на наиболее сложные вопросы, приведенные в конце каждой работы.

# 1 Лабораторная работа № 1. Основы искусственного интеллекта

**Цель работы**: ознакомиться с примерами использования искусственного интеллекта в финансовых технологиях.

Понятие искусственного интеллекта (ИИ) появилось более 60 лет назад и описывается как разработка компьютерных систем, способных выполнять задачи, которые обычно требуют человеческого интеллекта.

Однако, эта технология не появлялась в мире финансовых услуг до начала 1980-х гг. После короткого периода «великой иллюзии» она практически была забыта, но теперь вновь набирает стремительные обороты.

На протяжении многих лет искусственный интеллект прошел этапы и большого воодушевления, и инвестиций со стороны предприятий, и разочарования, когда только университеты продолжали исследования в этом направлении.

В начале 1980 г., например, инвестиционный банк «Ситибанк» [1] попробовал построить несколько системных экспертов, используя одну из ветвей искусственного интеллекта, которая должна была обладать способностью принятия решений на уровне эксперта-человека. Он стал не единственным.

В 1987 г. национальный банк SP [1] запустил программу для предотвращения мошенничества, направленную на автоматическое посредством применения искусственного интеллекта противодействие несанкционированному использованию дебетовых карт в банкоматах и магазинах .

Все эти проекты дали некоторые полезные результаты, в частности, за счет применения систем искусственных нейронных сетей для автоматического обнаружения необычных действий и процессов, которые в дальнейшем могли быть исследованы человеком.

Несмотря на первые успехи, вскоре компании поняли, что развитие систем искусственного интеллекта довольно дорогостоящее и затратное по времени, чем ожидалось, и определили такие системы экономически неэффективными.

В 1990 г. использование искусственного интеллекта забросили почти все, наступил длительный период, когда только в университетах продолжались исследования по этому вопросу. В настоящее время наступила новая и более мощная волна возрождения этой технологии, связанная с обещанием [1]: «искусственный интеллект изменит тот мир, каким мы его знали».

Сегодня следующие научно-технические достижения способствовали развитию и новой волне возрождения искусственного интеллекта:

– достижения в области аппаратного и программного обеспечения компьютеров в последние годы дали немыслимые ранее вычислительные мощности;

– компьютерные системы, обладающие большой мощностью, стали значительно дешевле. Теперь компании имеют компьютеры гораздо более мощные, но за значительно меньшие деньги;

– широкое использование социальных сетей, мобильных смартфонов, планшетов и так называемых «wearables» (устройства, носимые в предметах одежды), наряду с прогрессом, в области «умных» городов появление хорошо знакомого «интернета вещей» (IoT) обеспечивает гигантский объем данных или *big data*, которые идеально подходят для обработки искусственным интеллектом и позволяют работать с максимальной эффективностью.

В последние годы эксперты в области искусственного интеллекта вышли из университетов в мир бизнеса и уже начинают просматриваться первые результаты. Большая часть крупных технологических компаний, таких как Google, Facebook или Microsoft используют ИИ в своих наиболее известных продуктах. Пресса в течение последних лет была заполнена именами и марками, связанными с искусственным интеллектом.

Одним из основных применений ИИ во всех секторах – клиентский сервис, который позволяет адаптировать различные инструменты с помощью процесса машинного обучения под предпочтения различных пользователей. Финансовый сектор не является исключением.

Банки используют системы ИИ для организации своих операций, инвестирования средств в ценные бумаги и управление различными процессами, например, как средство для управления рисками, связанными с незаконными действиями инсайдеров. Есть даже фонды, которые проводят инвестирование с помощью роботов–консультантов. Такие «консультанты» в зависимости от информации в их распоряжении автоматически решают, какие инвестиции в настоящий момент являются лучшими.

В этом контексте следует отметить, что уже в августе 2001 г. при моделировании торговой конкуренции на финансовых рынках, роботы превзошли человека.

Согласно СНБиСи (CNBC), только за последние два года в ИИ было инвестировано около 700 млн долл. Произошедшие изменения показали огромный потенциал технологии для увеличения доходов, сокращения расходов и минимизации рисков.

Не все эксперты сходятся во мнении, что за искусственным интеллектом будущее финансового сектора. Некоторые из ученых довольно осторожны в высказываниях и показывают, что глубокое обучение и другие методы искусственного интеллекта могут быть не совсем подходящими для финансового сектора. Например, Стивен Робертс (Stephen Roberts), профессор по машинному обучению в Оксфордском университете, отмечает, что «глубокое обучение» может быть полезно для выявления тенденций, информации и скрытых взаимосвязей, но является недостаточным при управлении неопределенностями с высоким уровнем шума, что часто встречается в финансовом секторе.

**Порядок выполнения работы.**

1 Составить конспект теоретического материала.

2 Ответить на контрольные вопросы.

***Контрольные вопросы***

1 Что понимается под ИИ?

2 Назовите основные направления использования ИИ.

3 Какие задачи решает ИИ в банковском секторе?

4 Почему некоторые эксперты скептически относятся к ИИ в финансах?

# 2 Лабораторная работа № 2. Системы поддержки принятия решений

**Цель работы**: ознакомиться с системами поддержки принятия решений.

Система поддержки принятия решения (СППР) – это класс человеко-машинных систем, предназначенных для оказания помощи пользователям в их профессиональной повседневной деятельности по использованию данных, знаний и моделей при подготовке, принятии и реализации обоснованных решений. В качестве областей применения СППР выделяют микроэкономику, макроэкономику, офисную деятельность, оценку и распространение технологий, юриспруденцию, медицину и другие приложения.

СППР AssistantChoice предназначена для решения задач многокритериального выбора оптимальных решений в сфере экономики и управления:

– подбор и расстановка кадров;

– распределение фондов между подразделениями;

– анализ конкурентоспособности;

– задачи размещения (выбор места расположения вредных и опасных производств, пунктов обслуживания);

– выбор перспективных инновационных проектов;

– определение политики инвестиций;

– поддержка проведения конкурсов;

– выбор средств и методов рекламы;

– разрешение конфликтных ситуаций;

– оценка контрактов и портфелей ценных бумаг и др.

В СППР AssistantChoice в качестве метода ППР используется модификация метода анализа иерархий Саати. Особенность модификации заключается в том, что эксперты непосредственно оценивают важность каждого элемента иерархии. Экспертные оценки выставляются по десятибалльной шкале:

10 баллов – очень высокая важность;

9 баллов – важность в промежутке между высокой и очень высокой;

8 баллов – высокая важность;

7 баллов – важность в промежутке между средней и высокой;

6 баллов – средняя важность;

5 баллов – важность в промежутке между низкой и средней;

4 балла – низкая важность;

3 балла – важность в промежутке между низкой и очень низкой;

2 балла – очень низкая важность;

1 балл – важность ниже очень низкой.

Процесс решения задачи с помощью СППР AssistantChoice включает следующие этапы:

1) задание наименования нового эксперимента (проблемы);

2) задание соответствующих проблеме критериев оценки в виде иерархии;

3) оценивание критериев и определение вектора коэффициентов относительной важности критериев;

4) оценивание альтернатив по всем критериям;

5) выбор наиболее приемлемой альтернативы.

Основные элементы интерфейса СППР AssistantChoice (рисунок 2.1):

– строчное меню (команды Проблема, Помощь);

– панель инструментов (кнопки <Справка>, <Новая проблема>, <Открыть проблему>, <Редактировать проблему>, <Сохранить проблему>, <Печать результатов>, <Экспорт в MS Word> и <Выход>);

– строка состояния (в нижней части окна программы);

– рабочая область окна программы, в левой части которой отображается иерархия критериев, в правой части вверху страницы Оценка критериев, Выбор альтернативы, Результат, внизу – значения оценок.

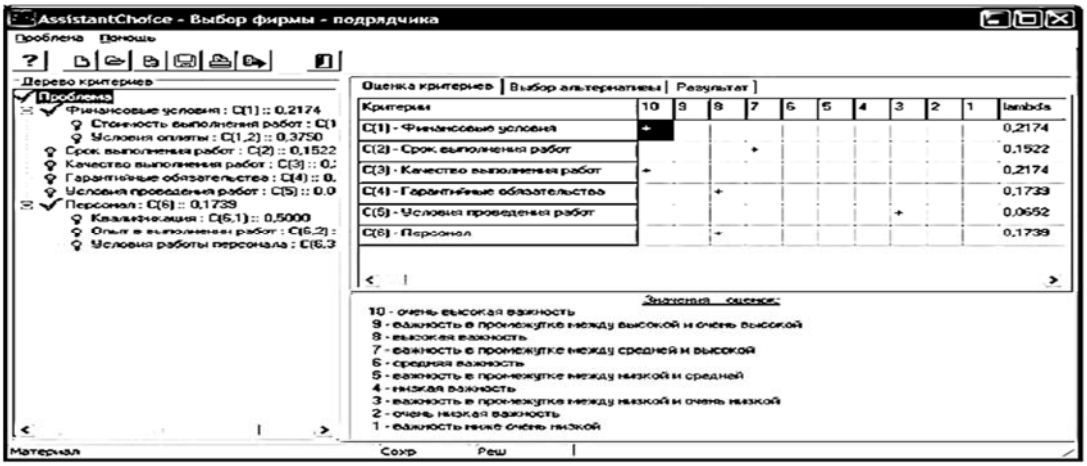


Рисунок 2.1 – Интерфейс СППР AssistantChoice

Решение задач выбора наилучшей альтернативы в СППР AssistantChoice рассмотрим на примере следующей ситуации.

Перед организацией стоит проблема выбора фирмы–поставщика материала, необходимого для производства готовой продукции. Имеются три фирмы, производящие нужный материал. Все они высказали свое согласие сотрудничать

с данной организацией, однако предлагают разные условия в отношении поставок, цен, скидок и т. д. Эти фирмы будут рассматриваться как возможные альтернативные решения проблемы поставок. Вся необходимая информация о фирмах, которая в дальнейшем будет использоваться для решения проблемы выбора, находится в таблице 2.1.

Таблица 2.1 – Исходная информация

| Фирма | Цена за материал, р. | Качество материала | Скидки и льготы, % | Предоплата, % | Форма доставки | Расстояние, км | Размер минимальной партии, т | Форма собственности |
|---|---|---|---|---|---|---|---|---|
| АО «Космос» | 105 | 1 сорт | 5 | 50 | Самовывоз | 70 | 1 | Акционерная |
| Завод «Гранат» | 110 | 1 сорт | 3 | 100 | За счет поставщика | 300 | 5 | Государственная |
| МП «Ирина» | 99,9 | Высший сорт | 7 | 80 | Ж.-д. транспорт | 5 | 1 | Частная |

Результатом решения задачи должен быть вывод о наиболее приемлемом варианте поставщика материала.

*Решение*

1 Сформировать критерии, по которым будут сравниваться поставщики материала (альтернативы).

Сравнение вариантов в решаемой задаче можно проводить по следующим критериям:

1) цена за материал;
2) качество материала;
3) скидки и льготы;
4) предоплата;
5) форма доставки;
6) расстояние;
7) размер минимальной партии;
8) форма собственности.

Названные критерии можно объединить в группы, образующие более высокий уровень иерархии критериев (таблица 2.2).

2 Сформировать дерево критериев средствами СППР AssistantChoice. Для этого необходимо выбрать команду <Новая группа>, затем ввести в поле «Общее название» формулировку рассматриваемой проблемы, использовать кнопки <Добавить критерий> и <Добавить подкритерий> для ввода названий критериев 1-го и 2-го уровня иерархии критериев, при завершении

формирования иерархии критериев нажать кнопку <Закрыть и сохранить> (рисунок 2.2).

Таблица 2.2 – Иерархия критериев

| Наименование критерия | Содержание критерия |
|---|---|
| Материал | Цена за материал<br>Качество материала |
| Финансы | Скидки и льготы<br>Предоплата |
| Доставка | Форма доставки<br>Расстояние<br>Размер минимальной партии |
| Статус фирмы | Форма собственности |

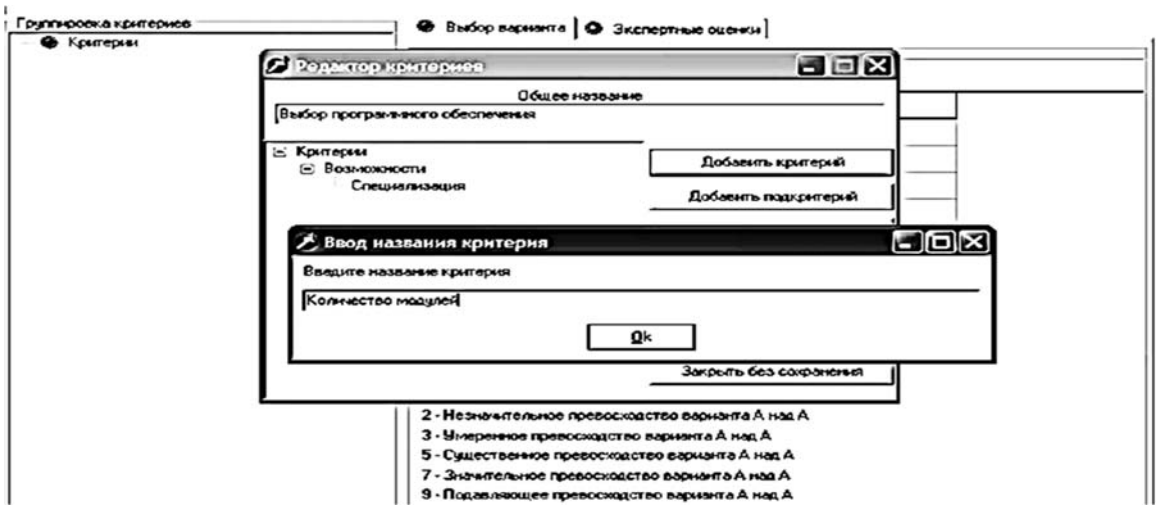


Рисунок 2.2 – Формирование дерева критериев

3 Оценить критерии и определить векторы локальных приоритетов критериев средствами СППР AssistantChoice. Для этого на иерархии критериев последовательно выделять все элементы иерархии, помеченные красным кружком, и на странице Оценка критериев производить оценку критериев путем выбора соответствующей оценки в матрице оценок (щелчком мыши). После окончания этой процедуры все элементы иерархии критериев должны быть помечены зеленым флажком (рисунок 2.3).

4 Оценить альтернативы по всем критериям средствами СППР AssistantChoice. Для этого необходимо перейти на страницу Выбор альтернативы, задать количество альтернатив, последовательно выделять все элементы иерархии критериев, имеющие слева изображение белой лампочки, и производить оценку альтернатив относительно каждого из критериев путем выбора соответствующей оценки в матрице оценок, при этом цвет лампочек изменится на желтый. По окончании этой процедуры все элементы иерархии

критериев нижнего уровня должны иметь слева изображение желтой лампочки (рисунок 2.4).

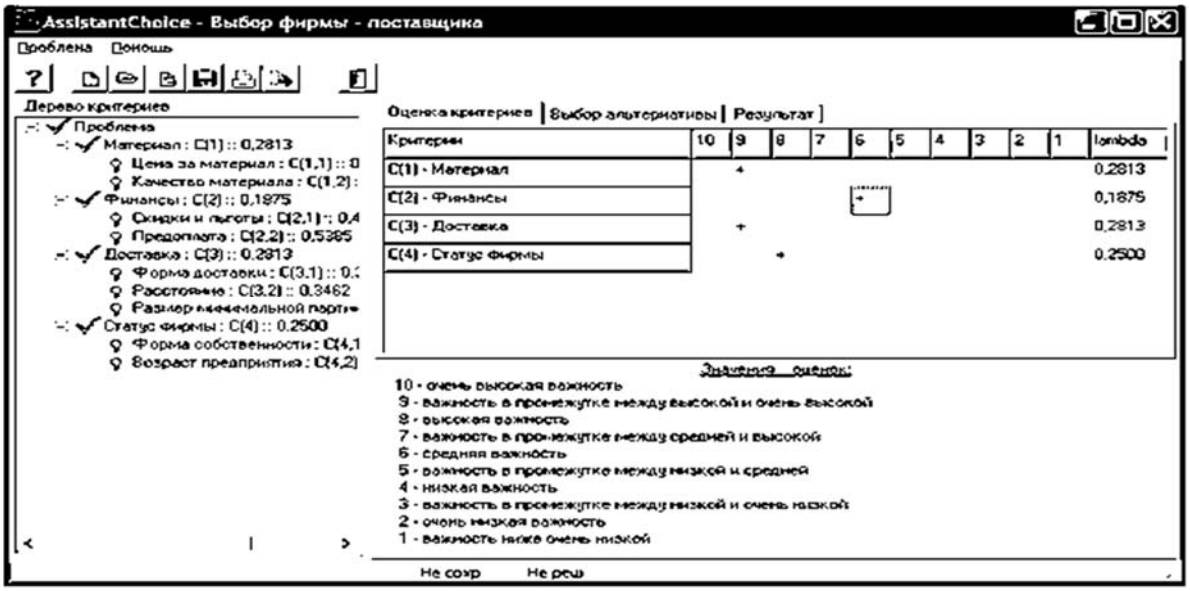


Рисунок 2.3 – Оценка критериев в СППР AssistantChoice

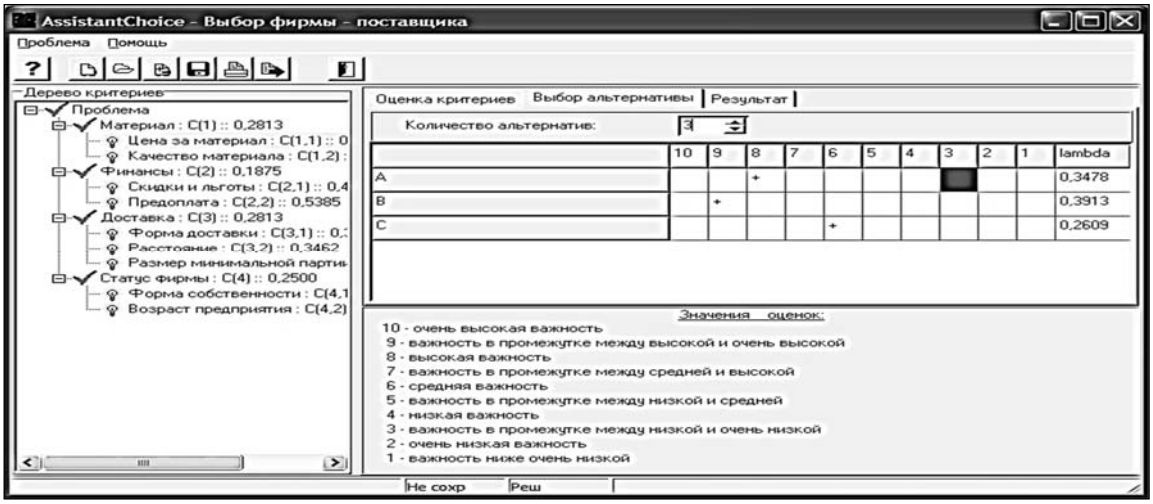


Рисунок 2.4 – Оценка альтернатив в СППР AssistantChoice

5 Выбрать наиболее приемлемую альтернативу. Для этого необходимо перейти на страницу Результат и просмотреть значения вектора глобальных приоритетов альтернатив и рекомендацию программы о наиболее приемлемой альтернативе (рисунок 2.5).

В СППР AssistantChoice предусмотрено редактирование описания проблемы, включающее редактирование названия проблемы и дерева критериев. Для этого используется кнопка <Редактировать проблему> на панели инструментов. В окне Редактирование проблемы (рисунок 2.6) можно изменять название проблемы, удалять критерии или подкритерии, добавлять новые критерии, перемещать критерии по иерархии вверх и вниз (с помощью соответствующих кнопок).

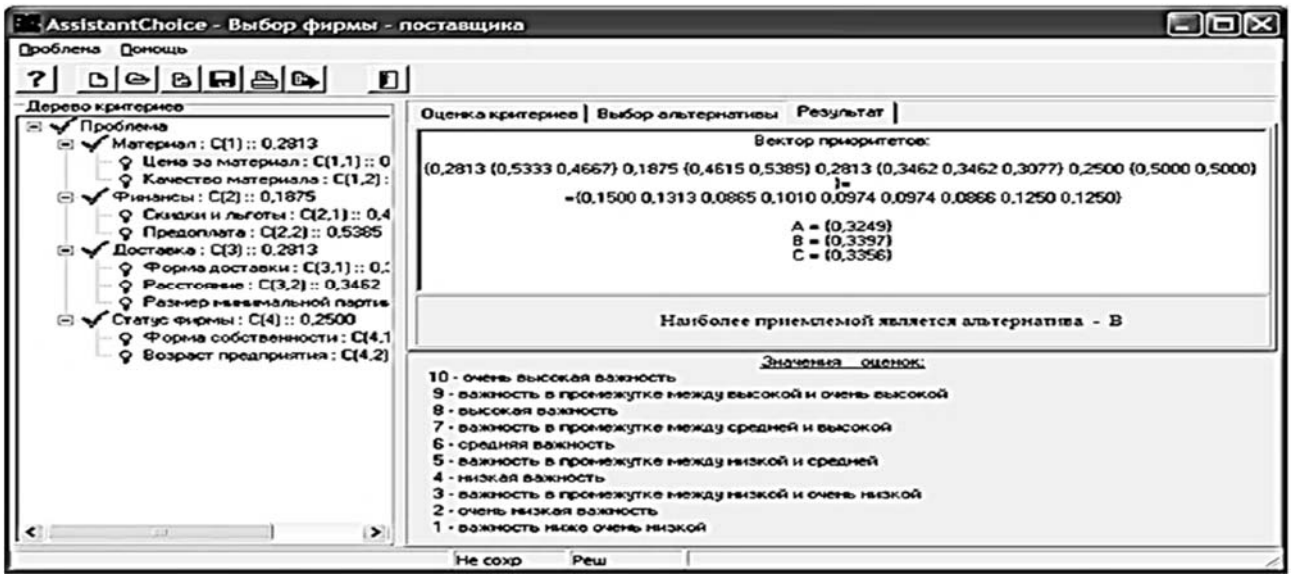


Рисунок 2.5 – Результаты работы СППР AssistantChoice

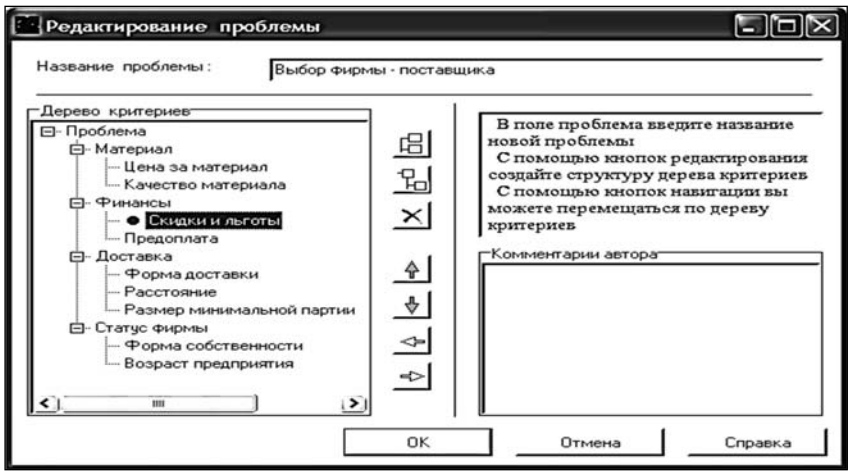


Рисунок 2.6 – Окно редактирования проблемы в СППР AssistantChoice

С помощью кнопки <Экспорт в MS Word> на панели инструментов можно получить протокол работы программы.

**Порядок выполнения работы.**

1 Используя СППР AssistantChoice, выполнить обоснованный выбор программного обеспечения автоматизированной системы обработки экономической информации для предприятия (по вариантам).

2 Для проверки представить документ, подготовленный в текстовом процессоре Word, включающий фамилию и инициалы студента, формулировки проблем, описание альтернативных вариантов их решения, протоколы работы СППР AssistantChoice, выводы о выборе альтернатив.

***Контрольные вопросы***

1 В каких областях получила приложение теория принятия решений?

2 Что такое процесс принятия решений? Из каких этапов он состоит?

3 Назовите основные особенности информационной технологии поддержки принятия решений.

4 Какой метод принятия решений реализован в СППР AssistantChoice?

5 Назовите основные этапы решения задачи выбора в AssistantChoice.

# 3 Лабораторная работа № 3. Системы Business Intelligence

**Цель работы**: изучить систему Business Intelligence.

Business Intelligence (BI) или Бизнес-аналитика это набор IT-технологий для сбора, хранения и анализа данных, позволяющих предоставлять пользователям достоверную аналитику в удобном формате, на основе которой можно принимать эффективные решения для управления бизнес-процессами компании. Все уровни пользователей, от сотрудников до учредителей, получают гибкий доступ к необходимой им управленческой отчетности, не прибегая к помощи IT-специалистов.

Сегодня на рынке существует несколько платформ Бизнес-аналитики (BI), концептуально (рисунок 3.1) они представляют собой следующее:

ETL-инструменты: программы, позволяющие выполнять загрузку данных в DWH из различных учетных систем;

DWH-хранилище: полноценная база данных SQL для подготовки и хранения данных для аналитики;

OLAP-кубы: технология, позволяющая делать в реальном времени (1…5 с) любые отчеты и проводить полноценный анализ данных;

Клиентские приложения: как правило, для детального анализа данных и построения динамических отчетов пользователи используют Сводные таблицы Microsoft Excel, подключенные к OLAP-кубам.

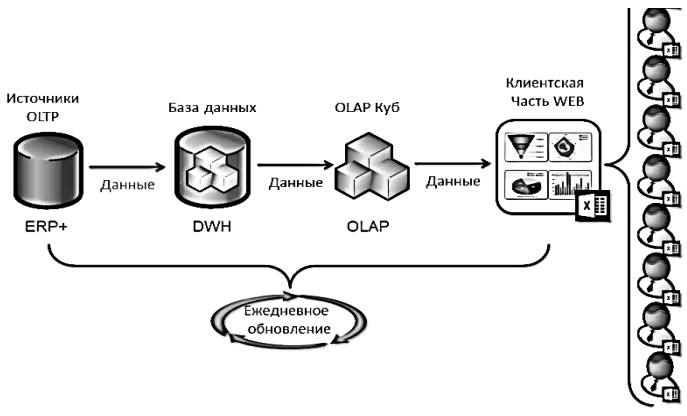


Рисунок 3.1 – Конценция платформы BI

На сегодняшний день платформа Microsoft BI – это лучшее решение на рынке BI-систем, в первую очередь, по соотношению «Цена – Качество – Современность». И что также очень важно – основным и «родным» приложением для этой платформы является уже известный всем Microsoft Excel.

Более того, все компоненты этой BI–платформы доступны в одном программном обеспечении – Microsoft SQL Server, которое приобретается один раз без необходимости последующих платежей за использование.

OLAP (от англ. online analytical processing) – аналитическая технология обработки данных в реальном времени. Простым языком – хранилище с многомерными данными (Куб), еще проще – просто база данных, из которой можно получить данные в Excel и проанализировать с помощью инструмента Excel  Сводные таблицы. Сводные таблицы – это пользовательский интерфейс для отображения многомерных данных. Иными словами – это специальный вид таблиц, с помощью которых можно сделать практически любой отчет.

Сравним Обычную таблицу (рисунок 3.2) со Сводной таблицей (рисунок 3.3).

| Факт (руб) | Название столбцов | | | | |
|---|---|---|---|---|---|
| Название строк | Квартал 1, 2015 | Квартал 2, 2015 | Квартал 3, 2015 | Квартал 4, 2015 | Общий итог |
| Бренд №5020186731486 | 307 880 609 | 415 930 621 | 416 833 968 | 1 055 547 944 | 2 196 193 142 |
| Бренд №5020006115451 | 306 496 902 | 348 075 855 | 449 363 663 | 465 952 027 | 1 569 888 448 |
| Бренд №5020006093550 | 270 523 521 | 81 816 233 | 925 982 207 | 127 518 168 | 1 405 840 129 |
| Бренд №5020127708034 | -139 155 607 | 44 945 161 | 690 737 528 | 408 144 102 | 1 004 671 185 |
| Бренд №5020006093537 | 283 147 703 | 116 651 948 | 408 662 955 | 185 960 617 | 994 423 223 |
| Бренд №5020006093560 | 147 860 844 | 115 884 269 | 320 998 328 | 287 629 292 | 872 372 732 |
| Бренд №5020006115675 | 148 987 445 | 248 176 009 | 156 561 955 | 250 107 530 | 803 832 939 |
| Бренд №5020060085901 | 119 401 210 | 134 298 836 | 123 112 169 | 267 736 797 | 644 549 011 |
| Бренд №5020393961644 | 13 038 418 | 178 614 423 | 195 952 550 | 231 183 546 | 618 788 937 |
| Бренд №5020006093564 | 125 716 377 | 86 797 159 | 212 224 370 | 170 127 113 | 594 865 018 |
| **Общий итог** | **1 583 897 421** | **1 771 190 513** | **3 900 429 692** | **3 449 907 137** | **10 705 424 764** |

Данные

Рисунок 3.2 – Обычная таблица

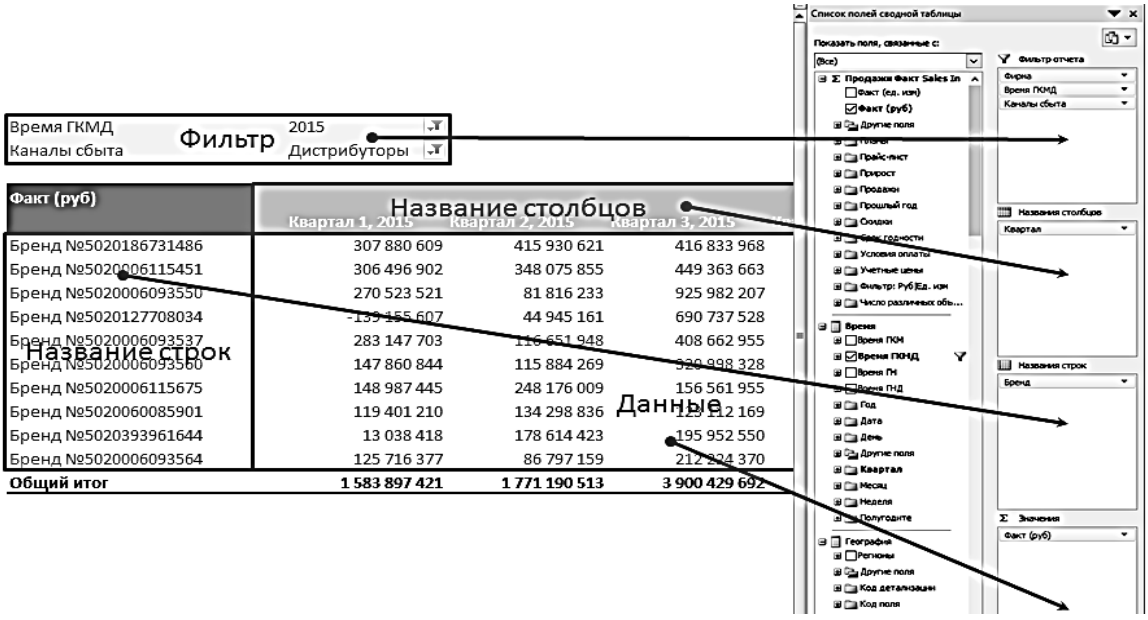


Рисунок 3.3 – Сводная таблица

Основное отличие Сводных таблиц – это наличие окна Список полей сводной таблицы, из которого можно выбирать нужные поля и получать любую таблицу автоматически.

**Порядок выполнения работы.**

1 Открыть файл Excel, который подключен к OLAP-кубу, например, BIWEB (рисунок 3.4).

2 Перетащить нужные поля, чтобы получить сводную таблицу (рисунок 3.5).

3 Ответить на контрольные вопросы.

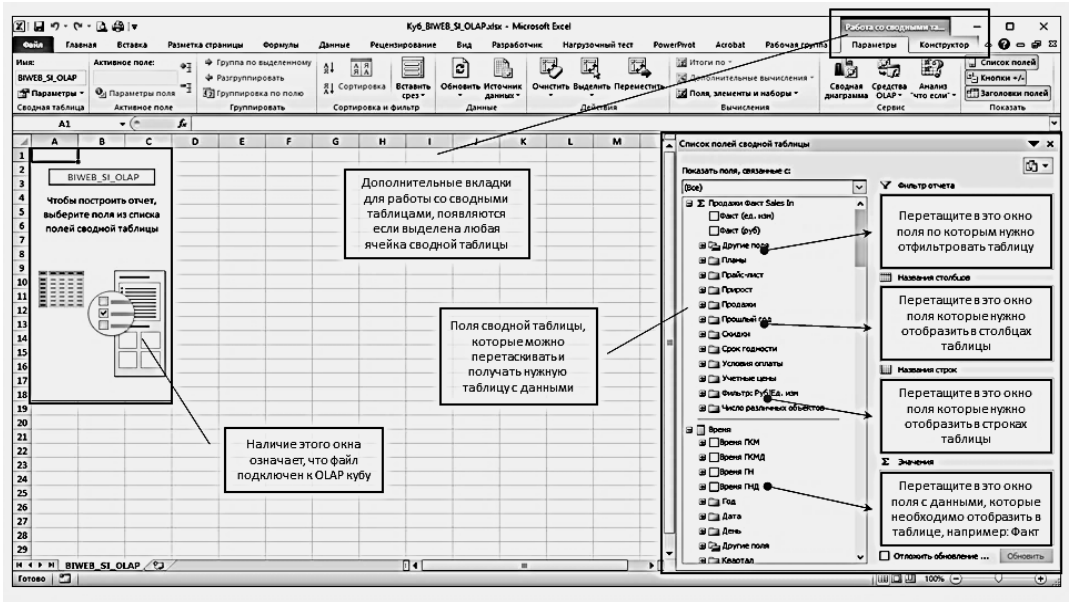


Рисунок 3.4 – Файл Excel подключен к OLAP-кубу

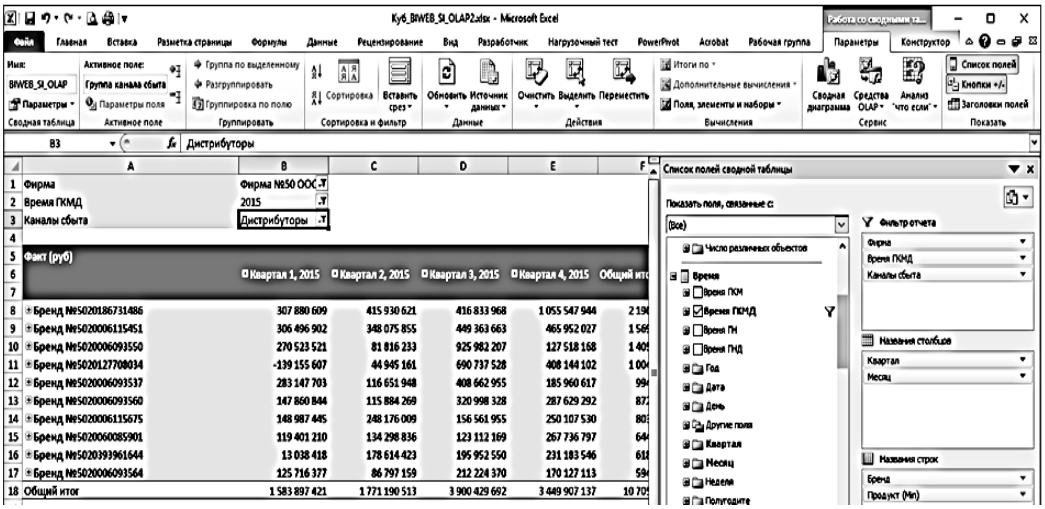

Рисунок 3.5 – Сводная таблица с выбранными полями

***Контрольные вопросы***

1 Что понимается под Business Intelligence (BI)?
2 Что включает концепция платформы BI?
3 Что такое OLAP?
4 Чем отличается обычная таблица Excel от сводной таблицы?

# 4 Лабораторная работа № 4. Экспертные системы

**Цель работы**: изучить экспертные системы.

Экспертные системы – это направление исследований в области искусственного интеллекта по созданию вычислительных систем, умеющих принимать решения, схожие с решениями экспертов в заданной предметной области.

Экспертные системы имеют одно большое отличие от других систем искусственного интеллекта: они не предназначены для решения каких-то универсальных задач, как, например, нейронные сети или генетические алгоритмы. Экспертные системы предназначены для качественного решения задач в определенной разработчиками области, в редких случаях – областях.

Экспертное знание – это сочетание теоретического понимания проблемы и практических навыков ее решения, эффективность которых доказана в результате практической деятельности экспертов в данной области. Фундаментом экспертной системы любого типа является база знаний, которая составляется на основе экспертных знаний специалистов. Правильно выбранный эксперт и удачная формализация его знаний позволяет наделить экспертную систему уникальными и ценными знаниями. Врач, к примеру, хорошо диагностирует болезни и эффективно назначает лечение не потому, что он обладает некими врожденными способностями, а потому, что имеет качественное медицинское образование и большой опыт в лечении своих пациентов. Поэтому ценность всей экспертной системы, как законченного продукта, на 90 % определяется качеством созданной базы знаний.

Экспертная система – это не простая программа, которая пишется одним или несколькими программистами. Экспертная система является плодом совместной работы экспертов в данной предметной области, инженеров по знаниям и программистов. Но стоит отметить, что встречаются случаи, когда программы пишутся самими экспертами в данной области. Эксперт предоставляет необходимые знания о тщательно отобранных примерах проблем и путей их решения. Например, при создании экспертной системы диагностики заболеваний врач рассказывает инженеру по знаниям об известных ему заболеваниях. Далее эксперт раскрывает список симптомов, которые сопровождают каждое заболевание, и в заключение рассказывает об известных ему методах лечения.

Инженер по знаниям формализует всю полученную информацию в виде базы знаний и помогает программисту в написании экспертной системы.

Например, разработаем фрагмент экспертной системы в предметной области диагностики неисправностей автомобилей. Для удобства анализа предметной области данные сводим в таблицу 4.1. В ней столбцы обозначены названиями неисправности, а строки – названиями причин неисправности. На пересечении соответствующих столбцов и строк стоит знак «+», если причина действительно принадлежит исследуемой неисправности. Одни и те же причины могут являться признаками одной и той же неисправности, поэтому некоторые из них (причин) перекрываются.

Таблица 4.1 – Продукционная модель

| Объект / атрибут | Топливная система | Снижение производительности топливного насоса | Засорение топливного фильтра | Засорение топливопровода | Негерметичность системы |
|---|---|---|---|---|---|
| Повышение расхода топлива | + | – | – | + | + |
| Затрудненный пуск | + | + | + | + | – |
| Неустойчивый холостой ход | + | – | + | + | + |
| Подтеки топлива | + | – | – | – | + |
| Запах в салоне | – | – | – | – | + |

Семантическая модель этой экспертной системы, реализованная на языке C++, имеет вид:

```
#include<iostream.h>
#include<conio.h>
main ()
{
int z;
clrscr();
cout<<"\nvvedite nomer polomki ot 1 do 5";
cin>>z;
switch(z)
{
case 5:cout<<"05";break;
```

```
case 4:cout<<"01";break;
case 1:cout<<"04";break;
case 3:cout<<"03";break;
case 2:cout<<"02";break;
default:cout<<("polomok net");
}
getch();
return 0;
}
```

**Порядок выполнения работы.**

1 Разработать фрагмент экспертной системы в предметной области по заданию преподавателя.

2 Ответить на контрольные вопросы с использованием сети Интернет.

***Контрольные вопросы***

1 Что Вы понимаете под экспертной системой?
2 Дайте определение базы знаний экспертной системы?
3 Что представляет собой подсистема вывода экспертной системы?
4 Чем отличается прямой и обратный порядок логического вывода?
5 Дайте понятие фреймовой модели представления знаний.
6 Какие модели представления знаний вы знаете?
7 Какие функции выполняет инженер по знаниям?
8 Чем отличается база данных от базы знаний?

# 5 Лабораторная работа № 5. Технологии Blockchain

**Цель работы**: изучить технологию блокчейн (Blockchain).

Судя из названия, блокчейн – это цепочка блоков. По сути, это технология децентрализованного хранения данных с особой структурой, позволяющей быть уверенным, что манипуляции с данными происходили в рамках четко заданных правил. Обеспечивается эта уверенность тем, что массив данных хранится сразу у всех, кто подключился к сети блокчейна – это значит, что недостаточно будет просто подменить весь массив в одном месте. А еще каждая следующая порция данных, так называемый блок, содержит в себе хеш предыдущего блока (рисунок 5.1), что дает два плюса:

1) в готовую цепочку невозможно подставить промежуточный блок;

2) сам блок нельзя изменить, не поменяв при этом его хеш, следовательно, это невозможно сделать без нарушения целостности цепочки.

Дерево Меркла – дерево хешей (рисунок 5.1), в данном случае используется для независимого подтверждения валидности отдельных транзакций. Транзакции – это и есть данные в блокчейне.


Рисунок 5.1 – Дерево Меркла – дерево хешей

Работу по добавлению блоков обеспечивают сами участники сети. Кому будет предоставлено право добавления следующего блока определяется специальным механизмом. Самые распространенные из таких механизмов – это Proof-of-Work и Proof-of-Stake. В первом блоки добавляют майнеры – участники сети, решающие вычислительно сложные задачи, конкурируя друг с другом за право создания блока на основе своего решения, а в награду за успешное создание блока получающие некоторое количество валюты этой сети. В Proof-of-Stake блоки добавляют валидаторы – участники сети, конкурирующие не за счет производительности, а на основе количества внутренней валюты этой сети на их аккаунте. Получают они при этом меньше, но и работы от них требуется меньше. В обоих случаях логика в том, что злоумышленнику для добавления поддельного блока придется потратить больше, чем удастся заработать. В первом случае – на оборудование для майнинга, соизмеримое по мощности с остальными майнерами вместе взятыми. Во втором случае – на покупку 50 % валюты сети.

Существуют разные реализации блокчейнов, среди которых самыми популярными сейчас являются Bitcoin и Ethereum. В то время как Bitcoin – это реализация криптовалюты на базе blockchain, целью Ethereum является создание платформы, позволяющей решать самые разные задачи с помощью умных контрактов. Поэтому логично первое знакомство начать именно с Ethereum.

Smart Contracts. Манипулирование данными в блокчейне обеспечивается так называемыми умными контрактами (smart contracts). Они описывают какие данные хранить на блокчейне и набор функций для операций над ними. Выполнение функций и получение доступа к данным осуществляется через предоставляемый каждым контрактом интерфейс. Этот интерфейс генерируется из исходного кода отдельно от компиляции и позволяет выполнять бинарный код. Данные для участников сети открыты, и чтение их ничего не стоит, ведь как уже было сказано, данные хранятся у всех участников сети. Изменение данных

происходит посредством транзакций. Каждую транзакцию можно представить структурой следующего вида.

1 Получатель транзакции.

2 Цифровая подпись отправителя.

3 Количество отправляемой валюты.

4 Произвольные данные (необязательно).

5 Лимит газа на транзакцию.

6 Цена за единицу газа.

Выполнение транзакций требует затрат внутренней валюты и ожидания когда очередной, созданный майнером, блок с вашей транзакцией включится в общую цепочку. Код контракта выполняется на компьютере майнера, в виртуальной машине EVM, а в награду майнер получает комиссию.

DApp – Decentralized Application или децентрализованное приложение. Приложение может быть построено на разных технологиях, но среди них есть и блокчейн со смарт–контрактами. Можно сказать, что на данный момент DApp – это логика на смарт–контрактах плюс некий пользовательский интерфейс. Хранение более-менее объемных данных и обмен сообщениями в идеальном DApp тоже должны быть децентрализованными, однако эти технологии только начинают появляться. Блокчейн же обеспечивает хранение текущего состояния и реализует бизнес-логику через смарт-контракты. Используя DApp, пользователь может получить доступ к блокчейну напрямую на своем компьютере, установив специальное ПО. Блокчейн также может использоваться для каких-то отдельных операций на стороне сервера привычных нам мобильных и веб-приложений. Выбор зависит от конкретной задачи. Упрощенный вариант DApp можно представить в виде на рисунке 5.2.

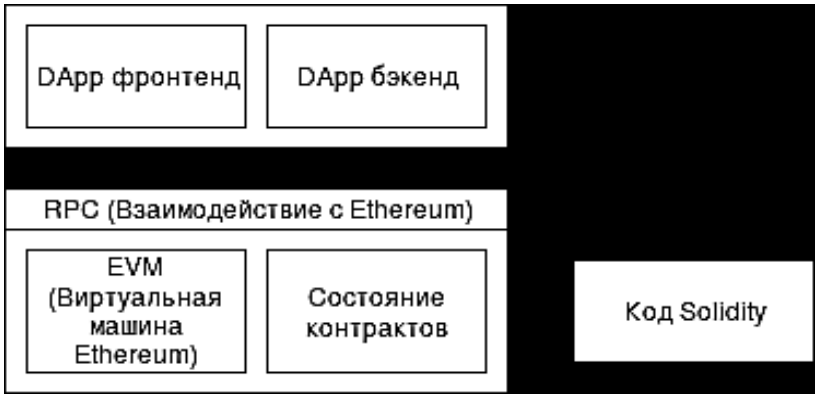


Рисунок 5.2 – Упрощенный вариант DApp

Фронтенд и бэкенд, в данном случае, – это классические элементы приложения, а функциональность с задействованием блокчейна выполняется на виртуальной машине EVM. Пользователю доступны стандартные функции виртуальной , такие как отправка транзакции или просмотр баланса аккаунта, а также функции, описанные в смарт-контрактах, например на языке solidity. Доступ к этой виртуальной машине предоставляется через RPC-интерфейс. Создание распределенных приложений должно, по нашему мнению, стать

довольно востребованным направлением, так как они позволяют решать многие проблемы: отсутствие доверия к хранителю данных, уязвимые для атак серверы в централизованных системах, закрытость систем.

Для первого подключения к блокчейну, чтобы стать участником сети, надо скачать Mist (последняя версия под номером 0.9.0) – кошелек Ethereum. Кошельком Mist называется потому, что в нем можно управлять своими аккаунтами и балансом на них. Основная валюта – ether (эфир), но можно выпускать собственные токены, они также будут отображаться в кошельке. Но Mist – это не только кошелек, а еще и браузер DApp для Ethereum-блокчейна. Он позволяет выкладывать и использовать смарт-контракты, а также пользоваться DApp-приложениями.

Для наглядности работы с блокчейном рекомендуем использовать пару клиентов на разных компьютерах: можно будет увидеть, что создаваемые данные доступны не только локально, но это не обязательно.

**Порядок выполнения работы.**

1 Запустить Mist и выбрать сеть Test network.

Для выполнения любых операций на блокчейне требуется валюта этой сети, в данном случае ether. В Main network эфир стоит реальных денег, а в Test network – ничего не стоит и его легче получить. Кроме того, перед запуском к вам на компьютер скачиваются все данные сети, для testnet Ropsten это меньше 7 Гбайт, для testnet Rinkeby – 800 Мбайт, для реальной сети – больше 40 Гбайт. Поэтому для начала выбираем Testnet. В реальной сети эфир можно получить, купив его на бирже за реальные деньги (это ≈ около 300 долл.), либо намайнить, но для этого требуются довольно большие мощности и затраты времени. Майнинг в Testnet занимает значительно меньше времени, чем в реальной сети, например на ноутбучном процессоре i5 6200u можно получить 5 эфиров в зависимости от везения за пару-тройку часов. Скорость майнинга в этом случае около 50 KH/s (50 KH/s – 50 килохешей, или 50 000 хешей в секунду), вы сможете ее увидеть у себя и прикинуть сколько времени потребуется лично вам. Кстати, намайнив несколько эфиров на одном клиенте можно будет без проблем передать часть на другой, например, если тот майнит медленнее. Стоит упомянуть, что в дальнейшем будем использовать только Ropsten, которая является Proof-of-Work-сетью, поэтому в ней и используется майнинг. В версиях Mist после 0.9 эта сеть больше не является сетью по умолчанию, поэтому если хотите использовать ее – сначала запустите Mist, нажав Launch Application, затем в пункте меню Develop-Network выберите нужную сеть. Надо отметить, что Rinkeby более удобен, так как не требует майнинга, быстрее и легче, поэтому вы не много потеряете используя его. Однако Ropsten более приближен к реальной сети и позволяет почувствовать ее особенности.

2 Задать пароль для своего аккаунта.

Логин не нужен, так как для идентификации используется файл приватного ключа. Приватный ключ хранится на линуксе в папке ~/.ethereum/testnet/keystore/

для Ropsten, ~/.ethereum/rinkeby/keystore/ – для Rinkeby. Обратите внимание, что для разных сетей создаются отдельные ключи и если вы собираетесь использовать Ropsten, то потребуется создать еще один аккаунт. Имя состоит из даты и времени создания и адреса. Под адресом понимается шестнадцатеричная строка в 20 байтов вида 0xe03269461f7672494fb0dbbe89c00614601b5d24. В названии файла начальный 0x опущен. Адрес используется для идентификации вашего аккаунта в блокчейне, на него можно отправлять ether с других аккаунтов.

3 Синхронизировать локальную базу.

На это для testnet Ropsten может уйти пара часов и больше, но необходимо дождаться завершения процесса. Иначе есть вероятность получить рассинхронизированную базу. Может быть ситуация, что при запущенном майнинге эфир начал набираться чересчур быстрыми темпами, но при этом его невозможно было использовать – все операции не были видны другим участникам сети. Проблема выясняется следующим образом – в Mist в левом нижнем углу отображается номер последнего блока (либо сколько блоков остается до окончания синхронизации, в этом случае все нормально и нужно лишь дождаться окончания процесса). Номер последнего блока в локальной копии можно сравнить с реальным значением для данного блокчейна, например, на ropsten.etherscan.io можно узнать последние номера блоков для сети Ropsten. Если ваше значение намного отличается в меньшую сторону – возможно ваша база не синхронизирована. Что делать, если синхронизация в mist дошла до конца, но номер блока неправильный? Решить эту проблему можно удалением данных и скачиванием их заново. Данные на Линуксе для сети Ropsten лежат в папке ~/.ethereum/testnet, которые можно удалить из подпапки chaindata. После чего необходимо запустить mist и уже на этот раз терпеливо дождаться окончания синхронизации.

4 После окончания синхронизации можно выбрать пункт меню Develop-Start mining.

Это необходимо для того, чтобы получить хоть немного эфира. Это актуально только для сети Ropsten. Если хотите использовать сеть Rinkeby – зайдите на www.rinkeby.io, вкладка Crypto Faucet, и следуйте приведенным инструкциям. Эфир нужен для любых операций по изменению данных, им оплачивается так называемый gas – абстрактная единица измерения, которая служит для оценки требующейся работы по выполнению транзакции. Она нужна для независимости этой оценки от текущей рыночной стоимости эфира. При отправке транзакции можно задать сколько эфира вы платите за каждую единицу газа и максимальное количество газа, которое вы готовы оплатить. Чем больше вы выделяете – тем более приоритетна ваша транзакция для потенциальных майнеров. Ведь по сути плата за gas – это оплата работы майнеров по выполнению вашей транзакции и включению ее в очередной блок. Поэтому при майнинге кроме фиксированной платы за найденный блок (это 5 эфиров), майнер также получает плату за транзакции, как правило, это несколько сотых эфира.

Количество газа за транзакцию зависит от вычислительной сложности операций над данными.

5 Создать простейший Smart Contract.

Как только у вас на аккаунте будет какое-то количество эфира – можно начинать эксперименты со смарт-контрактами. Язык, на котором пишутся контракты, – Solidity, напоминает C++ и JavaScript. Есть и другие языки, но Solidity самый популярный, активно поддерживаемый и хорошо документированный, поэтому рекомендуется использовать именно его. Рассмотрим простой контракт, единственная цель которого – хранить и обеспечивать возможность менять единственную строку.

Код контракта:

```
pragma solidity ^0.4.10
contract StringHolder {
contract StringHolder {
string savedString;
function setString( string newString ) {
savedString = newString;
}
function getString() constant returns( string ) {
return savedString;
    }
}
}
```

Строка pragma solidity ^0.4.10 означает, что минимальный требуемый компилятор для данного контракта – 0.4.10, а символ ^ запрещает использование компилятора начиная с 0.5.0. Это актуально, так как Solidity развивающийся язык и несмотря на желание разработчиков сохранять совместимость – это не всегда возможно.

Имя контракта задается после ключевого слова contract. В теле контракта описываются все хранящиеся данные, в данном случае, это поле savedString типа string. Манипуляции с данными осуществляются через сеттеры и геттеры. В данном случае, функция setString(string newString) присваивает в переменную контракта новое значение для строки.

Функция getString() constant returns(string) возвращает значение строки (тип возвращаемого значения задается как returns(<тип>)). Стоит особо отметить ключевое слово constant. Оно гарантирует, что никакие из данных не будут изменены при выполнении функции. Если данные не меняются – то не нужно платить за газ. Поэтому геттеры выполняются моментально и бесплатно. Сеттеры требуют оплаты и выполняются не моментально (только в результате включения транзакции в очередной блок блокчейна).

Для начальных экспериментов с контрактами очень удобна Remix IDE. Достаточно скопировать приведенный код контракта и вставить его в окошко

для кода. В правой панели нажать Create – создастся контракт без публикации в блокчейн. Увидите результат на рисунке 5.3.


Рисунок 5.3 – Результат создания простейшего Smart Contract

Синим отмечаются геттеры (getString), красным – сеттеры (setString). Показано сколько расходуется газа. Для задания строки в поле setString не забудьте поставить кавычки, иначе получите ошибку. Проверив, что get и set работают как надо, можно деплоить контракт в настоящий блокчейн. Для этого переключаемся обратно в Mist, заходим в Contracts и нажимаем Deploy New Contract. Копируем код в поле Solidity Contract Source Code и справа видим выпадающий список Pick a contract. Выбираем StringHolder, единственный пункт в данном случае. Выбираем размер оплаты, от которого будет зависеть время выполнения деплоя, нажимаем Deploy, в окне отобразится примерная стоимость, вводим пароль от аккаунта и нажимаем Send Transaction. В кошельке появится новая транзакция с прогрессом “x of 12 Confirmations” (x из 12 подтверждений). Первое подтверждение будет означать, что транзакция включена майнером в блок, последующие – что создано соответствующее количество блоков после блока с нашей транзакцией. Это дает большую гарантию, что блок с нашей транзакцией не будет отменен. Но для того чтобы контракт стал активным достаточно одного подтверждения. После подтверждения заходим в Contracts → String Holder. В mist отображается интерфейс контракта: слева геттеры (Read from contract), справа сеттеры (Write to contract) в виде выпадающего списка. Работает так же, как в Remix IDE, только задание строки – это уже настоящая транзакция, которая так же, как создание контракта, будет требовать подтверждения паролем и будет ожидать 12 подтверждений от майнеров.

***Контрольные вопросы***

1 Что понимается под технологией Blockchain?
2 Что понимается под транзакцией?
3 Что понимается под лимитом и ценой за газ?
4 Чем отличается Ethereum от Bitcoin?
5 Что такое DApp – Decentralized Application?

# 6 Лабораторная работа № 6. Технологии машинного обучения

**Цель работы**: изучить технологию машинного обучения.

Термин «машинное обучение» включает в себя любые попытки научить машину улучшаться самостоятельно – например, обучение на примерах или обучение с подкреплением. Машинное обучение – процесс, связанный с вводом и выводом данных, предполагающий использование некой математической модели – алгоритма.

Машинное обучение – разновидность искусственного интеллекта, предоставляющая компьютерам возможность обучаться без каких-либо строго запрограммированных сценариев поведения. Специалисты в этой области занимаются разработкой компьютерных программ, способных обучаться самостоятельно, расти и изменяться на основе новых данных. Компании применяют эту технологию для адаптации к постоянно изменяющимся условиям рынка.

Вот некоторые из таких компаний.

Kensho. Разработки компании сочетают в себе применение машинного интеллекта, работу с естественными языками, графические пользовательские интерфейсы и безопасные облачные вычисления и представляют собой новый класс аналитических инструментов для инвестиционных профессионалов. Умные компьютерные системы Kensho способны ответить на сложные финансовые вопросы, заданные на простом английском языке, и, согласно информации на официальном сайте компании, «способны решить сложнейшие аналитические задачи нашего времени». Компания была основана выпускниками Гарварда и MIT, в ней работают опытные бывшие сотрудники Google, Apple и Федерального резерва США, а в числе ее инвесторов значатся такие имена, как Google Ventures, Goldman Sachs, In-Q-Tel (венчурное подразделение ЦРУ).

Affirm. Финансовая компания, технологические инструменты которой собирают огромные массивы данных для их эффективного применения при оценке параметров кредитования. Машинное обучение используется для защиты от мошенничества и сбора кредитных данных.

Lending Club. Крупнейший в мире онлайн-рынок для заемщиков и инвесторов. Платформа использует машинное обучение для предсказания потенциально недоброкачественных займов.

Kabbage. Онлайн-компания из Атланты, специализирующаяся на финансовых технологиях и сборе данных. Kabbage предлагает услуги прямого финансирования малого бизнеса и потребителей в рамках автоматизированной платформы кредитования. Команда Kabbage специализируется на разработке инструментов машинного обучения следующего поколения и набора аналитических инструментов для создания моделей оценки кредитного риска и анализа существующих кредитных портфелей.

ZestFinance. Фирма использует техники машинного обучения и анализ большого объема данных для принятия более точных решений по кредитам. По информации на сайте компании, традиционный подход к оценке кредитного рейтинга использует всего 50 параметров, что составляет лишь малую часть от количества, учитываемого алгоритмами ZestFinance.

BillGuard. Предоставляет услуги персональной финансовой безопасности. Billguard защищает пользователей от хищения персональных данных во время финансовых операций, а также ошибочных списаний и серых транзакций. Компания специализируется на применении таких технологий, как «майнинг» данных, алгоритмы машинного обучения, безопасность и проектирование удобных веб-интерфейсов.

LendUp. Компания специализируется на микрокредитовании, в том числе позволяя другим организациям предоставлять аналогичные услуги с помощью собственного API. LendUp применяет машинное обучение и алгоритмы для точного определения тех 15 % заемщиков, которые согласно статистике будут способны с наибольшей вероятностью вернуть займы.

Bloomberg. Один из ведущих поставщиков информации для профессиональных участников финансовых рынков. Bloomberg оперативно предоставляет точную бизнес- и финансовую информацию, новости и экспертные мнения со всего мира. Используя методы статистики, обработки естественного языка и машинного обучения компания предлагает аналитические решения для финансового сообщества.

AlphaSense. Финансовая поисковая система, решающая фундаментальные проблемы избытка информации и ее фрагментации. Целевая аудитория компании – профессионалы из самых разных областей финансовой сферы. AlphaSense эффективно применяет собственные запатентованные алгоритмы обработки естественных языков и машинного обучения, предоставляя пользователям мощный и в высокой степени дифференцированный продукт с интуитивно понятным интерфейсом.

FinGenius. Платформа, ориентированная на работу с банками и страховыми компаниями. Набор технологий FinGenius представляет собой сочетание разных методик искусственного интеллекта, в том числе и машинное обучение, обработку естественных языков и моделирование человеческой логики с целью упрощения обработки массивов комплексных данных.

Dataminr. Компания предоставляет услуги поиска информации для клиентов из финансового сектора. Инструменты Dataminr в реальном времени «прочесывают» социальные сети и другие открытые источники информации с помощью алгоритмов машинного обучения в поисках важных информационных элементов и их последующего преобразования в полезные рекомендации и практические советы.

Feedzai. Компания применяет машинное обучение и работу с «большими данными» для обеспечения безопасности коммерческой деятельности своих клиентов. Модели самообучения Feedzai способны распознать мошенничество на 30% раньше традиционных методов.

Nymi (бывшая Bionym). Компания разработала и продвигает устройство биометрической аутентификации с помощью электрокардиограммы, применяя в числе прочего и алгоритмы машинного обучения.

EyeVerify. Фирменное ПО EyeVerify использует в качестве идентификатора личности так называемые отпечатки глаз – сосудистые узоры в глазных белках, также используя для этих целей технологию машинного обучения.

BioCatch. Лидирующий поставщик поведенческой биометрики, аутентификации и решений по обнаружению вредоносного ПО для мобильных и веб-приложений. Банки и онлайн-магазины используют Biocatch для избежания связанных с рискованными транзакциями конфликтов и защиты пользователей от киберугроз, таких как захват аккаунтов, браузерных троянов и атак с получением удаленного доступа.

Сеть машинного обучения MasterCard, сорвавшая атаку на банкоматы. Отдельного внимания заслуживает новость о технологии машинного обучения платежного гиганта MasterCard, позволившая оперативно взять под контроль три отдельных кибератаки, направленные на сеть банкоматов, ограничив общий урон примерно до 100 тыс. долл. в каждом из случаев.

Глобальная система Safety Net, запущенная в прошлом году, анализирует более 1.3 млрд операций с участием дебетовых и кредитных счетов MasterCard, мерчантов и банкоматов в день. Для этого система применяет алгоритмы оценки поведения клиентов в реальном времени. Система обнаружения мошенничества MasterCard Safety Net распознала активность, охватившую более 300 банкоматов в 26 странах. Тогда в течение 11 ч преступники попытались снять более 40 млн долл.

В числе прочего машинное обучение используется для «крауд-сбора» информации о состоянии финансовых рынков. Идея состоит в том, что «толпа», представленная как экспертами самых разных областей знаний, так и дилетантами, может за счет этого разнообразия мнений предоставить ценную информацию. Цель этого подхода – получение аналитики о том, что думают широкие слои населения об определенных компаниях и их действиях, рынке акции и других, связанных с финансами предметах. Полезные идеи извлекаются из «сознания толпы» путем масштабного «майнинга» информации из социальных сетей, блогов и газет. В силу естественной беспорядочности и отсутствия структуры в получаемых таким образом данных, специалистам

необходимо применять машинное обучение, обработку естественных языков и распознавание изображений для извлечения из них пользы.

Чаще всего для принятия решений инвесторы пользуются техническим и фундаментальным видами анализа. Технологии же «крауд-сбора» информации позволяют добавить третий компонент – социальный анализ финансовых рынков – и использовать всю возможную совокупность данных для улучшения процесса принятия решений. Более того, этот способ позволяет демократизировать информационный поток, поскольку хорошим пониманием ситуации зачастую обладает не только группа отдельных экспертов (которые нередко оказываются и не экспертами вовсе).

Сегодня в индустрии роботизированных финансовых советников оценка рисков и персонального профиля клиента происходит на основе опросника из 10 пунктов с несколькими возможными вариантами ответов. А теперь сравните этот подход с другим, в котором мы применяем «большие данные» для распознавания изображений, например, рекуррентные нейронные сети для определения объектов и сравнения их с усредненными графическими образами, или обработку естественных языков для понимания того, как люди выражают свою индивидуальность через тексты в социальных сетях. Представьте, что все это будет использовано для составления персональных характеристик клиентов, позволяющих получить целостный взгляд на их личные финансовые потребности и цели. Это и есть тот потенциал новых технологий, который так привлекает отрасль и может быть в равной степени применен для открытия счетов, CRM или финансового планирования.

Алгоритмы машинного обучения помогают компаниям победить в конкурентной борьбе. Сегодня инвесторы и заемщики со всех регионов мира ищут технологии, способные принимать решения за доли секунды, т. к. ускорение этого процесса гарантирует победу в гонке за первенство на рынке. Применение искусственного интеллекта, машинного обучения и других подобных технологий позволит компаниям в считанные секунды интерпретировать огромные массивы данных, накопленные в течение нескольких лет. Независимо от того, идет ли речь о торговле акциями, кредитовании или выявлении мошенничества, распознавание сложных закономерностей – один из ключей к успеху для любой финтех-компании. Чтобы снизить риски, алгоритмы могут быть очень полезны для предварительного экспериментирования и оценки сценариев. Новые алгоритмические технологии уже здесь, и благодаря им компании получили возможность коренным образом изменить свои ценностные предложения для клиентов. У финтех-компаний, воспользовавшихся алгоритмами в ближайшем будущем, есть все шансы на голову превзойти своих конкурентов.

**Порядок выполнения работы.**

1 Составить конспект теоретического материала.

2 Ответить на контрольные вопросы с использованием сети Интернет.

***Контрольные вопросы***

1 Что понимается под машинным обучением?

2 Приведите примеры успешного применения технологии машинного обучения.

3 Что понимается под технологией «крауд-сбора» информации?

4 Почему технологии машинного обучения помогают компаниям победить в конкурентной борьбе?

# 7 Лабораторная работа № 7. Информационные ресурсы инновационных технологий

**Цель работы**: изучить модели инноватики SWOT-анализа.

Для того чтобы получить ясную оценку сил предприятия и ситуации на рынке, существует SWOT-анализ. SWOT-анализ – это определение сильных и слабых сторон предприятия, а также возможностей и угроз, исходящих из его ближайшего окружения (внешней среды).

Сильные стороны (Strengths) – преимущества организации. Слабые стороны (Weaknesses) – недостатки организации. Возможности (Opportunities) – факторы внешней среды, использование которых создаст преимущества организации на рынке. Угрозы (Threats) – факторы, которые могут потенциально ухудшить положение организации на рынке.

Для проведения анализа необходимо:

– определить основное направление развития предприятия (его миссию);

– взвесить силы и оценить рыночную ситуацию, чтобы понять, возможно ли двигаться в указанном направлении и каким образом это лучше сделать (SWOT-анализ);

– поставить перед предприятием цели, учитывая его реальные возможности (определение стратегических целей предприятия).

Проведение SWOT-анализа сводится к заполнению матрицы. В соответствующие ячейки матрицы необходимо занести сильные и слабые стороны предприятия, а также рыночные возможности и угрозы.

Сильные стороны предприятия – то, в чем оно преуспело или какая-то особенность, предоставляющая дополнительные возможности. Сила может заключаться в имеющемся опыте, доступе к уникальным ресурсам, наличии передовой технологии и современного оборудования, высокой квалификации персонала, высоком качестве выпускаемой продукции, известности торговой марки и т. п.

Слабые стороны предприятия – это отсутствие чего-то важного для функционирования предприятия или что-то, что пока не удается по сравнению с другими компаниями и ставит предприятие в неблагоприятное положение.

В качестве примера слабых сторон можно привести слишком узкий ассортимент выпускаемых товаров, плохую репутацию компании на рынке, недостаток финансирования, низкий уровень сервиса и т. п.

Рыночные возможности – это благоприятные обстоятельства, которые предприятие может использовать для получения преимущества. В качестве примера рыночных возможностей можно привести ухудшение позиций конкурентов, резкий рост спроса, появление новых технологий производства продукции, рост уровня доходов населения и т. п. Следует отметить, что возможностями с точки зрения SWOT-анализа являются не все возможности, которые существуют на рынке, а только те, которые можно использовать.

Рыночные угрозы – события, наступление которых может оказать неблагоприятное воздействие на предприятие. Примеры рыночных угроз: выход на рынок новых конкурентов, рост налогов, изменение вкусов покупателей, снижение рождаемости и т. п.

Один и тот же фактор для разных предприятий может быть как угрозой, так и возможностью. Например, для магазина, торгующего дорогими продуктами, рост доходов населения может быть возможностью, так как приведет к увеличению числа покупателей. В то же время, для магазина-дискаунтера тот же фактор может стать угрозой, так как его покупатели с ростом зарплат могут перейти к конкурентам, предлагающим более высокий уровень сервиса.

**Порядок выполнения работы.**

1 Определить сильные и слабые стороны предприятия (по заданию преподавателя).

1.1 Составить перечень параметров, по которому будет оцениваться предприятие.

1.2 По каждому параметру определить, что является сильной стороной предприятия, а что – слабой.

1.3 Из всего перечня выбрать наиболее важные сильные и слабые стороны предприятия и занести их в матрицу SWOT-анализа (таблица 7.1).

2 Для оценки предприятия использовать следующие параметры.

2.1 Организация (здесь может оцениваться уровень квалификации сотрудников, их заинтересованность в развитии предприятия, наличие взаимодействия между отделами предприятия и т. п.).

2.2 Производство (оцениваются производственные мощности, качество и степень износа оборудования, качество выпускаемого товара, наличие патентов и лицензий (если они необходимы), себестоимость продукции, надежность каналов поставки сырья и материалов и т. п.).

2.3 Финансы (могут оцениваться издержки производства, доступность капитала, скорость оборота капитала, финансовая устойчивость предприятия, прибыльность бизнеса и т. п.).

Таблица 7.1 – Сильные и слабые стороны предприятия

| Параметры оценки | Сильные стороны | Слабые стороны |
|---|---|---|
| Организация | Высокий уровень квалификации руководящих сотрудников предприятия | Низкая заинтересованность рядовых сотрудников в развитии предприятия |
| Производство | Высокое качество выпускаемых товаров. Проверенный и надежный поставщик комплектующих | Высокая степень износа оборудования – до 80 % по отдельным группам. Себестоимость продукции на 10 % выше, чем у основных конкурентов |
| И т. д. | … | … |

2.4 Инновации (здесь может оцениваться частота внедрения новых продуктов и услуг на предприятии, степень их новизны (незначительные либо кардинальные изменения), сроки окупаемости средств, вложенных в разработку новинок и т. п.).

2.5 Маркетинг (здесь можно оценивать качество товаров/услуг (как это качество оценивают потребители), известность марки, полноту ассортимента, уровень цен, эффективность рекламы, репутацию предприятия, эффективность применяемой модели сбыта, ассортимент предлагаемых дополнительных услуг, квалификацию обслуживающего персонала).

3 Из всего списка сильных и слабых сторон предприятия необходимо выбрать наиболее важные (самые сильные и самые слабые стороны) и также записать их в соответствующие ячейки матрицы SWOT-анализа (см. таблицу 7.1).

4 Второй шаг SWOT-анализа – это оценка рынка. Этот этап позволяет оценить ситуацию вне предприятия – увидеть возможности и угрозы. Методика определения рыночных возможностей и угроз практически идентична методике определения сильных и слабых сторон предприятия. За основу взять следующий список параметров.

4.1 Факторы спроса (здесь целесообразно принять во внимание емкость рынка, темпы его роста либо сокращения, структуру спроса на продукцию вашего предприятия и т. п.).

4.2 Факторы конкуренции (следует учитывать количество основных конкурентов, наличие на рынке товаров-заменителей, высоту барьеров входа на рынок и выхода с него, распределение рыночных долей между основными участниками рынка и т. п.).

4.3 Факторы сбыта (необходимо уделить внимание количеству посредников, наличию сетей распределения, условиям поставок материалов и комплектующих и т. п.)

4.4 Экономические факторы (учитывается курс рубля (доллара, евро), уровень инфляции, изменение уровня доходов населения, налоговая политика государства и т. п.).

4.5 Политические и правовые факторы (оценивается уровень политической стабильности в стране, уровень правовой грамотности населения, уровень законопослушности, уровень коррумпированности власти и т. п.).

4.6 Научно-технические факторы (обычно принимается во внимание уровень развития науки, степень внедрения инноваций (новых товаров, технологий) в промышленное производство, уровень государственной поддержки развития науки и т. п.).

4.7 Социально-демографические факторы (следует учесть численность и половозрастную структуру населения региона, в котором работает предприятие, уровень рождаемости и смертности, уровень занятости населения и т. п.).

4.8 Социально-культурные факторы (обычно учитываются традиции и система ценностей общества, существующая культура потребления товаров и услуг, имеющиеся стереотипы поведения людей и т. п.).

4.9 Природные и экологические факторы (принимается в расчет климатическая зона, в которой работает предприятие, состояние окружающей среды, отношение общественности к защите окружающей среды и т. п.).

4.10 Международные факторы (среди них учитывается уровень стабильности в мире, наличие локальных конфликтов и т. п.).

5 Выбрать из всего списка возможностей и угроз наиболее важные, занести их в соответствующие ячейки матрицы SWOT-анализа (таблица 7.2). В заполненной матрице SWOT-анализа виден полный перечень основных сильных и слабых сторон предприятия, а также открывающиеся перед предприятием перспективы и грозящие ему опасности.

Таблица 7.2 – Определение рыночных возможностей и угроз

| Параметры оценки | Возможность | Угроза |
|---|---|---|
| Конкуренция | Повысились барьеры входа на рынок: с этого года необходимо получать лицензию на занятие данным видом деятельности | В этом году ожидается выход на рынок крупной иностранной компании-конкурента |
| Сбыт | На рынке появилась новая розничная сеть, которая в данный момент выбирает поставщиков | С этого года наш крупнейший оптовый покупатель определяет поставщиков по результатам тендера |
| И т. д. | … | … |

6 Сопоставить сильные и слабые сторон с рыночными возможностями и

угрозами, что позволяет ответить на следующие вопросы, касающиеся дальнейшего развития бизнеса.

6.1 Как можно воспользоваться открывающимися возможностями, используя сильные стороны предприятия?

6.2 Какие слабые стороны предприятия могут помешать?

6.3 За счет каких сильных сторон можно нейтрализовать существующие угрозы?

6.4 Каких угроз, усугубленных слабыми сторонами предприятия, нужно больше всего опасаться?

7 Для сопоставления возможностей предприятия условиям рынка применить немного видоизмененную матрицу SWOT-анализа (таблица 7.3). Заполнив такую матрицу, можно увидеть результат: определены основные направления развития предприятия; сформулированы основные проблемы предприятия, подлежащие скорейшему решению для успешного развития бизнеса. Итоговые показатели SWOT-анализа используются в стратегическом и тактическом планировании деятельности предприятия.

Таблица 7.3 – Матрица итогового SWOT-анализа

| | | |
|---|---|---|
| Внутренние стороны предприятия / внешние рыночные факторы | Возможности.:<br>1 Появление новой розничной сети.<br>2 И т. д. | Угрозы.<br>1 Появление крупного конкурента.<br>2 И т. д. |
| Сильные стороны.<br>1 Высокое качество продукции.<br>2 И т. д. | Как воспользоваться возможностями?<br>1 Попытаться войти в число поставщиков новой сети, сделав акцент на качестве нашей продукции.<br>2 И т. д. | За счет чего можно снизить угрозы?<br>1 Удержать наших покупателей от перехода к конкуренту, проинформировав их о высоком качестве нашей продукции.<br>2 И т. д. |
| Слабые стороны.<br>1 Высокая себестоимость продукции.<br>2 И т. д. | Что может помешать воспользоваться возможностями?<br>1 Новая сеть может отказаться от закупок нашей продукции, так как наши оптовые цены выше, чем у конкурентов.<br>2 И т. д. | Самые большие опасности для фирмы.<br>1 Появившийся конкурент может предложить рынку продукцию, аналогичную нашей, по более низким ценам.<br>2 И т. д. |

8 Ответить на контрольные вопросы.

***Контрольные вопросы***

1 Что понимают под внешней средой организации?
2 Назовите методы анализа внешней среды организации.
3 Раскройте суть метода построения профиля внешней среды организации.
4 Продолжите предложение: к слабым сторонам организации относятся… .

# 8 Лабораторная работа № 8. Криптографическая защита информации

**Цель работы**: исследовать основные методы криптографической защиты информации.

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных.

Важным аспектом безопасности является *обеспечение конфиденциальности сетевого трафика*, поскольку пакеты сообщения могут быть перехвачены на любом промежуточном узле по пути следования к получателю, а встроенных средств шифрования классический протокол IP не предоставляет. Для обеспечения конфиденциальности информации, передаваемой по сети, необходимо обеспечить ее шифрование на стороне отправителя и дешифрацию на стороне получателя по одному из алгоритмов.

В криптографии используются следующие основные алгоритмы шифрования (приложение А):

– алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;

– алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;

– гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;

– аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В асимметричных криптосистемах для зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ. Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных,

обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Существует несколько средств кодирования, которые шифруют информацию на разных уровнях модели OSI. Самым простым средством является шифрование информации на прикладном уровне. В этом случае шифрованию подвергается только непосредственно передаваемая информация, никакая служебная информация из заголовков сетевых пакетов в этом случае не кодируется.

Примером программы, которая осуществляет подобного рода шифрование, можно назвать PGP (Pretty Good Privacy). Одно из главных достоинств этой программы состоит в том, что существуют версии PGP практически для всех программных платформ: DOS, Windows, Unix, Macintosh. PGP представляет собой криптосистему, которая позволяет шифровать данные (содержимое файлов, буфера обмена) по асимметричной схеме, а также формировать ЭЦП для передаваемых сообщений. В PGP используются следующие алгоритмы: RSA, SHA, DES, CAST, IDEA, DSS. Закодированная информация сохраняется в виде файла, который может быть передан по сети любым способом (электронная почта, FTP). Для удобства работы PGP может интегрироваться с почтовыми программами, такими как OutlookExpress, TheBat, Eudora. Еще одно достоинство PGP – то, что существуют свободно распространяемые версии этой программы (freeware), которые можно найти по адресу http://www.pgpru.com.

Применение программы PGP и подобных ей может оказаться неудобным вследствие того, что пользователю необходимо самому принимать меры для шифрации сообщений. Для того чтобы сделать процедуру шифрования прозрачной для пользователя, существуют различные сетевые протоколы, реализующие технологии защищенных соединений. Рассмотрим один из подобных протоколов – протокол SSL (Secure Socket Layer). Протокол SSL спроектирован компанией Netscape для своего браузера Netscape Navigator для обеспечения конфиденциальности обмена между двумя прикладными процессами клиента и сервера. Он предоставляет также возможность аутентификации сервера и, опционно, клиента. SSL работает на представительском уровне модели OSI поверх протокола TCP.

Преимуществом SSL является то, что он независим от прикладного протокола. Прикладные протоколы, такие как HTTP, FTP, TELNET и другие, могут работать поверх протокола SSL совершенно прозрачно. Протокол SSL может согласовывать алгоритм шифрования и ключ сессии, а также аутентифицировать сервер до того как приложение примет или передаст первый байт данных. Все протокольные прикладные данные передаются зашифрованными с гарантией конфиденциальности. Протокол SSL предоставляет безопасный канал, который имеет три основные свойства.

1 Канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.

2 Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, в то время как клиентская – аутентифицируется опционно.

3 Канал надежен. Транспортировка сообщений включает в себя проверку целостности.

Протокол SSL использует следующие криптографические алгоритмы: DES, DSA, MD5, RC2, RC4. Все современные браузеры поддерживают протокол SSL. Если пользователь вводит в адресной строке URL, начинающийся с аббревиатуры HTTPS, то начинает работать протокол HTTPS, который представляет собой стандартный протокол HTTP, защищенный средствами SSL. При этом подключение происходит к порту номер 443, который для HTTPS обычно используется по умолчанию. После этого браузер и сервер обмениваются пакетами, проводя взаимную аутентификацию по имеющимся у них сертификатам, обмениваются сеансовыми ключами шифрования и начинают обмен информацией в зашифрованном виде (рисунок 8.1).


Рисунок 8.1 – Обобщенная схема установки соединения по протоколу SSL

Альтернативой использованию протокола SSL может стать применение протокола TLS (Transport Layer Security), имеющего практически аналогичную функциональность.

Для защиты информации на более низком – сетевом – уровне модели OSI используется технология VPN (Virtual Private Network). VPN предполагает использование криптографических методов защиты для обеспечения конфиденциальности и целостности информации на сетевом уровне с использованием ряда современных протоколов сетевого уровня (IPSec, PPTP, L2TP, L2P) при передаче информации по сетям общего пользования. Шифрование происходит прозрачно для пользователей программными или программно-аппаратными средствами. При этом данные всех сетевых пакетов, начиная с транспортного уровня, шифруются и помещаются в закодированном виде в область данных пакета сетевого уровня. Так образуется скрытый от посторонних «туннель», по

которому информация может передаваться в сети общего доступа между узлами воображаемой виртуальной сети. По сравнению с протоколом SSL, VPN предоставляет возможность скрыть от злоумышленника такую информацию, как номера используемых портов, а при использовании механизма туннелирования и используемые в локальной сети IP-адреса, что затрудняет возможности сканирования сети, поиска слабых мест в ней.

**Порядок выполнения работы.**

1 Составить конспект теоретического материала.

2 Зашифровать любыми четырьмя методами свои данные: Фамилию, Имя, Отчество, любимую фразу.

3 Ответить на контрольные вопросы.

***Контрольные вопросы***

1 Объяснить цель и задачи криптографии.

2 Шифры одиночной перестановки.

3 Шифры двойной перестановки.

4 Шифрование с помощью магического квадрата.

5 Пояснить алгоритм шифрования RSA.

6 Какими средствами кодирования шифруют информацию на разных уровнях модели OSI?

# 9 Лабораторная работа № 9. Управление информационной безопасностью

**Цель работы**: освоить средства управления информационной безопасности защищенных версий операционной системы Windows.

Главная цель мер административного уровня управления информационной безопасностью (ИБ) – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Термин «политика безопасности» является не совсем точным переводом английского словосочетания security policy, однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные правила безопасности. Мы будем иметь в виду не отдельные правила или их наборы, а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений на верхнем уровне детализации может включать в себя следующие элементы:

– решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;

– формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;

– обеспечение базы для соблюдения законов и правил;

– формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками

своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле политика безопасности является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

**Порядок выполнения работы.**

1 Составить конспект теоретического материала.

2 Освоить средства определения политики безопасности.

2.1 Открыть окно определения параметров политики безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности).

2.2 Установить заголовок «ПРЕДУПРЕЖДЕНИЕ» в качестве значения параметра «Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему».

2.3 Установить текст «На этом компьютере могут работать только зарегистрированные пользователи!» в качестве значения параметра «Интерактивный вход в систему: текст сообщения для пользователей при входе в систему».

2.4 Установить значение «Отключен» для параметра «Интерактивный вход в систему: не требовать нажатия CTRL + ALT + DEL».

2.5 Установить значение «Включен» для параметра «Интерактивный вход в систему: не отображать последнего имени пользователя».

2.6 Установить значение «7 дней» для параметра «Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее».

2.7 Включить в отчет о лабораторной работе сведения о порядке назначения параметров политики безопасности, относящихся к интерактивному входу, и ответ на вопрос о смысле этих параметров.

2.8 Включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к интерактивному входу.

2.9 С помощью раздела Справки Windows «Параметры безопасности» включить в отчет о лабораторной работе пояснения отдельных параметров локальной политики безопасности компьютерной системы и их возможных

значений (в соответствии с заданием преподавателя). Обязательно ответить на вопрос, чем может угрожать неправильное определение данного параметра.

3 Освоить средства определениея политики аудита.

3.1 Открыть окно определения параметров политики аудита (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Политика аудита).

3.2 С помощью параметров политики аудита установить регистрацию в журнале аудита успешных и неудачных попыток:

– входа в систему;

– изменения политики;

– использования привилегий;

– событий входа в систему;

– управления учетными записями.

3.3 Открыть окно определения параметров безопасности (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Параметры безопасности) и включить в отчет о лабораторной работе ответ на вопрос, какие еще параметры политики аудита могут быть определены.

3.4 Открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность), выполнить команду «Свойства» контекстного меню (или команду Действие | Свойства) и включить в отчет о лабораторной работе ответы на вопросы:

– какие еще параметры политики аудита могут быть изменены;

– где расположен журнал аудита событий безопасности.

3.5 Включить в отчет о лабораторной работе сведения о порядке назначения параметров политики аудита и ответ на вопрос о смысле этих параметров.

3.6 Включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики аудита.

4 Освоить средства просмотра журнала аудита событий безопасности.

4.1 Открыть окно просмотра журнала аудита событий безопасности (Панель управления | Просмотр событий | Безопасность).

4.2 Включить в отчет о лабораторной работе копии экранных форм с краткой и полной информацией о просматриваемом событии безопасности.

4.3 С помощью буфера обмена Windows и соответствующей кнопки в окне свойств события включить в отчет о лабораторной работе полную информацию о нескольких событиях безопасности.

5 Освоить средства определения политики ограниченного использования программ.

5.1 Открыть окно определения уровней безопасности политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Уровни безопасности).

5.2 Включить в отчет о лабораторной работе пояснения к возможным уровням безопасности при запуске программ и копии соответствующих экранных форм.

5.3 Открыть окно определения дополнительных правил политики ограниченного использования программ (Панель управления | Администрирование | Локальная политика безопасности | Политики ограниченного использования программ | Дополнительные правила).

5.4 Включить в отчет о лабораторной работе ответы на вопросы, какие дополнительные правила для работы с программами могут быть определены (с помощью команд контекстного меню или меню «Действие») и в чем их смысл, а также копии соответствующих экранных форм.

6 Ответить на контрольные вопросы.

### *Контрольные вопросы*

1 Какие события безопасности должны фиксироваться в журнале аудита?

2 Какие параметры определяют политику аудита?

3 Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?

4 Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?

5 Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?

6 Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?

7 Какое из дополнительных правил ограниченного использования программ кажется вам наиболее эффективным и почему?

8 Из каких этапов состоит построение политики безопасности для компьютерной системы?

9 К чему может привести ошибочное определение политики безопасности (приведите примеры)?

10 Почему, на ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной лабораторной работе параметров политики безопасности?

# Список литературы

1 **Chishti, S.** The FINTECH Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries [Электронный ресурс] / S. Chishti, J. Barderis // John Wiley & Sons. – 2016. – Режим доступа: https://www.twirpx.com. – Дата доступа: 03.04.2020.

2 **Swan, M.** Blockchain: Blueprint for a new economy [Электронный ресурс] / M. Swan // O'Reilly Media, Inc. – 2015. – Режим доступа: https://www.twirpx.com. – Дата доступа: 03.04.2020..

3 Data Mining: Practical machine learning tools and techniques [Электронный ресурс] / I. H. Witten [et al.] // Morgan Kaufmann. – 2016. – Режим доступа: ftp://ftp.ingv.it/pub/manuela.sbarra/Data%20Miningf/. – Дата доступа: 03.04.2020.

4 **Кузьмин, В. А.** Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика / В. А. Кузьмин, А. А. Усков. – Москва: Горячая Линия-Телеком, 2014. – 144 с.

# Приложение А
# (справочное)

# Основные алгоритмы шифрования

## *А.1 Симметричные криптосистемы*

### *А.1.1 Шифры перестановки.*

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае являются размеры таблицы. Например, сообщение «Неясное становится еще более непонятным» записывается в таблицу из 5 строк и 7 столбцов по столбцам (таблица А.1).

Таблица А.1 – Таблица-ключ

| | | | | | | |
|---|---|---|---|---|---|---|
| Н | О | Н | С | Б | Н | Я |
| С | Е | О | Я | О | Е | Т |
| Я | С | В | Е | Л | П | Н |
| Е | Т | И | Щ | Е | О | Ы |
| Н | А | Т | Е | Е | Н | М |

Для получения шифрованного сообщения текст считывается по строкам и группируется по пять букв: НОНСБ НЯСЕО ЯОЕТЯ СИУЛП НЕТИЩ ЕОЫНА ТЕЕНМ.

Несколько большей стойкостью к раскрытию обладает метод одиночной перестановки по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово ЛУНАТИК, получим следующую таблицу А.2.

Таблица А.2 – Метод одиночной перестановки по ключу

| До перестановки | | | | | | | После перестановки | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Л | У | Н | А | Т | И | К | А | И | К | Л | Н | Т | У |
| 4 | 7 | 5 | 1 | 6 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Н | О | Н | С | Б | Н | Я | С | Н | Я | Н | Н | Б | О |
| С | Е | О | Я | О | Е | Т | Я | Е | Т | С | О | О | Е |
| Я | С | В | Е | Л | П | Н | Е | П | Н | Я | В | Л | С |
| Е | Т | И | Щ | Е | О | Ы | Щ | О | Ы | Е | И | Е | Т |
| Н | А | Т | Е | Е | Н | М | Е | Н | М | Н | Т | Е | А |

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв

ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: СНЯНН БОЯЕТ СООЕЕ ПНЯВЛ СЩОЫЕ ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в таблице А.3.

Таблица А.3 – Двойная перестановка столбцов и строк

| | 2 | 4 | 1 | 3 | | 1 | 2 | 3 | 4 | | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | П | Р | И | Е | 4 | И | П | Е | Р | 1 | А | З | Ю | Ж |
| 1 | З | Ж | А | Ю | 1 | А | З | Ю | Ж | 2 | Е | – | С | Ш |
| 2 | – | Ш | Е | С | 2 | Е | – | С | Ш | 3 | Г | Т | О | О |
| 3 | Т | О | Г | О | 3 | Г | Т | О | О | 4 | И | П | Е | Р |

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы. Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 × 3 их 36, для 4 × 4 их 576, а для 5 × 5 их 14400.

В средние века для шифрования применялись и *магические квадраты*. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения (таблица А.4).

Таблица А.4 – Шифрование с помощью магического квадрата 4 × 4

| П | Р | И | Е | З | Ж | А | Ю | – | Ш | Е | С | Т | О | Г | О |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Магический квадрат 4 × 4 | | | | | | | | | | | Шифровка | | | | |
| 16 | 3 | 2 | 13 | | | | | | | | О | И | Р | Т | |
| 5 | 10 | 11 | 8 | | | | | | | | З | Ш | Е | Ю | |
| 9 | 6 | 7 | 12 | | | | | | | | – | Ж | А | С | |
| 4 | 15 | 14 | 1 | | | | | | | | Е | Г | О | П | |

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3 × 3 таких квадратов – 1; для таблицы 4 × 4 – 880; а для таблицы 5 × 5 – 250000.

*А.1.2 Шифры простой замены.*

Система шифрования Цезаря – частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на *K* букв.

Известная фраза Юлия Цезаря VENI VINI VICI – «пришел, увидел, победил», зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на четыре символа).

Греческим писателем Полибием за 100 лет до н. э. был изобретен так называемый полибианский квадрат размером 5 × 5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

*А.1.3 Шифры сложной замены.*

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда:

– сообщение: СОВЕРШЕННО СЕКРЕТНО;

– ключ: Ключ 31431431431431431431;

– шифровка: ФПЖИСЬИОССАХИЛФИУСС.

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит) (таблица А.5).

Таблица А.5 – Шифр простой замена

| | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_ |
|---|---|
| А | АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_ |
| Б | _АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ |
| В | Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ |
| Г | ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ |
| … | … |
| Я | ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ |
| _ | БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А |

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО, получаем следующую шифровку:

– сообщение: ПРИЕЗЖАЮ_ШЕСТОГО;

– ключ: АГАВААГАВААГАВАА ;

– шифровка: ПНИГЗЖЮЮЮШЕОТМГО.

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

## *А.2 Асимметричные криптосистемы*

*А.2.1 Криптосистема шифрования данных RSA.*

Предложена в 1978 г. авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Последовательность действий пользователя:

1) получатель выбирает два больших простых целых числа $p$ и $q$, на основе которых вычисляет $N = pq; M = (p-1)(q-1)$;

2) получатель выбирает целое случайное число $d$, которое является взаимопростым со значением *M*, и вычисляет значение $e$ из условия $ed = 1/(\mathrm{mod}\, M)$;

3) $d$ и $N$ публикуются как открытый ключ, $e$ и $M$ являются закрытым ключом;

4) если $S$ – сообщение и его длина: $(1S) < N$, то зашифровать этот текст можно как $S' = S^d (\mathrm{mod}\, N)$ , то есть шифруется открытым ключом;

5) получатель расшифровывает с помощью закрытого ключа;

6) представить шифруемое сообщение как последовательность целых чисел в диапазоне 0…32. Пусть буква А изображается числом 1, буква Б – числом 2, буква В – числом 3 и т. д. Тогда сообщение будет принимать вид числовой последовательности, которое зашифровывается с помощью открытого ключа. Надо расшифровать его с помощью закрытого ключа.

Зашифруем сообщение «САВ». Для простоты будем использовать маленькие числа (на практике применяются гораздо большие).

Выберем $p = 3$ и $q = 11$.

Определим $n = 3 \cdot 11 = 33$.

Найдем $(p-1)(q-1) = 20$. Следовательно, в качестве $d$, взаимопростое с 20, например, $d = 3$.

Выберем число $e$. В качестве такого числа может быть взято любое число, для которого удовлетворяет соотношение $(e^3)(\mathrm{mod}\, 20) = 1$, например 7.

Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: A1, B2, C3. Тогда сообщение принимает вид (3,1,2). Зашифруем сообщение с помощью ключа {7,33}.

$$ШТ1 = (3^7)(\mathrm{mod}\,33) = 9;$$

$$ШТ2 = (1^7)(\mathrm{mod}\,33) = 1(\mathrm{mod}\,33) = 9;$$

$$ШТ3 = (2^7)(\mathrm{mod}\,33) = 128(\mathrm{mod}\,33) = 29.$$

Расшифруем полученное зашифрованное сообщение (9,1,29) на основе закрытого ключа {3,33}:

$$ИТ1 = (9^3)(\mathrm{mod}\,33) = 129(\mathrm{mod}\,33) = 3;$$

$$ИТ2 = (1^3)(\mathrm{mod}\,33) = 1(\mathrm{mod}\,33) = 1;$$

$$ИТ3 = (29^3)(\mathrm{mod}\,33) = 24389(\mathrm{mod}\,33) = 2.$$

Итак, в реальных системах алгоритм RSA реализуется следующим образом: каждый пользователь выбирает два больших числа и в соответствии с описанным выше алгоритмом выбирает два простых числа $e$ и $d$. Как результат умножения первых двух чисел $(p\ и\ q)$ устанавливается $\{e,n\}$ – образует открытый ключ, а $\{p,n\}$ – закрытый (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования сообщение невозможно раскрыть с помощью открытого ключа. Владелец же закрытого ключа без труда может расшифровать принятое сообщение.

*А.2.2 Схема шифрования Эль-Гамаля.*

Алгоритм шифрования Эль-Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

**Последовательность действий пользователя.**

1 Получатель сообщения выбирает большое, простое число $P$ и большое целое число $G$, причем $P > G$.

2 Получатель выбирает секретный ключ – случайное целое число $X < P$.

3 Вычисляется открытый ключ $Y = G^x \bmod P$.

4 Получатель выбирает случайное целое число $K$ $(1 < K < (P-1))$, такое, что числа $K$ и $(P-1)$ являются взаимно простыми.

5 Шифрование сообщения $(M): a = G^K \bmod P, b = Y^K M \bmod P$, где пара чисел $(a,b)$ является шифротекстом.

6 Надо придумать сообщение $M$, зашифровать его, а потом с помощью секретного ключа $X$ расшифровать сообщение.

***Шифрование.***

1 Допустим, что нужно зашифровать сообщение $M = 5$.

2 Произведем генерацию ключей.

2.1 Пусть $p = 11,\ q = 2$. Выберем $x = 8$ случайное целое число $x$ такое, что $1 < x < p$.

2.2 Вычислим $y = q^x \bmod p = 2^8 \bmod 11 = 3$. Итак, открытым является тройка $(p, g, y) = (11, 2, 3)$, а закрытым ключом является число $x = 8$.

3 Выбираем случайное целое число $k$ такое, что $1 < k < (p-1)$. Пусть $k = 9$.

4 Вычисляем число $a = q^k \bmod p = 2^9 \bmod 11 = 6$.

5 Вычисляем число $b = y^k M \bmod p = 3^9 \cdot 5 \bmod 11 = 512 \bmod 11 = 9$.

6 Полученная пара $(a,b) = (6,9)$ является шифротекстом.

***Расшифрование.***

1 Необходимо получить сообщение $M = 5$ по известному шифротексту и закрытому ключу $x = 8$.

2 Вычисляем $M$ по формуле $M = b(a^x)^{-1} \bmod p = 9(6^8) \bmod 11 = 5$.

3 Получили исходное сообщение $M = 5$.