

СЕКЦИЯ 7

«НАУЧНО- МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

СОДЕРЖАНИЕ

НАУЧНО-МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ Абдршина В.В.	1385
ПРИМЕНЕНИЕ МАКРОСОВ ТАБЛИЧНОГО ПРОЦЕССОРА В ЗАДАЧЕ ИССЛЕДОВАНИЯ ИМИТАЦИОННОЙ МОДЕЛИ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ Абрамова Т. В., Аралбаев Т. З., д-р техн. наук, профессор	1389
ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ МАТЕМАТИЧЕСКОГО ПАКЕТА НА ОС ANDROID Амантаева А.С.	1396
КЛАСТЕРНЫЙ АНАЛИЗ КАК ИНСТРУМЕНТ ПОСТРОЕНИЯ И ИССЛЕДОВАНИЯПРОСТРАНСТВЕННО-ВРЕМЕННЫХ МОДЕЛЕЙ УГРОЗ Аралбаев Т.З., д-р техн. наук, профессор, Абрамова Т.В., Гетьман М.А.	1401
АЛГОРИТМ КОЛЛЕКТИВНОЙ САМООЦЕНКИ РЕЗУЛЬТАТОВ ТЕСТА В УСЛОВИЯХ ДЕФИЦИТА АППАРАТНО-ВРЕМЕННОГО РЕСУРСА Аралбаев Т.З., д-р техн. наук, профессор, Калинина В.А.	1406
О ГЕНЕРАТОРАХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ Бахтиярова А.И., Благовисная А.Н.	1410
ПРИМЕНЕНИЕ УЧЕБНОГО СТЕНДА ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БАКАЛАВРА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Бурькова Е.В., канд. пед. наук, доцент	1414
КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ДОКУМЕНТООБОРОТА ПРЕДПРИЯТИЯ Бурькова Е.В., канд. пед наук, доцент, Иванова И.В.	1419
МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ Бурькова Е.В., канд. пед. наук, доцент, Кулик М.А.	1424
ОПЫТ ВНЕДРЕНИЯ В УЧЕБНЫЙ ПРОЦЕСС ПРЕПОДАВАНИЯ ДИСЦИПЛИН ГЕОМЕТРО-ГРАФИЧЕСКОГО ЦИКЛА ЭЛЕКТРОННЫХ КУРСОВ В СИСТЕМЕ ОБУЧЕНИЯ MOODLE Ваншина Е.А., канд. пед. наук, доцент	1430
МЕТОДИКА ИЗУЧЕНИЯ IP-КАМЕР В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КАФЕДРЫ ВУЗА ГАЛИМОВ Р.Р., КАНД.ТЕХН. НАУК, ДОЦЕНТ, АЛИЕВ Р.М.	1435

АНАЛИЗ ЗАЩИЩЕННОСТИ СРЕДСТВ УДАЛЕННОГО ДОСТУПА ККОРПОРАТИВНОЙ СЕТИ Галимов Р.Р. канд.техн.наук, доцент, Корнейченко А.В., Мазалов Е.А.....	1441
МЕТОДИКА ПРЕПОДАВАНИЕ ДИСЦИПЛИНЫ «ЧИСЛЕННЫЕ МЕТОДЫ» НА МАТЕМАТИЧЕСКИХ СПЕЦИАЛЬНОСТЯХ Джукашев К.Р., канд.физ.-мат.наук	1448
ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ МАТЕМАТИКЕ Калматаева Б.Б.	1454
РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ ОБРАБОТКИ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ на языке JavaScript Кобылкин Д.С.,канд.тех. наук, Юсупова О.В.....	1459
МАТЕМАТИЧЕСКИЕ ЗАДАЧИ С ЭКОНОМИЧЕСКИМ СОДЕРЖАНИЕМ В ОБРАЗОВАНИИ Колобов А.Н., канд. техн. наук, доцент.....	1468
ЭКОНОМИЧЕСКИЕ ЗАДАЧИ С РАЗЛИЧНЫМИ ВИДАМИ ВЫПЛАТ В МАТЕМАТИКЕ Колобов А.Н., канд. техн. наук, доцент.....	1475
ЭЛЕМЕНТЫ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ И ДИФФЕРЕНЦИАЛЬНОГО ИСЧИСЛЕНИЯ ПРИ РЕШЕНИИ ЭКОНОМИЧЕСКИХ ЗАДАЧ В МАТЕМАТИКЕ Колобов А.Н., канд. техн. наук, доцент	1483
ПОДХОДЫ К ОРГАНИЗАЦИИ СИСТЕМЫ БЕЗОПАСНОСТИ СЕТЕЙ IOT- УСТРОЙСТВ Кузнецова Л.Ю., Парфёнов Д.И., кан. тех. наук,	1491
АЛГОРИТМЫ ФОРМИРОВАНИЯ ДИСКОВЫХ ОБРАЗОВ ДЛЯ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА К УДАЛЕННЫМ РАБОЧИМ ОКРУЖЕНИЯМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ Легашев Л.В., канд.техн.наук, Полежаев П.Н., Коннов А.Л., канд.техн.наук, доцент, Грибович И.О, Матвеев А.А.	1499
ИССЛЕДОВАНИЕ АЛГОРИТМОВ РАБОТЫ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА К УДАЛЕННЫМ РАБОЧИМ ОКРУЖЕНИЯМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ Легашев Л.В., канд.техн.наук, Полежаев П.Н., Коннов А.Л., канд.техн.наук, доцент, Грибович И.О., Матвеев А.А.	1508
АКТИВИЗАЦИЯ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ Максименко Н.В.	1515
МЕТОДЫ КЛАСТЕРИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ Морковина Э.Ф., канд. пед. наук, доцент, Ходырева Д.В.....	1519
РАЗРАБОТКА САЙТА И МЕТОДЫ ЗАЩИТЫ БАЗЫ ДАННЫХ МУХТУБАЕВА С.Н.....	1524

РЕШЕНИЕ ЗАДАЧИ КАТЕГОРИАЛЬНОЙ РЕГРЕССИИ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ И ГРАДИЕНТНОГО БУСТИНГА ДЛЯ ПРОГНОЗИРОВАНИЯ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ МАССОВЫХ ОТКРЫТЫХ ОНЛАЙН-КУРСОВ Нигматулин Г.А., Парфёнов Д.И., канд. техн. наук, Болодурина И.П., д-р техн. наук, проф., Запорожко В.В., канд. пед. наук	1529
ОБ ОРГАНИЗАЦИИ ПРОПЕДЕВТИЧЕСКОГО ИЗУЧЕНИЯ МАТЕМАТИЧЕСКОГО РАЗДЕЛА «ЛИНЕЙНАЯ АЛГЕБРА» СТУДЕНТАМИ ГУМАНИТАРНЫХ НАПРАВЛЕНИЙ Павленко А.Н., канд. физ.-мат. наук, доцент, Пихтилькова О.А., канд. физ.-мат. наук, доцент...	1534
ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ СЕМАНТИЧЕСКОГО АНАЛИЗА И КЛАССИФИКАЦИИ ОБРАЩЕНИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ SERVICEDESK Парфёнов Д.И., кан. тех. наук, Кузнецова Л.Ю.	1538
ПРОБЛЕМЫ М. ДЕНА В КОМБИНАТОРНОЙ ТЕОРИИ ГРУПП Пихтилькова О.А., канд. физ.-мат. наук, доцент, Павленко А.Н., канд. физ.-мат. наук, доцент	1542
ОПЫТ МЕТОДИЧЕСКОЙ РАБОТЫ В ИЗЛОЖЕНИИ ТЕМЫ «ПОНЯТИЕ ПРОИЗВОДНОЙ ФУНКЦИИ» Рассоха Е.Н., канд. пед. наук, доцент, Анциферова Л.М., канд. пед. наук	1548
ПРИМЕНЕНИЕ ИМИТАЦИОННОЙ СРЕДЫ RASCTETTRACER ДЛЯ ИССЛЕДОВАНИЯ БАЗОВЫХ СРЕДСТВ ЗАЩИТЫ СЕТЕВЫХ УСТРОЙСТВ Рычкова А.А., канд. пед. наук, Пантич Д.Р.	1555
О МЕТОДАХ ПРОВЕРКИ ЧИСЛА НА ПРОСТОТУ Сикорская Г.А., д-р пед. наук, доцент, Галушкин Д.А., Данильчук М.В.	1560
О ПРИМЕНЕНИИ АЛГЕБРАИЧЕСКИХ МЕТОДОВ ПРИ РЕШЕНИИ ЭКОНОМИЧЕСКИХ ЗАДАЧ Сикорская Г.А., д-р пед. наук, доцент, Яковлева О.Е.	1570
АНАЛИЗ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ВЫСОКОГО УРОВНЯ Синицын Ю.И., канд. техн. наук, доцент, Байков В.А.	1581
ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ Синицын Ю. И., канд. техн. наук, доцент, Гриценко А. Д.	1586
ДИСТРИБУТИВЫ LINUX КАК АЛЬТЕРНАТИВА ОС WINDOWS	1591
В ПОДГОТОВКЕ ИТ-СПЕЦИАЛИСТОВ Токарева М.А., канд. техн. наук, доцент, Кулантаева И.А., канд. пед. наук	1591

РАЗРАБОТКА ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ «ТЕХНИЧЕСКИЕ СРЕДСТВА РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ» Токарева М.А., канд. техн. наук, доцент, Тлегенова Т.Е., канд. пед. наук	1602
ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДОВ СТЕГОАНАЛИЗА ГРАФИЧЕСКИХ ФАЙЛОВ Шухман А.Е. ¹ , канд.пед.наук, доцент, Шухман Е.В. ² , канд.физ.-мат.наук.....	1608

НАУЧНО-МЕТОДИЧЕСКИЕ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Абдршина В.В.

**Университетский колледж федерального государственного
бюджетного образовательного учреждения высшего образования
«Оренбургский государственный университет»**

Как известно, в современном мире ни одна сфера деятельности человека не обходится без применения средств и методов информационных технологий (ИТ). Развитие ИТ-сферы является основой для совершенствования таких сфер деятельности, как медицина, экономика, строительство и другие. Благодаря высокому уровню развития информационных и инфо-коммуникационных технологий появились так называемые автоматизированные рабочие места, и вся бумажная волокита просто ушла в прошлое, что позволило увеличить производительность труда и снизить вероятности ошибок сотрудника. Столь быстрый темп развития информационных технологий приводит к необходимости подготовки специалистов, обладающих не только соответствующими их профессии знаниями и навыками, но и развитыми умениями в области инфо-коммуникационных технологий (ИКТ). Даже работая преподавателем русского языка и литературы, истории, биологии и др. важно уметь использовать персональный компьютер, мультимедийные комплексы и различное программное обеспечение, работать в сети Интернет. Это необходимо не только для разработки учебно-методического обеспечения дисциплин, но и для применения различного рода технологий при преподавании, что делает процесс восприятия материала обучающимися более интересным и доступным. Проблеме подготовки специалистов в сфере информационных технологий наше государство уделяет особое внимание. Еще в 2010 году была утверждена Государственная программа Российской Федерации «Информационное общество 2011-2020 гг», где основная идея заключается в том, что для развития информационного общества, необходимо повысить качество подготовки специалистов и создать непрерывную систему для обучения в области информационных технологий [1].

Для обеспечения непрерывного обучения важно создать такую среду, где полученные ранее знания будут совершенствоваться на более высоких ступенях образования, то есть так называемое преемственное обучение [2].

Рассмотрим проблемы подготовки в области информационных технологий обучающихся специальности 15.02.07 Автоматизация технологических процессов и производств (по отраслям). На рисунке 1 представлен анализ знаний обучающихся третьего курса данной специальности в различных областях информатики и информационных технологий.

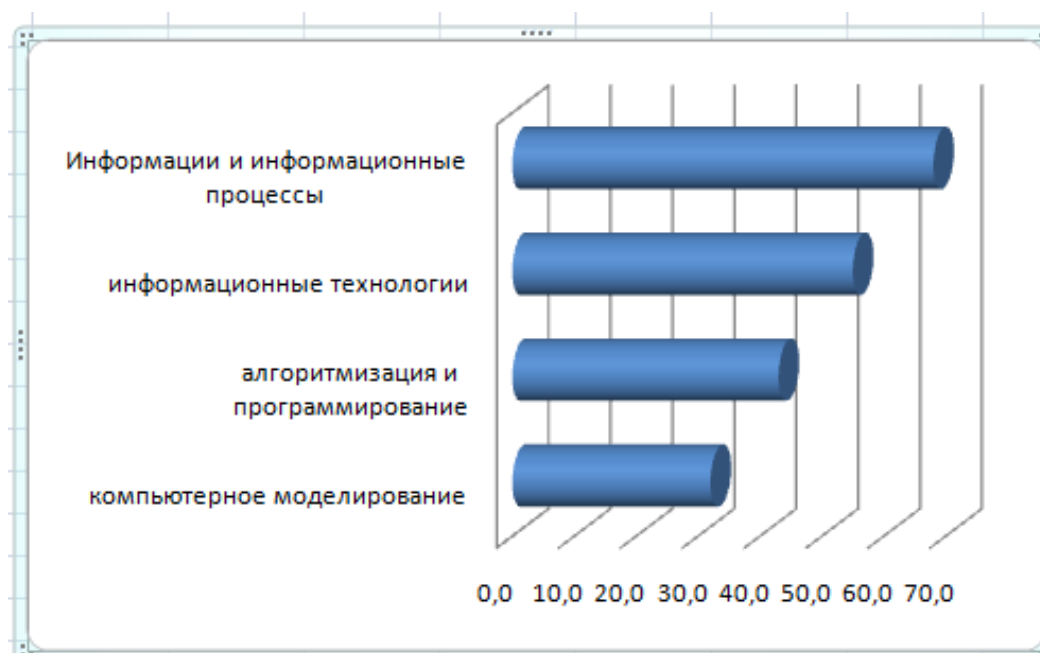


Рисунок 1 – Количественные показания освоения обучающимися третьего курса школьного курса информатики

Анализируя диаграмму, можно констатировать следующее:

- 1) более половины обучающихся имеют низкий уровень подготовки в области компьютерного моделирования и алгоритмизации и программирования (32 % и 43 % соответственно);
- 2) более высокие показатели подготовки можно отметить по разделам «Информатика и информационные процессы» – 68 % и «Информационные технологии» – 55 %.

Вышеперечисленные показатели говорят о достаточно слабом освоении разделов школьной программы, что говорит о возникновении трудностей в желаемой стратегии преемственности обучения «школа-колледж».

Рассмотрим к чему может привести недостаточная подготовка обучающихся по представленным разделам информатики и ИКТ.

Для обучающихся третьего курса специальности Автоматизация технологических процессов и производств (по отраслям) для изучения в шестом семестре предусмотрены дисциплины «Компьютерное моделирование» и «Основы программирования», освоение которых подразумевает определенный объем уже имеющихся знаний обучающихся [3]. Профессиональные компетенции данной специальности включают в себя владение не только навыками работы в тестовых процессорах, но и способности создавать автоматизированные информационные системы. Для освоения профессиональных компетенций обучающийся должен быть уверенным пользователем персонального компьютера.

При имеющихся показателях преподавателю дисциплины «Основы программирования» необходимо восполнить недостающие знания, например, в разработке многотабличных баз данных (БД) с использованием системы

управления базами данных MSOfficeAccess, создании запросов, форм и отчетов к БД. Так же нехватка знаний отмечается при составлении алгоритмов в виде в блок-схем, несмотря на то, что задания такого типа встречаются в программе Единого Государственного Экзамена (ЕГЭ) по информатике.

Ниже представлен вариант задания ЕГЭ по информатике.

В2. Запишите значение переменной a после выполнения фрагмента алгоритма [4-5]:

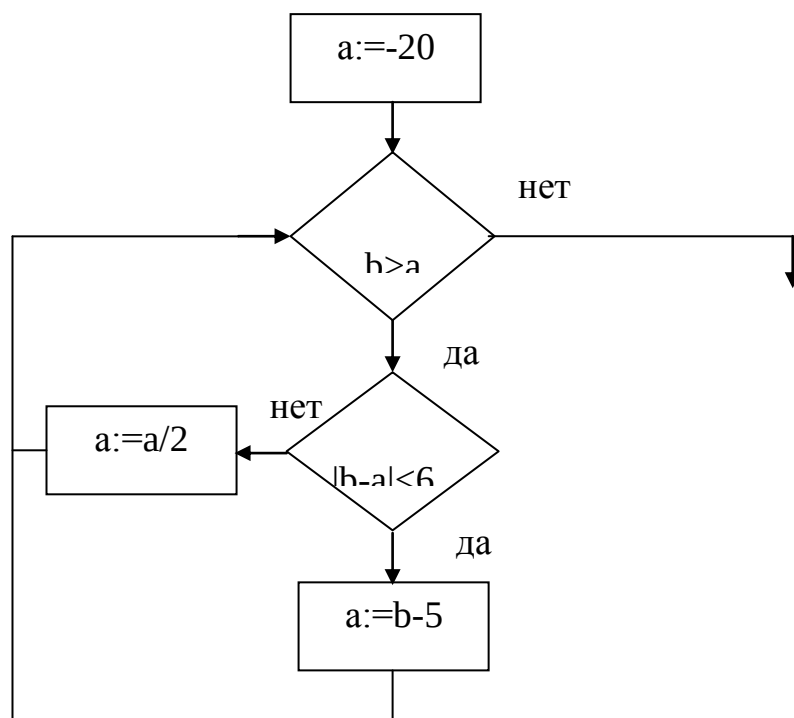


Рисунок 2 – Алгоритм задания из тестов ЕГЭ по информатике

Таким образом главная проблема изучения дисциплин профессионального цикла для обучающихся колледжа состоит в разном уровне освоения школьного курса информатики. Выходом из сложившейся ситуации может стать изучение дополнительных курсов, обеспечивающих совершенствование и тем самым выравнивание знаний, навыком и умений до того уровня, который позволит свободно осваивать профессиональные дисциплины. Реализация данной программы уже давно реализуется в Университетском колледже ОГУ: курс дополнительного профессионального образования включает более десяти направлений.

В заключение хотелось бы отметить, что в 2019-2020 учебном году в Университетском колледже ОГУ разработана программа дополнительного профессионального образования «Основы компьютерной грамотности (технический профиль)», которая позволит обучающимся улучшить знания в области ИКТ, приобрести необходимые для дальнейшего обучения умения и навыки.

Список литературы

1. Государственная программа Российской Федерации «Информационное общество 2011-2020 гг» [Электронный ресурс] .- Режим доступа: <http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html>
2. Президентская программа повышения квалификации инженерных кадров [Электронный ресурс] .- Режим доступа: <http://engineer-cadry.ru/>
3. Иванов, А.А. Автоматизация технологических процессов и производств : учеб. пособие для вузов / А.А. Иванов .– 2-е изд., испр и доп.– М. : ФОРУМ : ИНФРА-М, 2016 .– 224 с.– (Высшее образование) .– ISBN 978-5-91134-948-6
4. Портал федерального Интернет-экзамена в сфере профессионального образования [Электронный ресурс] .- Режим доступа: <http://www.i-exam.ru/>
5. Портал федерального Интернет-экзамена в сфере профессионального образования [Электронный ресурс] .- Режим доступа: <http://www.fepo-nisa.ru/> .- Загл. с экрана .- 09.12.2019.

ПРИМЕНЕНИЕ МАКРОСОВ ТАБЛИЧНОГО ПРОЦЕССОРА В ЗАДАЧЕ ИССЛЕДОВАНИЯ ИМИТАЦИОННОЙ МОДЕЛИ МАРШРУТИЗАЦИИ СЕТЕВЫХ ПОТОКОВ

**Абрамова Т. В., Аралбаев Т. З., д-р техн. наук, профессор
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Актуальность темы работы определяется необходимостью подготовки и предоставления методического материала студентам, изучающим вопросы защиты передачи технологической информации в распределенных системах управления с резервным каналом связи. В качестве технологического объекта в работе рассмотрена распределенная автоматизированная система управления (АСУ) процессом транспортировки нефтегазового сырья [1].

Анализ методических разработок по теме исследования, в частности, [1-4], показал, что в настоящее время перечень работ, позволяющих предоставить учащимся в доступной форме актуальные сведения по вопросам имитационного моделирования процессов маршрутизации сетевых потоков в режимах переключения на резервные каналы связи, ограничен.

Цель работы: освоить методику исследования имитационной модели маршрутизации сетевых потоков информации с использованием макросов табличного процессора.

Для достижения цели в работе представлены:

- графовая модель потоков сетевого трафика в системе сбора и регистрации данных резервным каналом связи;
- порядок построения имитационной модели маршрутизации сетевых потоков с использованием макросов табличного процессора;
- алгоритм исследования имитационной модели;
- экранная форма полученных результатов.

Графовая модель потоков сетевого трафика в системе сбора и регистрации данных о состоянии технологического объекта представлена на рисунке 1. Концепция защиты передачи технологической информации, положенная в основу данной модели, предполагает, что после обнаружения обрыва линии связи, источники информации, потерявшие связь с диспетчером, воспользуются резервным каналом передачи информации – высоковольтной линией электропередач. Остальные источники будут работать в обычном режиме, продолжая передавать информацию по основному каналу.

При этом, информация о состоянии технологического объекта будет передана диспетчеру своевременно и без потерь.

- $R3$ - подмножество ребер, обозначающих линии связи между узлами коммутации и портами обмена информацией.

Задача определения маршрута передачи данных при обрыве линии связи ставится следующим образом:

- $M=\{M_1, M_2, \dots, M_n\}$ – множество разрешенных маршрутов передачи информации;

- $m=\{m_1, m_2, \dots, m_s\}$ – множество звеньев маршрута; s –количество звеньев маршрута.

- $O=\{O_1, O_2, \dots, O_n\}$ – множество возможных событий обрыва.

Для каждого источника информации I требуется определить маршрут передачи данных M^x диспетчеру D , при котором при любом возможном событии O будет обеспечена полнота получаемой диспетчером информациио состоянии технологического объекта.

Обеспечение данного условия осуществляется путем переключения портов на узлах коммутации. Для переключения используются следующие правила: если источник информации теряет связь с диспетчером, то ближайший к нему узел коммутации переключается на порт резервного канала связи; если связь с диспетчером установлена, то источник продолжает передавать данные по основному каналу связи. Ввиду наличия линейной топологии сети, все источники информации, находящиеся дальше места обрыва, переключаются на резервный канал, как показано в выражениях (1).

$$\begin{aligned} k_{es} &= 1, k_{ls} = 0, \text{ ЕСЛИ } (e_1 \cap e_2 \cap \dots \cap e_s) = 1 \\ k_{es} &= 0, k_{ls} = 1, \text{ ЕСЛИ } (e_1 \cap e_2 \cap \dots \cap e_s) = 0 \end{aligned} \quad (1)$$

Для определения маршрутов в режимах переключения на резервные каналы связи целесообразно использовать матрицу смежности, позволяющую наглядно показать связи между узлами системы. Матрица смежности для графа, изображенного на рисунке 1(а), представлена на рисунке 1(б).

В качестве примера реализации модели была рассмотрена автоматизированная система управления, включающая диспетчера и три источника информации о состоянии технологического объекта. Графовая модель потоков сетевого трафика для рассмотренного примера включает 14 вершин. Таблица маршрутизации сетевых потоков информации представлена в таблице 1.

Таблица 1 - Таблица маршрутизации сетевых потоков в режиме переключения на резервные каналы связи для 3 источников информации

Источник информации	Узел коммутации	Маршруты	
		Участок обрыва	Маршрут
1	2	нет обрыва	1-2-3-7-11-13-14
		е1, е2, е3	1-2-4-8-12-13-14
5	6	нет обрыва	5-6-7-11-13-14
		е2, е3	5-6-8-12-13-14
9	10	нет обрыва	9-10-11-13-14
		е3	9-10-12-13-14

Порядок построения имитационной модели с использованием макросов табличного процессора имеет ниже перечисленные пункты.

1. Задается матрица смежности для рассматриваемого графа.
2. С помощью генератора случайных чисел задаются значения состояния сегментов основного канала связи в диапазоне от 0 до 1 (1 – регламентированное состояние, 0 – обрыв линии связи). Данные генерируются автоматически с применением макросов табличного процессора. Ячейки, содержащие нулевые значения, выделяются цветом.

3. С помощью функций табличного процессора определяются порты передачи информации. Ячейки, содержащие значения состояния активных портов заштриховываются с применением настроек условного форматирования.

4. В соответствии с математическими выражениями (1) и таблицей 1, программируются маршруты передачи информации с применением макросов табличного процессора.

На рисунке 2 представлена экранная форма процесса имитационного моделирования маршрутизации сетевых потоков информации с использованием макросов табличного процессора. На вход модели подаются данные о состоянии сегментов основного канала связи. Результатом работы имитационной модели является таблица маршрутов передачи данных для каждого из источников, построенная с учетом наличия и места обрыва основного канала связи. На рисунке красным цветом выделены ячейки, характеризующие состояние сегментов основного канала. Заштрихованные ячейки показывают активные порты передачи данных.

Рисунок 2 – Экранная форма процесса имитационного моделирования маршрутизации сетевых потоков информации с использованием макросов табличного процессора

Разработанная в табличном процессоре MSExcel имитационная модель на основе стандартных формул обычно позволяет проводить исследования в статическом режиме. Для исследования модели в динамике для ряда последовательных тактов применение только данного механизма является недостаточным, поскольку необходимо вручную задавать входные данные для каждого нового шага.

Одним из вариантов устранения этого недостатка является использование макросов, созданных при помощи языка Visual Basic Application(VBA) [5]. В рамках данной работы разработаны макросы *Break_simulation* и *Routing*, вызываемые по нажатию кнопок «Моделирование обрыва линии связи» и «Определить маршрут», соответственно. По нажатию первой кнопки вызывается макрос, генерирующий значения состояния сегментов основного канала связи в диапазоне от 0 до 1 в соответствующих ячейках. При нажатии второй кнопки в соответствии с состоянием линий связи рассчитываются маршруты передачи данных. Полученные результаты записываются в таблицу маршрутизации.

На рисунке 3 представлена экранная форма программного кода макроса *Routing*.



Рисунок 3 - Экранная форма программного кода макроса *Routing*

Таким образом, использование макросов позволяет автоматизировать процесс проведения вычислительных экспериментов и исследовать модель в динамике. При этом необходимо отметить простоту программирования, использования и реализации макросов.

Достоинствами предложенной методики являются:

- доступность и наглядность представления имитационных моделей, средствами офисных приложений операционной системы;
- возможность разработки и использования имитационной модели студентами с различным уровнем подготовки в области знаний языков программирования;
- рассмотренная программа может быть интегрирована с программами на языках высокого уровня для демонстрации и визуализации результатов моделирования.

Данная методика успешно апробирована на кафедре вычислительной техники и защиты информации ОГУ в процессе выполнения лабораторных работ по дисциплинам бакалавриата и магистратуры студентами профилей «Комплексная защита объектов информатизации» и «Информатика и вычислительная техника».

Список литературы

1. Абрамова, Т. В. Моделирование процессов защиты передачи технологической информации по резервному каналу на основе анализа сетевого трафика/Т. В. Абрамова, Т. З. Аралбаев, А. В. Манжосов // «Инновационные, информационные и коммуникационные технологии:

сборник трудов XVI международной научно-практической конференции; Сочи, 2019. – 5 с

2. Аралбаев, Т. З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, 2018. -160 с. ISBN – 978-5-7410-2202-3 2.

3. Ежов, А. В. Натурное моделирование процесса многомерной маршрутизации пакетов в TCP/IP сети // Вестник науки и образования. 2017. №2 (26). URL: <https://cyberleninka.ru/article/n/naturnoe-modelirovanie-protsessa-mnogomernoy-marshrutizatsii-paketov-v-tcp-ip-seti> (дата обращения: 18.12.2019).

4. Попов, Г. А. Алгоритм маршрутизации сетевых потоков с учетом требований по безопасности/Г. А. Попов, Е. А. Попова // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2016. №2. URL: <https://cyberleninka.ru/article/n/algorithm-marshrutizatsii-setevyh-potokov-s-uchetom-trebovaniy-po-bezopasnosti> (дата обращения: 25.12.2019).

5. Михеев Р.Н. VBA и программирование в MS Office для пользователей/Р.Н. Михеев. –СПб.: БХВ-Петербург, 2006. -384 с.

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ МАТЕМАТИЧЕСКОГО ПАКЕТА НА ОС ANDROID

Амантаева А.С.

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

В наше время нет необходимости пользоваться таблицей умножения или в совершенстве знать понятие логарифма для того, чтобы найти произведение ряда чисел. С помощью даже простейшего калькулятора выполнять любые арифметические действия намного проще и надежнее, чем в уме или даже на бумаге[1]. Для вычисления самых «заумных» специальных математических функций достаточно воспользоваться научным микрокалькулятором или подходящей программой для вычисления таких функций, но в современном мире они не всегда оказываются под рукой, нежели, чем мобильный телефон чаще с ОС Android.

Математическое программирование на сегодняшний день занимает важную составляющую всего программирования. Громоздкие и трудные вычисления благодаря несложным программам становятся простыми.

Поэтому развитие реализаций математических пакетов для ОС Android имеет огромное практическое значение.

В данной работе рассматривается вопрос создания программы математический пакет для Android.

Объект исследования в этой работе – математический пакет для операционной системы Android.

Предмет исследования – способы создания универсального математического пакета для операционной системы Android.

Цель работы – реализовать математический пакет для операционной системы Android.

Прежде чем начать проектирование программного средства, необходимо рассмотреть способы вычислений какого-либо алгоритма:

1. Вручную на бумаге – возможность ошибиться при подстановке или на разных этапах вычислений. Данный способ ограничивается человеческим фактором и временем, затраченным на его реализацию.

2. В уме – возможность ошибки, недостаточный объем памяти, длительный ресурс времени. Данный способ является недостаточно точным, так как важную роль играет человеческий фактор.

3. Микрокалькулятор – маленький объем памяти, производит расчёт не по всем алгоритмам, ответ приближителен и, при слишком больших или маленьких числах, представляется в форме $a \cdot 10^b$.

4. Решение-онлайн – не всегда есть доступ в интернет, чаще представлен в форме $a \cdot 10^b$.

Одним из наиболее эффективных способов вычислений с практической точки зрения является вычисление с помощью математического пакета на мобильном приложении, у которого бесплатная установка, и после неё не требует выхода в интернет.

Суть вычисления на мобильном приложении заключается в том, чтобы вычисления занимали как можно меньше времени, рассчитывались с большим объёмом данных, были точны в расчётах, а также производились без выхода в интернет и имея удобный интерфейс.

Математический пакет на мобильном приложении, как способ вычисления, можно считать сравнительно новым и перспективным (первые статьи, посвященные расчёту через мобильное приложение, появились примерно три-четыре года назад).

На рынке операционных систем мобильных приложений Android всегда занимал лидирующие позиции среди пользования. По этой причине в данном случае будем рассматривать мобильное приложение математический пакет именно на ОС Android.

Для создания программного средства была выбрана каскадная модель жизненного цикла. Предпочтение было отдано данной модели ЖЦ, так как приложение не является достаточно крупным и полномасштабным проектом для склонения к спиральной модели ЖЦ.

Основная задача данного программного средства – вычисление задач линейной алгебры и теории чисел.

Для проектирования работы программного продукта составим диаграмму последовательности (англ. Sequence diagram) – диаграмма, на которой для некоторого набора объектов на единой временной оси показан жизненный цикл какого-либо определённого объекта и взаимодействие пользователей в рамках какого-либо определённого прецедента, либо всего программного продукта[2].

Диаграмма последовательности для прецедента выбора файла с исходным кодом представлена на рисунке 1.

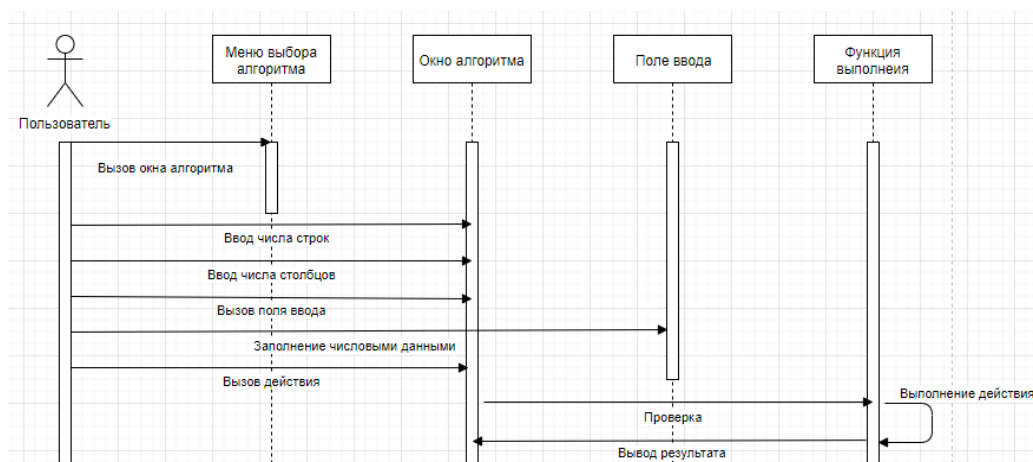


Рисунок 1

Пользователь на главном меню выбора алгоритма выбирает подходящий для себя алгоритм, который будет удовлетворять решению определенной задачи и вызывает «Окно выбора алгоритма». Вводит число строк и столбцов и вызывает «Поле ввода».

Дальше пользователь заполняет поля числовыми данными и вызывает действие, которое хочет совершить над этим полем.

После данные отправляются на проверку в функцию проверки, если данные соответствуют требованиям, то выполняется действие и происходит вывод результата действия на окно алгоритма.

Приступим к разработке. Требования к приложению я сформулировала так:

1) Максимально широкий охват поддерживаемых устройств. Отсюда минимальный API level 8;

2) Поддержка экранов различных разрешений и портретной ориентации;

3) Математика безгранична[3]. Все не реализовать. Поэтому начальный функционал включает в себя действия над матрицами, вычисление факториала, НОД, НОК, функции Эйлера, символа Якоби и символа Лежандра. При их реализации использовались бы такие методы как: нахождение определителя, обратной матрицы, транспонированной матрицы, ранга, умножение матрицы на число, возведение матрицы в степень, сложение двух матриц, произведение двух матриц, разность двух матриц.

Далее в зависимости от предпочтений пользователей:

1) Возможность вставки текста, но функционал редактирования текста для начала минимальный;

2) Удобность использования и качество имеют приоритет над функционалом;

3) Языки только те, что знаю сама для комфортного пользования без обращения к переводчику.

Для разработки данного программного средства была выбрана среда разработки Android Studio, основанная на программном обеспечении IntelliJ IDEA от компании JetBrains, позволяющая разрабатывать приложения для любых устройств на ОС Android. Данная IDE имеет множество достоинств, некоторые из которых:

1 В данной IDE происходит рефакторинг кода.

2 Сборка приложения основана на Gradle, система автоматической сборки, построенная на принципах Apache Ant и Apache Maven.

3 Статический анализатор кода (Lint), позволяющий находить проблемы производительности, несовместимости версий и другое.

4 Различные виды сборок и генерация нескольких .apk файлов.

5 Поддержка разработки приложений для Android Wear и Android TV [4].

Для написания программы был выбран язык программирования высокого уровня – Java, так как он является многофункциональным, удобным объектно-ориентированным языком.

Для реализации пользовательского интерфейса был использован расширенный редактор макетов: WYSIWYG, способность работать с UI компонентами при помощи Drag-and-Drop.

После открытия файла MobMath.apk, появляется главное окно приложения для вычисления (рисунок 2), которое состоит из подсказок нажатия и кнопок для взаимодействия программы с пользователем.

Чтобы начать работу с приложением необходимо выбрать требуемый алгоритм для последующих вычислений и нажать на соответствующую кнопку («Действия над матрицами», «Факториал», «НОД», «НОК», «Функция Эйлера», «Символ Якоби», «Символ Лежандра»).

При нажатии на кнопку «Факториал» открывается диалоговое окно, которое предлагает ввести число, для которого требуется посчитать факториал. Если пользователь попытается ввести букву, то на экран ничего не выведется, так как предусмотрено введение только числовых данных.

После ввода числа, пользователь нажимает на кнопку «Рассчитать» и ответ выводится на не редактируемое поле. Факториал считается при вводе числа не более 66666. Результат выводится с точностью до последнего числа с возможностью листать ответ. На следующем скриншоте можно ознакомиться с интерфейсом приложения.

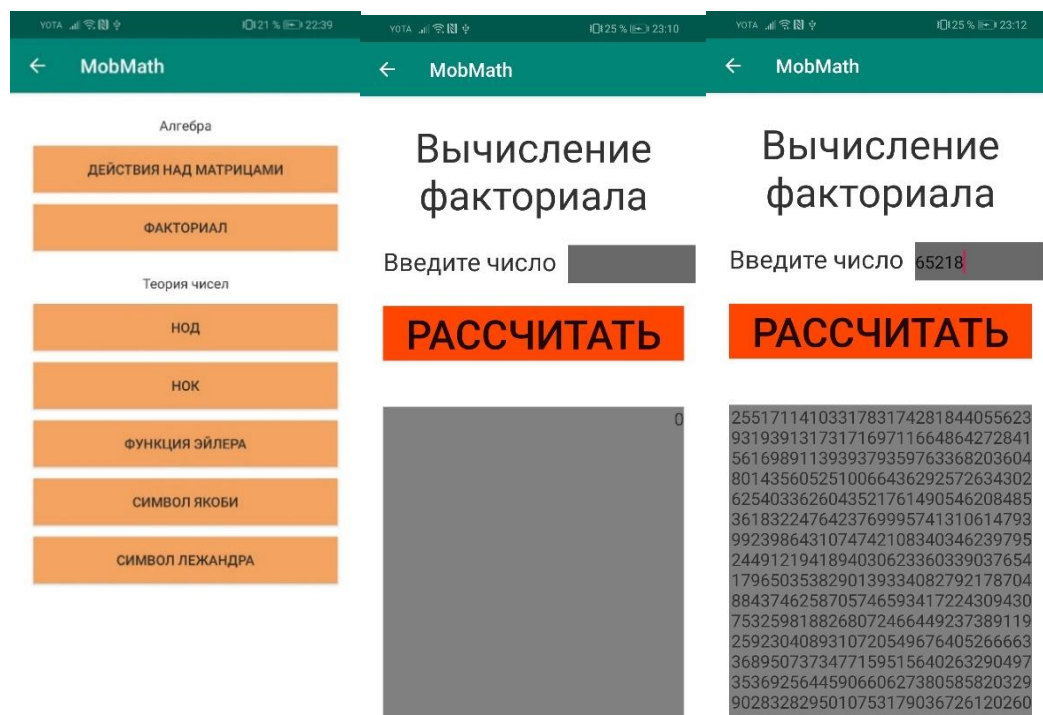


Рисунок 2

Таким образом, в рамках статьи был разработан математический пакет для мобильного приложения на ОС Android. В следующем этапе реализации планируется добавление новых нужных вещей, такие как графики функций и возможно что-то из криптографии.

Список литературы

1 Дьяконов, В.П. Новые информационные технологии: Учебное пособие. Часть 3. Основы математики и математическое моделирование / Дьяконов, В.П, Абраменкова, И.В, Пеньков, А.А. – Смоленск: СГПУ, 2003. - 7 с.

2 Статья из свободной энциклопедии о диаграмме последовательности [Электронный ресурс]. – 2019. – Режим доступа: http://ru.wikipedia.org/wiki/Диаграмма_последовательности – 18.10.2019.

3 Блог на хабре о разработке под Android [Электронный ресурс]. – 2019. – Режим доступа: http://habrahabr.ru/blogs/android_development/ – 20.10.2019.

4 Статья из свободной энциклопедии о диаграмме последовательности [Электронный ресурс]. – 2019. – Режим доступа: http://ru.wikipedia.org/wiki/Android_Studio – 19.10.2019.

КЛАСТЕРНЫЙ АНАЛИЗ КАК ИНСТРУМЕНТ ПОСТРОЕНИЯ И ИССЛЕДОВАНИЯ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ МОДЕЛЕЙ УГРОЗ

**Аралбаев Т.З., д-р техн. наук, профессор, Абрамова Т.В., Гетьман М.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Одной из начальных задач разработки системы защиты объектов информатизации является построение модели угроз (МУ). Актуальность применения кластерного анализа в задачах построения МУ в настоящей работе обусловлена необходимостью разработки инструментального средства, позволяющего реализовать дифференцированный подход к защите распределенного объекта информатизации (РОИ). Анализ публикаций [5,7] позволил определить современное состояние исследований по теме кластерного анализа угроз информационной безопасности. Главным недостатком данных исследований является отсутствие решений, предназначенных для РОИ, а вопросы дифференцирования пространственно-временных моделей угроз (ПВМУ), рассмотренные в [8], не позволяют в должной мере использовать возможности кластерного анализа ПВМУ.

Целью работы является повышение уровня понимания процедуры построения и анализа моделей угроз студентами профилей информационной безопасности.

Для достижения поставленной цели решены следующие задачи:

- разработано математическое описание метода кластерного анализа частных моделей угроз информационной безопасности на основе матричной модели;
- разработано программное обеспечение, позволяющие исследовать пространственно-временные модели угроз (ПВМУ);
- представлены рекомендации по применению в учебном процессе метода кластерного анализа ПВМУ.

Отличительной особенностью задачи построения модели угроз для распределенных объектов информатизации является изменение характера угроз в пространстве и во времени. Это приводит к необходимости применения дифференцированного подхода в задаче построения МУ, обеспечивающего выделение отдельных участков объекта защиты с характерными угрозами и, соответственно, методов защиты на этих участках. Это наглядно представлено на рисунке 1 для РОИ, на котором «МУ-1»..«МУ-20» обозначено множество частных моделей угроз для защищаемого объекта.

Для формализации задачи кластеризации моделей угроз использованы следующие условные обозначения [6]:

- $Q = \{q_1, .. q_N\}$ – множество моделей угроз, где N – число моделей угроз, подлежащих кластеризации;

- $Y=\{y_1, .. y_M\}$ – множество угроз информационной безопасности, где M – число угроз Q ;
- $\langle s_{n,i} \rangle$ – значение для i -ой угрозы в множестве моделей угроз N , где $i=1...M, n=1$ где $i=1...N$;
- m_i – среднее значение параметров для i -ой угрозы по всем исследуемым моделям угроз;
- $K_n= k_1k_2..k_i$ – классификационные коды моделей угроз, где $i=1...N$.

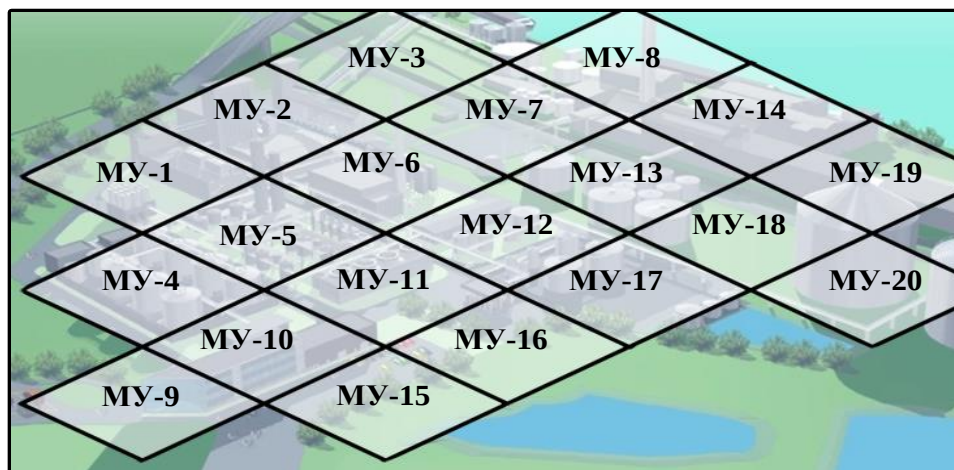


Рисунок 1 – Схема разбиения распределенного объекта информатизации на частные модели угроз

$$k_{nm} = \begin{cases} 1, \text{если } \langle s_{n,i} \rangle \geq m_i; \\ 0, \text{если } \langle s_{n,i} \rangle < m_i; \end{cases} \text{ где } i = 1..M, n = 1..N, \quad (1)$$

$$m_i = \frac{\sum_{n=1}^N s_{n,i}}{N}, \text{ где } i = 1..M, n = 1..N. \quad (2)$$

В таблице 1 для примера представлены результаты расчёта частных классификационных кодов по выражению (1).

Таблица 1 – Таблица классификационных кодов для каждой модели угроз

	МУ 1	МУ 2	МУ 3		МУ N
Угр оза 1	0	0	1		1
Угр оза 2	1	0	1		0
...	...	...	...		...
Угр оза M	0	1	0		0
K_n	01 ... 0	00 ... 1	11 ... 0		10 ... 0

Представленная математическая модель реализована в виде программ [1,2], используемых в качестве инструментальных средств студентами при разработке и исследовании моделей угроз РОИ.

На рисунках 2-3, в частности, представлены экранные формы результатов работы программы [1], реализующей алгоритм кластеризации, представленный в работе [6].

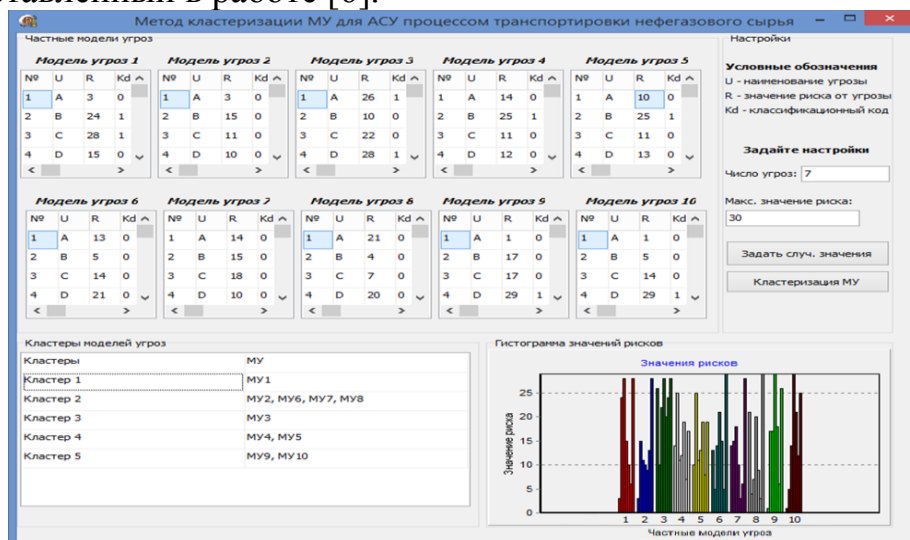


Рисунок 2 – Экранная форма программы «Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья»

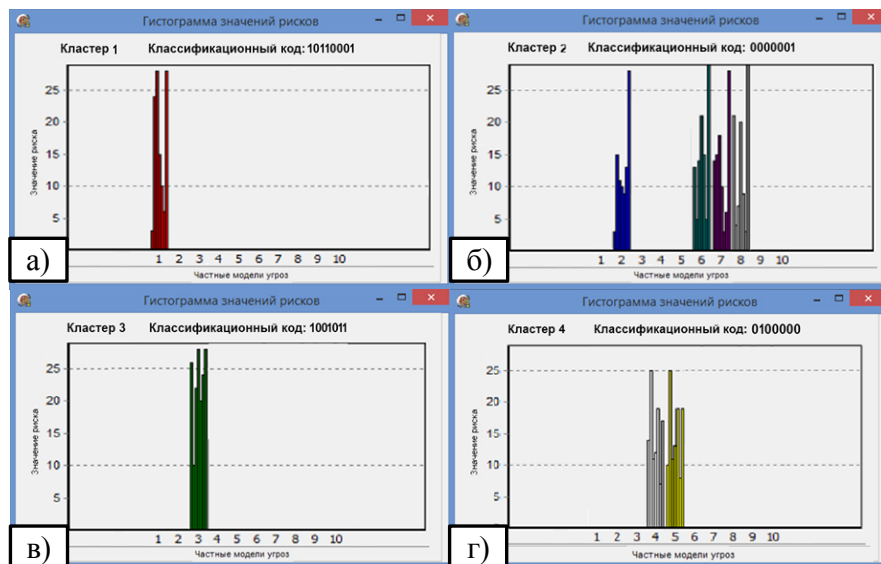


Рисунок 3 – Гистограммы значений рисков от угроз для частных МУ: а) кластера 1; б) кластера 2; в) кластера 3; г) кластера 4.

К достоинствам разработанных программ относятся:

- автоматизация процесса кластеризации частных моделей угроз информационной безопасности;
- простота и наглядность представления состава и расположения угроз в пространстве;
- демонстрация дифференцированного подхода к задаче построения модели угроз.

Применение метода кластеризации частных МУ для РОИ позволяет:

- изучить матричный подход в задаче кодирования и классификации угроз, позволяющий уточнить степень актуальности угроз информационной безопасности и принять адекватные меры при построении систем защиты для РОИ;
- объединить множество частных моделей угроз в группы с общими параметрами (такими, как вероятность возникновения угрозы, ущерб и риск), на основе анализа которых студенты могут исследовать характер изменения угроз, принимать рациональные технические решения.

Представленные инструментальные средства успешно апробированы в учебном процессе кафедры вычислительной техники и защиты информации ОГУ.

Список литературы

- 1 Абрамова, Т. В. Метод кластеризации моделей угроз для распределенной АСУ процессом транспортировки нефтегазового сырья [Электронный ресурс]: прикладная программа / Т. В. Абрамова, Т. З. Аралбаев; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург: ОГУ. - 2019. - 10 с.
- 2 Аралбаев, Т. З. Кластерный анализ моделей угроз для мобильных объектов информатизации [Электронный ресурс]: прикладная программа / Т. З. Аралбаев, М. А. Гетьман; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т". - Оренбург: ОГУ. - 2019. - 8 с.
- 3 Аралбаев, Т. З. Оптимизация методов контроля технического состояния распределенных автоматизированных систем в условиях воздействия пространственно-временных угроз на основе мониторинга сетевых информационных потоков: монография / Т. З. Аралбаев, Г. Г. Аралбаева, Т. В. Абрамова, Р. Р. Галимов, А. В. Манжосов; Оренбургский гос. ун-т. - Оренбург: ОГУ, - 2018. - 160 с.
- 4 Банк данных угроз безопасности информации // ФСТЭК России [Электронный ресурс]. – режим доступа: <https://bdu.fstec.ru/threat>
- 5 Бурькова, Е. В. Применение метода кластеризации данных для решения задачи оценки рисков информационной безопасности / Бурькова Е. В., Извекова Л. А. // Национальная безопасность и стратегическое планирование, 2019. - № 2 (26). - С. 81-86. - 6 с.

6 Гетьман, М.А. Метод кластеризации моделей угроз для мобильных объектов информатизации / М.А. Гетьман, Т.З. Аралбаев // Студент года 2019: сборник статей Международного научно-исследовательского конкурса. В 3-х частях. Часть 3.– Петрозаводск:МЦНП «Новая наука», 2019. –С. 9-15. – 7 с.

7 Лось, А.Б. Особенности использования кластерного анализа в системе менеджмента информационной безопасности [Электронный ресурс] / А.Б. Лось, А.С. Кабанов, В.И. Трунцев // Промышленные АСУ и контроллеры, 2013. - № 8. - С. 67-71. - 5 с.

8 Попов, Ю.В. Применение кластерного анализа для группирования угроз информации, зарегистрированной самописцем / Ю.В. Попов // Научный вестник МГТУ ГА, 2005. - №86. – С. 99-123. – 5 с.

АЛГОРИТМ КОЛЛЕКТИВНОЙ САМООЦЕНКИ РЕЗУЛЬТАТОВ ТЕСТА В УСЛОВИЯХ ДЕФИЦИТА АППАРАТНО-ВРЕМЕННОГО РЕСУРСА

Аралбаев Т.З., д-р техн. наук, профессор, Калинина В.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

Одной из актуальных задач управления учебным процессом является наличие обратной связи в контуре управления с достоверной информацией о состоянии системы обучения, в данном случае о степени усвоения изучаемого материала.

В современной научно-методической литературе известен большой перечень публикаций посвященных вопросу оценки знаний с использованием современных компьютерных технологий. Примерами тому являются, в частности, работы [1,2]. Общим недостатком этих работ является необходимость привлечения большого потенциала мультимедийной аппаратуры и аппаратно-программных средств для проведения тестирования учащихся, также отсутствие визуального контроля за процессом проверки знаний при дистанционной форме тестирования, что снижает достоверность оценки результатов. В частности, как отмечается в работе [1], при компьютерном тестировании при наличии 50 терминалов и длительности тестирования 45 минут затраты времени на всю процедуру тестирования составляют 2,25 часа.

К особенностям процедуры тестирования следует отнести возможные неточности при внесении данных в бланки ответов, двойственность ответов при постановке тестовых вопросов, технические погрешности в виде опечаток, нечеткой записи ответов и другие.

Целью разработки предложенного алгоритма является повышение достоверности оценки результатов проверки знаний в условиях ограниченного времени на основе коллективной самооценки результатов теста.

Целевая функция предлагаемой процедуры тестирования имеет следующий вид:

$$D = \frac{N_k}{N_o} \cdot 100\% \rightarrow \max,$$
$$T_r \leq T_d; Z_a \leq Z_d,$$

где D – достоверность оценки теста;

N_k – число корректных вопросов, на которые даны точные ответы;

N_o – общее число вопросов теста;

T_r и T_d – реальное время и допустимое время на проведение тестирования;

Z_r и Z_d – соответственно, реальные и допустимые затраты на аппаратно-программные средства на проведение тестирования.

Ресурсы для проведения интерактивного тестирования:

- презентация с вопросами теста (ПТ1);
- презентация с вопросами теста и ответами (ПТ2).
- мультимедийная система: компьютер, проектор, экран.
- бланк тестирования (БТ).

На рисунке 1 представлен предлагаемый алгоритм коллективной самооценки результатов теста в условиях дефицита аппаратно-временного ресурса.

Вершины графа обозначают узлы маршрута передачи информации в системе тестирования, а ребра – направления и возможные характеристики маршрутов. Каждому шагу тестирования соответствует свой фрагмент в графовой модели. Принцип работы алгоритма понятен из его схемы и описания условных обозначений.

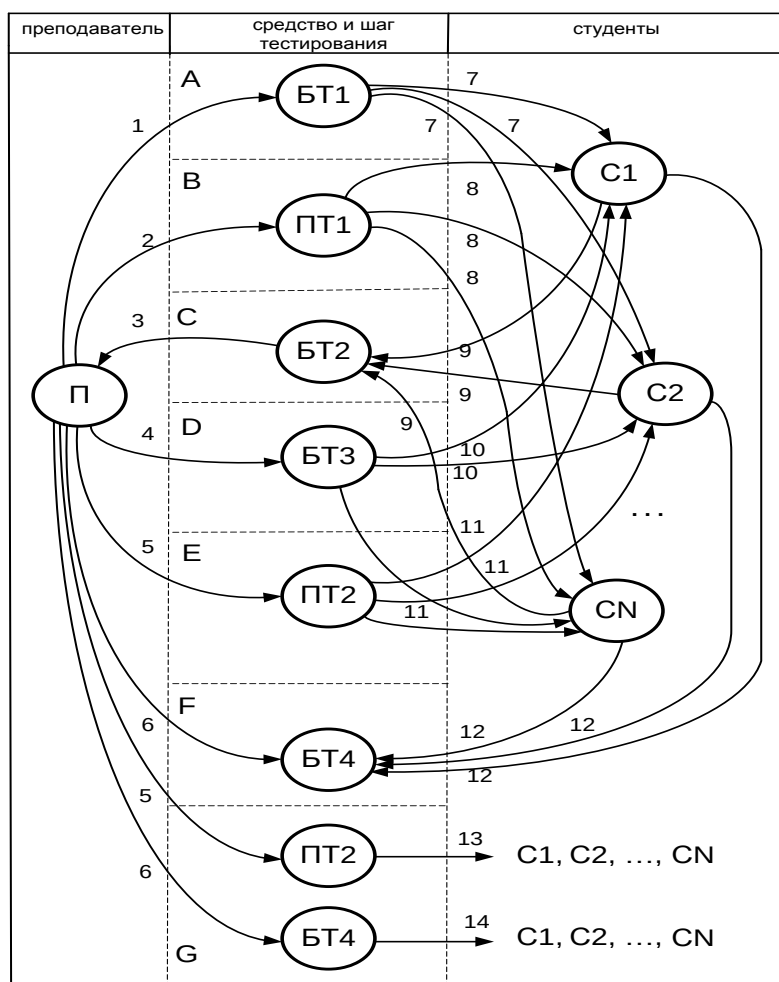


Рисунок 1 – Граф-схема алгоритма коллективной самооценки результатов теста

На рисунке 1 приняты следующие условные обозначения:

- П – преподаватель;

- БТ1, БТ2, БТ3 и БТ4 – соответственно бланки тестирования: исходный, после ответа на тесты, после присвоения идентификационного номера и отреза шапки бланка тестирования и после выставления оценок студентами;

- ПТ1 и ПТ2 – соответственно: презентации тестов без ответов и с ответами;

- С1, С2, СN - студенты, N – число тестируемых студентов;

- А, В, С, D, E, F и G– обозначения шагов тестирования:соответственно, выдача студентам БТ1, подача теста в виде ПТ1, сбор БТ2, выдача БТ3 после присвоения и идентификационного номера и отреза шапки БТ2, подача презентации ПТ2, оглашение результатов оценки и обсуждение результатов тестирования.

Для тестирования необходимо подготовить бланки тестирования в соответствии с рисунком 2, презентацию с вопросами и презентацию с вопросами и ответами.

Таблица 1 – Форма бланка тестирования

ФИО студента: <i>Иванов Иван Иванович</i> (заполняется студентом на шаге А)					
Идентификационный номер (<i>выставляется преподавателем на шаге С в двух позициях * и **</i>)					001 *
линия разреза (шапка отрезается на шаге D)					001 **
№ вопроса	Код ответа студента (<i>выставляется тестируемым студентом на шаге С</i>)	Код ответа по тесту (<i>выставляется проверяющим студентом на шаге F</i>)	№ вопроса	Код ответа студента (<i>выставляется тестируемым студентом на шаге С</i>)	Код ответа по тесту(<i>выставляется проверяющим студентом на шаге F</i>)
1			11		
2			12		
9			13		
...	...	...	...	...	...
10			20		
Общее число совпадений: (<i>выставляется проверяющим студентом на шаге F</i>)					
Процент совпадений по тесту: (<i>выставляется проверяющим студентом на шаге F</i>)					

Алгоритм тестирования в соответствии с рисунком 1 содержит 7 шагов, обозначенных латинскими буквами от А до G:

А: Раздача студентам бланков тестирования; Студенты заполняют регистрационную область в полученных бланках, указывая своё имя и фамилию;

В: Запуск презентации с вопросами, переход к процедуре ответов;

С: Сбор бланков с результатами тестирования с фамилиями студентов и их ответами на тест;

Д: Выставление преподавателем идентификационного номера студента (ИНС), отрезание шапки бланка и передача бланков студентам для проверки. Личности проверяющих студентов могут быть любые (или случайные) по усмотрению преподавателя, шапка бланка остается у преподавателя;

Е: Запускается презентация с ответами, студенты выставляют правильные ответы в столбцах с названием «код ответа по тесту», просчитывают процент ответов, совпадающих с ответами на презентации;

Ф: Преподаватель называет идентификационный номер студента, проверяющий студент по данному ИНС называет оценку и передает бланк тестирования тестируемому студенту по его фамилии;

Г: Производится обсуждение результатов тестирования с использованием презентации с ответами и бланков результатов тестирования.

Достоверность оценки результатов тестирования повышается за счет участия в процедуре оценки как минимум четырех субъектов: преподавателя, тестируемого, третьего лица из числа студентов, проверяющего результат теста, и всего контингента тестируемых при обсуждении оценки теста.

К достоинствам алгоритма можно отнести малую чувствительность времени тестирования к контингенту N студентов, поскольку численность коллектива проверяющих студентов также равна N , в частности, для тестирования одной группы студентов при $N=25$ достаточно полутора часов. Предложенная процедура тестирования может быть модифицирована под конкретную дисциплину.

Алгоритм был успешно применен на кафедре вычислительной техники и защиты информации в процессе рубежного тестирования студентов направления «Информационная безопасность».

Список литературы

1. Использование компьютерного тестирования как фактора повышения качества оценки высшего образования / В.А. Березовский, В.Н. Фокина // ООО «Олбест» [Электронный ресурс]. – режим доступа: https://revolution.allbest.ru/pedagogics/00991768_0.html

2. Кириллова, Т.А. Методика создания и использования электронных образовательных ресурсов (программная среда Moodle): учебное пособие для преподавателей / Т. А. Кириллова. – Петрозаводск: Издательство ПетрГУ, 2015 – 56 с.

О ГЕНЕРАТОРАХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Бахтиярова А.И., Благовисная А.Н.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

Псевдослучайные последовательности являются популярным объектом исследований в математике. Это обусловлено тем, что они находят широкое применение в различных задачах науки и техники. Особое значение имеют псевдослучайные последовательности в таких областях, как криптография и теория кодирования.

Последовательность чисел называется псевдослучайной, если она, будучи вычисленной по некоторым детерминированным алгоритмам, обладает некоторыми свойствами случайной последовательности. Свойства случайности последовательности определяются в зависимости от области задач, в которых необходимо использование псевдослучайных последовательностей.

В публикациях, посвященных псевдослучайным последовательностям, отражаются такие направления исследований, как разработка генераторов псевдослучайных последовательностей, исследование генераторов псевдослучайных последовательностей, разработка методов тестирования генераторов псевдослучайных последовательностей.

Для построения генераторов псевдослучайных последовательностей используются различные математические объекты. Большое количество работ посвящено генераторам последовательностей, основанным на эллиптических кривых.

Эллиптические кривые над конечными полями используются для построения криптосистем, реализации криптографических протоколов. В то же время аппарат теории эллиптических кривых над конечными полями оказывается продуктивным при создании и реализации алгоритмов генерации псевдослучайных чисел.

Эллиптическую кривую E над полем F можно определить как множество пар точек $(x, y) \in F^2$, удовлетворяющих уравнению

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in F. \quad (1)$$

На множестве $E(F)$, состоящем из точек эллиптической кривой и ещё одного элемента – бесконечно удаленной точки кривой O , можно определить операцию, обладающую свойствами операции абелевой группы. Получающуюся группу рассматривают как аддитивную группу, операцию называют операцией сложения и обозначают знаком плюс. Бесконечно

удаленная точка кривой O выполняет роль нейтрального элемента (нуля) группы. Более подробную информацию об эллиптических кривых можно найти, например, в [6].

Эллиптические кривые могут использоваться для получения псевдослучайных последовательностей на основе уже известных генераторов (алгоритмов). К таким генераторам относятся линейный конгруэнтный генератор и его модификации, BBS-генератор, регистр сдвига и другие. Так, в работе [5] рассматриваются линейные рекуррентные последовательности на эллиптических кривых. В статьях [2] и [8] рассматриваются модели построения псевдослучайных последовательностей на основе линейных рекуррент на эллиптической кривой. Следует отметить публикацию [1], в которой описывается алгоритм построения псевдослучайных последовательностей на эллиптических кривых на основе генератора «Вихрь Мерсенна». Исследователями разрабатываются и другие вариации генераторов, в частности с использованием изоморфных трансформаций кривой [3] или нейронных сетей [7].

Приведем пример алгоритма генерации последовательностей на эллиптической кривой на основе конгруэнтного или инверсивного генераторов, предложенный в [4]. Согласно данному алгоритму необходимо:

- выбрать конечное поле $GF(q)$;
- выбрать кривую E ;
- выбрать генератор. Например, линейный конгруэнтный генератор, заданный уравнением $X_{i+1} = cX_i + P$ или инверсивный генератор с уравнением $X_{i+1} = c(X_i)^{-1} + P$;
- выбрать фиксированное целое число c , начальную точку X_0 и фиксированную точку P , причем $cX_0 + P \neq X_0$.
- вычислить последовательность состояний генератора $X_0, X_1, X_2, \dots$, используя формулу $X_{i+1} = cX_i + P$ или формулу $X_{i+1} = c(X_i)^{-1} + P$.

В этой же работе [4] приведен алгоритм формирования псевдослучайной последовательности над эллиптической кривой на основе регистров сдвига с линейными обратными связями.

Продemonстрируем получение последовательности точек эллиптической кривой согласно алгоритмам на основе конгруэнтного и инверсивного генераторов с помощью реализованного авторами учебного программного средства работы с точками эллиптических кривых над конечными полями. Программное средство реализовано в среде VisualStudio на языке программирования C#.

На рисунке 1 приведен пример поиска точек кривой над полем $GF(29)$, заданной уравнением $y = x^3 + 4x + 4$, с помощью конгруэнтного генератора, уравнение которого имеет вид:

$$X_{i+1} = 11X_i + P, \text{ где } P(2,7).$$

В качестве начальной точки выбрана точка $X_0 = (0, 2)$.

Введите эллиптическую кривую:

$y^2 = x^3 + 4x + 4 \mod 29$

Найти точки

Сложение точек: $(11;4) + 2.7$

Умножение(kP): $11 * (23;5)$

Очистить

$X1 = 11X0 + P = 11(0;2) + (2;7) = (2;7) + (2;7) = (5;2)$
 $X2 = 11X1 + P = 11(5;2) + (2;7) = (23;24) + (2;7) = (28;12)$
 $X3 = 11X2 + P = 11(28;12) + (2;7) = (0;2) + (2;7) = (26;20)$
 $X4 = 11X3 + P = 11(26;20) + (2;7) = (1;26) + (2;7) = (10;0)$
 $X5 = 11X4 + P = 11(10;0) + (2;7) = (10;0) + (2;7) = (1;3)$
 $X6 = 11X5 + P = 11(1;3) + (2;7) = (5;27) + (2;7) = (2;22)$
 $X7 = 11X6 + P = 11(2;22) + (2;7) = (13;7) + (2;7) = (14;22)$
 $X8 = 11X7 + P = 11(14;22) + (2;7) = (26;20) + (2;7) = (24;27)$
 $X9 = 11X8 + P = 11(24;27) + (2;7) = (28;12) + (2;7) = (5;27)$
 $X10 = 11X9 + P = 11(5;27) + (2;7) = (23;5) + (2;7) = (24;2)$
 $X11 = 11X9 + P = 11(24;2) + (2;7) = (28;17) + (2;7) = (23;5)$
 $X12 = 11X10 + P = 11(23;5) + (2;7) = (11;4) + (2;7) = (0;2)$

Рисунок 1 – Поиск точек последовательности на основе линейного конгруэнтного генератора

На рисунке 2 приведен пример поиска точек кривой над полем $GF(13)$, заданной уравнением $y = x^3 + 11x + 8$, с помощью инверсивного генератора, уравнение которого имеет вид:

$$X_{i+1} = 9(X_i)^{-1} + P, \text{ где } P(7,5).$$

В качестве начальной точки выбрана точка $X_0 = (2,5)$.

Введите эллиптическую кривую:

$y^2 = x^3 + 11x + 8 \mod 13$

Найти точки

Сложение точек: $(8;7) + 7.5$

Умножение(kP): $9 * (4;8)$

Очистить

$X1 = 9(X0)^{-1} + P = 9(2;5)^{-1} + (7;5) = 9(2;8) + (7;5) = (2;8) + (7;5) = (8;6)$
 $X2 = 9(X1)^{-1} + P = 9(8;6)^{-1} + (7;5) = 9(8;7) + (7;5) = (4;8) + (7;5) = (3;4)$
 $X3 = 9(X2)^{-1} + P = (3;4)^{-1} + (7;5) = 9(3;9) + (7;5) = (12;3) + (7;5) = (3;9)$
 $X4 = 9(X3)^{-1} + P = (3;9)^{-1} + (7;5) = 9(3;4) + (7;5) = (12;10) + (7;5) = (8;7)$
 $X5 = 9(X4)^{-1} + P = (8;7)^{-1} + (7;5) = 9(8;6) + (7;5) = (4;5) + (7;5) = (2;8)$
 $X6 = 9(X5)^{-1} + P = (2;8)^{-1} + (7;5) = 9(2;5) + (7;5) = (2;5) + (7;5) = (4;8)$
 $X7 = 9(X6)^{-1} + P = (4;8)^{-1} + (7;5) = 9(4;5) + (7;5) = (8;6) + (7;5) = (12;3)$
 $X8 = 9(X7)^{-1} + P = (12;3)^{-1} + (7;5) = 9(12;10) + (7;5) = (3;4) + (7;5) = (12;10)$
 $X9 = 9(X8)^{-1} + P = (12;10)^{-1} + (7;5) = 9(12;3) + (7;5) = (3;9) + (7;5) = (4;5)$
 $X10 = 9(X9)^{-1} + P = (4;5)^{-1} + (7;5) = 9(4;8) + (7;5) = (8;7) + (7;5) = (2;5)$

Рисунок 2 – Поиск точек последовательности на основе инверсивного генератора

В заключение отметим, что реализованные алгоритмы построения последовательностей точек эллиптических кривых могут послужить основой для проведения учебно-исследовательских работ. Например, для создания генераторов усложнения получающихся последовательностей с целью прохождения последовательностями тестов, проверяющих свойства случайности, выявления характеристик эллиптических кривых и генераторов, позволяющих получать последовательности, применяемые в криптографических приложениях.

Список литературы

1. Бабенко, М.Г. Генератор псевдослучайных чисел на эллиптической кривой/ М.Г. Бабенко // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 182–187.
2. Бабенко, М.Г. Разработка генератора псевдослучайных чисел на точках эллиптической кривой / М.Г. Бабенко, Н.Н. Вершкова, Н.Н. Кучеров, В.А. Кучуков // Инженерный вестник Дона. – 2012. – № 4–2(23). – С. 68.
3. Бессалов, А.В. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой // А.В. Бессалов, В.Е. Чевардин // Прикладная радиоэлектроника. – 2012. – Т. 11. – № 2. – С. 234–237.
4. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов, И.В. Чугунков. – Москва: НИЯУ МИФИ, 2012. – 400 с.
5. Тараканов, В.Е. Линейные рекуррентные последовательности на эллиптических кривых и их применение в криптографии / В.Е. Тараканов // Труды по дискретной математике. – 2006. – Т. 9. – С. 340–356.
6. Фролов А.Б. Элементарное введение в эллиптическую криптографию. Книга 1. Алгебраические и алгоритмические основы / А.Б. Фролов, С.Б. Гашков. – М.: Едиториал УРСС, 2019. – 376 с.
7. Червяков, Н.И. Реализация ЕС-последовательностей на точках эллиптической кривой с использованием нейронных сетей / Н.И. Червяков, М.Г. Бабенко, А.С. Назаров, И.С. Крисина // Высокопроизводительные параллельные вычисления на кластерных системах. Материалы XIII Всероссийской конференции (Н. Новгород, 14–16 ноября 2013 г.) – Нижний Новгород: Изд-во Нижегородского госуниверситета. – 2013. – С. 274–278.
8. Червяков, Н.И. Линейные рекуррентные последовательности на эллиптической кривой / Н.И. Червяков, М.Г. Бабенко // Научно-технические ведомости СПбГТУ. – 2010. – № 2. – С. 164–166.

ПРИМЕНЕНИЕ УЧЕБНОГО СТЕНДА ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ДЛЯ ФОРМИРОВАНИЯ ПРОФЕССИОНАЛЬНЫХ КОМПЕТЕНЦИЙ БАКАЛАВРА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Бурькова Е.В., канд. пед. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Современные условия экономического и социального развития общества предъявляют высокие требования к специалистам в области информационной безопасности. Возрастает потребность в кадрах нового поколения, способных быстро адаптироваться к изменяющимся условиям информационной безопасности, обладающих высоким уровнем профессиональной компетентности. Основопологающие принципы обеспечения высокого качества подготовки специалистов в области информационной безопасности предполагают продуктивное взаимодействие с работодателями, ориентацию образовательного процесса на синхронизацию с потребностями региона. В качестве перспективных путей повышения эффективности образовательного процесса используется компетентностный подход, который усиливает практикоориентированность образования, подчеркивает важность умения решать профессиональные задачи, определяет формирование компетенций как результата образования[1].

Важным инструментом образовательного процесса являются учебные стенды, которые применяются для освоения многих дисциплин таких, как «Электротехника», «Электроника и схемотехника», «Микропроцессорные системы», «Системы охранно-пожарной сигнализации». Примеры учебных стендов:

- SDK-1.1, разработанный ООО «ЛМТ» (г. Санкт-Петербург),
- LESO 1,2,3,4, разработанный Лабораторией электронного обучения ЛЭСО СибГУТИ (г. Новосибирск),
- КРИСТАЛЛ-1Ц,2М,21М,3Э, разработанные в НПП Техноинжиниринг (г. Чебоксары).

В основе перечисленных стендов использованы микроконтроллеры ADuC812, ADuC842, PIC16, PIC18. Программирование стенда осуществляется через порты USB, RS-232, RS-485. Работа происходит в интегрированных средах проектирования Keil Software (для SDK) LabVIEW (для LESO), MPLAB-IDE (для PIC-контроллеров). Описание и сравнительная характеристика стендов рассмотрена в статье [2].

Отличие современных стендов от ранее применяемых заключается в том, что они должны быть не только демонстрационными, но и исследовательскими, что позволит выполнять задачи моделирования, анализа и синтеза различных процессов, выполнять расчеты и формулировать выводы

по результатам исследований. Однако чаще всего подобные стенды, выпускаемые научно-исследовательскими центрами, институтами, достаточно дорогие, и в случае выхода их из строя требуют ремонта профессионалами-разработчиками. В связи с этим задача разработки собственных стендов для целей сопровождения образовательного процесса является актуальной и своевременной.

На базе кафедры вычислительной техники и защиты информации под руководством заведующего кафедрой был разработан стенд охранно-пожарной сигнализации (далее стенд ОПС), позволяющий изучить основы построения и освоить навыки работы входящих в его состав приборов, ознакомиться с программированием режимов его работы. Стенд охранно-пожарной сигнализации представляет собой модель системы охранно-пожарной сигнализации на основе приборов фирмы Bolid. Реализованы функции взятия под охрану, снятия с охраны, контроля подключенных извещателей и оповещателей, демонстрация срабатывания извещателей, сопровождающееся звуковым сигналом тревоги.

В целях изучения режимов работы охранно-пожарной сигнализации необходимо проводить со студентами тренировочные занятия по программированию пульта, расположенного на учебном стенде. Программирование пульта осуществляется с помощью специальной программы PProg, которая является свободно распространяемой. Программа PProg устанавливается на компьютер, подключаемый к пульту через USB-порт, и работает под управлением операционных систем Windows 7 и Windows 8. Программа предназначена для конфигурирования пульта, который осуществляет централизованное управление совместной работой всех извещателей и оповещателей [3]. Создаваемая в PProg конфигурация определяет функции системы охранно-пожарной сигнализации и логику взаимодействия приборов.

Перечень и описание заданий для одной из практических работ для студентов по освоению программы приведен в таблице.

Таблица

№ этапа	Подготовка к выполнению этапа	Описание действий
1	2	3
1	Согласно индивидуальному заданию построить план помещения, расположить приборы, обосновать их количество	Задать адрес каждому охранному и пожарному извещателю
2	Изучить технические характеристики прибора охранно-пожарного С2000	В главном окне программы PProg добавить прибор приемно-контрольный охранно-пожарный.
3	Определить тип прибора приемно-контрольного охранно-пожарного	Записать конфигурацию в прибор С2000М

Продолжение таблицы

1	2	3
4	В соответствии с разработанным планом разделить защищаемый объект на зоны, дать им названия это и будут разделы	Создать разделы для системы охраной сигнализации. Во вкладке «Разделы» в зоне «Разделы» добавить несколько разделов при помощи кнопки меню и дать им название
5	Определить количество шлейфов и подсоединенных к ним извещателей и оповещателей. Первоначально все шлейфы записать в один список	В зоне «Приборы» раскрыть список шлейфов С2000-КДЛ и согласно исходным данным адресов охранных извещателей интегрированной системы «Орион», задать тип охранного извещателя
6	Разделить шлейфы по закрепленным зонам	В созданные разделы добавить измененные адреса шлейфов. Каждый адрес шлейфов перетаскивать в свой раздел.
7	Провести сохранение выбранной конфигурации для дальнейшей работы	Сохранить конфигурацию в текстовом файле

Экранная форма окна программы PProg приведена на рисунке.

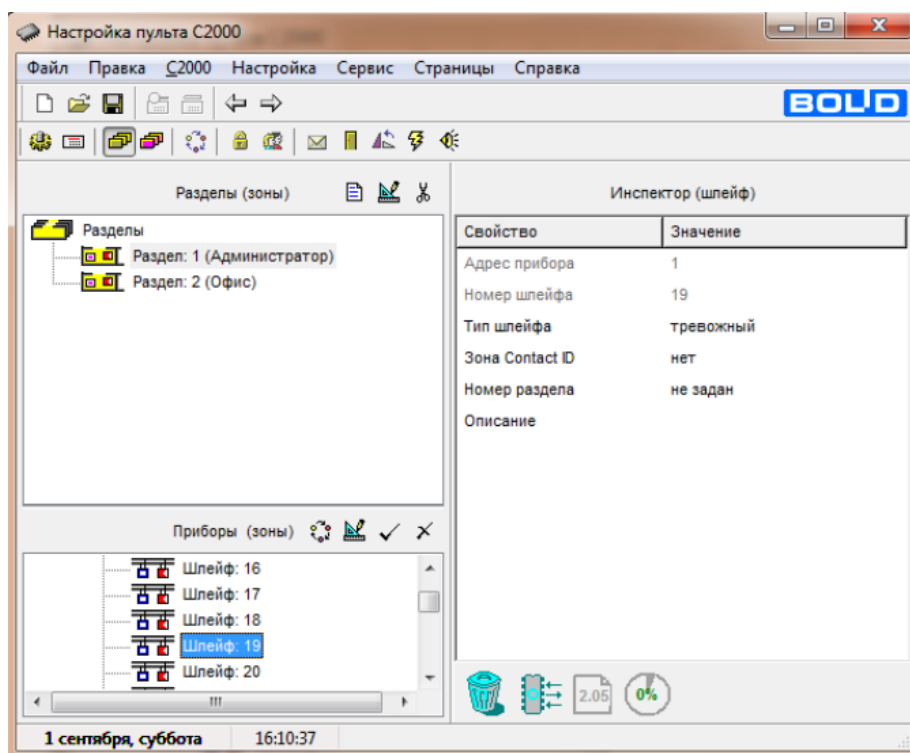


Рисунок - Экранная форма окна программы PProg

Программа позволяет выполнить следующие функции:

- задать защищаемые зоны и назначить разделы;
- выбрать тип охранных и пожарных извещателей;
- выбрать необходимые шлейфы сигнализации;
- настроить привязку приборов к шлейфам и зонам;
- осуществить контроль доступа на основе создания уровней доступа;
- настраивать сценарии управления пожаротушением, доступом, реле или постановкой на охрану и снятием с охраны.

Интерес представляет также возможность, предоставляемая программой, осуществления назначения уровня доступа в различные зоны. Предварительная работа студентов в этом направлении позволит получить навыки распределения зон защищаемого объекта по условиям доступа в соответствии с важностью размещенных в них информационных и иных ресурсов. Знание принципов разделения защищаемого объекта на контролируемые зоны напрямую связано с задачей категорирования объектов защиты и информации [4].

Учебный стенд позволяет не только ознакомиться с работой пульта и всех подключенных к нему приборов, но создать новую конфигурацию системы охранно-пожарной сигнализации с помощью перепрограммирования стенда.

Программирование конфигурации и режимов работы приборов помощью программы PProg позволяет студентам освоить навыки работы с реальными приборами охранно-пожарной сигнализации, размещенными на стенде охранно-пожарной сигнализации, сформировать профессиональные

компетенции в соответствии с требованиями образовательного стандарта по направлению подготовки 10.03.01 Информационная безопасность.

В целях дальнейшего развития применения данного стенда в образовательном процессе ведется работа по расширению возможностей учебного стенда в направлении организации беспроводного управления работой приборов охранно-пожарной сигнализации, контроля их состояния и передачи тревожных сообщений на мобильные устройства.

Список литературы

1. Бурькова, Е.В. Профессиональная подготовка специалистов в области информационной безопасности / Е.В. Бурькова // Вестник Оренбургского государственного университета. – 2016. – № 2. – С. 3- 9.
2. Кадыров, Р.Р. Характеристика учебно-исследовательских стендов по курсам «Схемотехника» и «Микропроцессорные системы» / Р.Р. Кадыров, Е.В. Бурькова // Современные информационные технологии в науке, образовании и практике: материалы XI Всерос. науч.-практ. конф. - Оренбург:-ОГУ, 2014. - С. 125-128.
3. Bolid. Системы безопасности. Режим доступа: <https://bolid.ru/support/>
4. Бурькова, Е.В. Категорирование объектов информатизации для выбора средств физической защиты / Бурькова Е. В. // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всерос. науч.-практ. конф., Оренбург: ОГУ, 2017. - С. 3073-3076.

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ МОДЕРНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ДОКУМЕНТООБОРОТА ПРЕДПРИЯТИЯ

**Бурькова Е.В., канд. пед наук, доцент, Иванова И.В.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Высокий уровень информатизации является характерной чертой современного предприятия. Сбор, хранение и обработка информации осуществляется в автоматизированных системах, при этом основная часть документов содержит либо коммерческую, либо служебную тайну, а также персональные данные сотрудников и клиентов. Данная информация представляет собой информацию ограниченного доступа, а значит, является конфиденциальной, и подлежит защите от несанкционированного доступа, утраты и утечки [2]. Особенностью конфиденциального документа является то, что он представляет собой одновременно не только саму информацию – обязательный объект защиты, но и массовый носитель информации, основной источник накопления и распространения этой информации, в том числе и утечки. То есть конфиденциальна, прежде всего, информация, а уже затем становятся конфиденциальными и документы, в которых эта информация зафиксирована.

Условия, при которых информация может быть отнесена к конфиденциальной, перечислены в ст. 139 части 1 Гражданского кодекса Российской Федерации. К ним относятся:

- действительная или потенциальная коммерческая ценность информации в силу ее неизвестности третьим лицам;
- отсутствие свободного доступа к этой информации на законном основании;
- принятие обладателем информации необходимых мер к охране ее конфиденциальности.

Любые нарушения защищаемых свойств информации могут привести к значительному ущербу для предприятия, а также для частных лиц. В связи с этим задача обеспечения защиты документооборота предприятия является актуальной.

В качестве объекта исследования рассматривается организация Управление Росреестра по Оренбургской области. В информационных системах данного объекта циркулирует конфиденциальная информация разного рода, требующая защиты от угроз. При построении модели угроз безопасности были выявлены актуальные угрозы: угроза подмены системного программного обеспечения, угроза копирования защищаемой информации, угроза несанкционированной модификации, угроза перехвата сетевого трафика, угроза утраты (потери) носителей данных, угроза перехвата одноразовых паролей в режиме реального времени. Было определено, что

информационная система имеет третий уровень защищенности и в соответствии с требованиями нормативных документов ФСТЭК система защиты должна состоять из десяти подсистем.

Создание концептуальной модели процесса защиты документооборота позволит определить цель и результат, а также последовательность проведения работ [3].

Нами была разработана концептуальная модель модернизации системы защиты документооборота данного предприятия, представленная на рисунке.

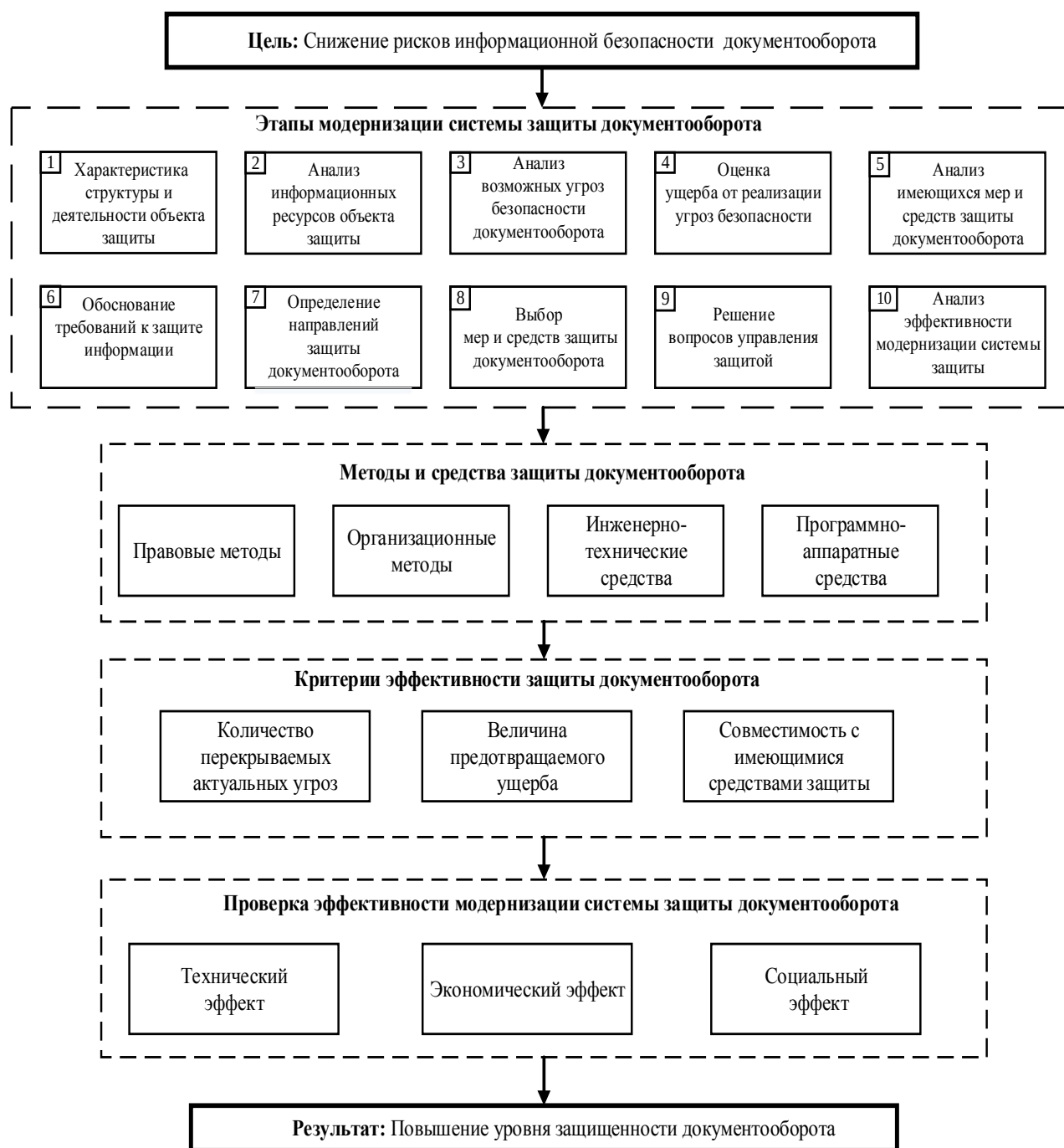


Рисунок - Концептуальная модель модернизации системы защиты документооборота

Концептуальная модель модернизации документооборота представляет собой совокупность следующих элементов:

- цель модернизации системы защиты документооборота;
- этапы модернизации системы защиты документооборота;
- методы и средства защиты документооборота;
- критерии эффективности системы защиты документооборота;
- проверка эффективности модернизации системы защиты документооборота;
- результат модернизации системы защиты.

Целью модернизации является снижение рисков информационной безопасности документооборота. Для достижения цели необходимо разбить весь процесс модернизации на этапы.

Первоначальной задачей является анализ защищаемого объекта, в ходе которого необходимо провести:

- анализ структуры и деятельности защищаемого объекта;
- определение перечня защищаемых информационных ресурсов;
- анализ угроз безопасности для конфиденциального документооборота;
- оценка возможного ущерба от реализации угроз;
- анализ существующих мер и средств защиты.

На первом и втором этапах проводится исследование структуры и деятельности объекта защиты, анализ защищаемых информационных ресурсов и информационных потоков. Оценка обстановки является важным этапом, который определяет уровень обеспечения безопасности информации на объекте. Она основывается на результатах комплексного обследования объекта, в ходе которого, проводится определение защищаемой информации и категория её важности. На этом этапе выясняется:

- функционально-отраслевая принадлежность объекта;
- категория защищаемой информации (виды тайн);
- состав, содержание и местонахождение защищаемых ресурсов.

В результате обследования определяется категория объекта по следующим признакам: уровню важности, уровню секретности, численности персонала, стоимости материальных активов [1].

На третьем этапе проводится анализ возможных угроз безопасности документооборота и строится модель угроз и нарушителя, для это необходимо осуществить:

- оценку возможности несанкционированного доступа к конфиденциальному документообороту;
- выявление возможных технических каналов утечки информации;
- анализ возможностей программно-математического воздействия на информацию.

Четвертый этап предусматривает оценку возможного ущерба от реализации угроз. На данном этапе проводится оценка непосредственного

ущерба от реализации угроз и оценка опосредованного ущерба от реализации угроз.

В результате определяется вид и величина вероятного ущерба от нарушений защищаемых свойств информации.

На пятом этапе проводится анализ имеющихся на объекте мер и средств защиты документооборота:

- от физического доступа;
- от утечки по техническим каналам информации;
- от несанкционированного доступа;
- от программно-математических воздействий;
- от электромагнитных воздействий.

Далее, на шестом этапе проводится обоснование требований по защите информации в соответствии с нормативными документами уполномоченных федеральных органов исполнительной власти.

На седьмом этапе необходимо выбрать направления модернизации – определить, какие именно методы защиты информации будут использоваться для устранения существующих недостатков системы.

После того, как были определены направления модернизации, на восьмом этапе необходимо выбрать конкретные меры и средства обеспечения защиты документооборота. Выбор мер и средств осуществляется в соответствии с требованиями и выполняемыми функциями.

Девятый этап модернизации подразумевает решение вопросов управления защитой. Вопросы управления защитой решаются в плане реализации определенного метода доступа к информации, разработка соответствующих распорядительных документов, в которых содержатся перечни сотрудников и их права доступа к защищаемым ресурсам.

Заключительный десятый этап предусматривает анализ эффективности модернизации системы защиты документооборота, необходимо провести оценку эффективности модернизированной системы.

Методы и средства защиты документооборота подразделяются на правовые методы, которые осуществляют защиту информации на основе законодательной базы, организационные методы информации включают меры, мероприятия и действия, которые должны осуществлять должностные лица для обеспечения заданного уровня безопасности информации и инженерно-технические средства - устройства, инженерные сооружения, затрудняющие или исключаяющие проникновения злоумышленников к носителям конфиденциальной информации. Программно-аппаратные средства защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав автоматизированной системы объекта.

В качестве критериев эффективности защиты документооборота выступают:

- количество перекрываемых угроз, то есть, сколько угроз безопасности перекрыли выбранные меры и средства;

- величина предотвращенного ущерба;
- совместимость с имеющимися средствами защиты.

Данные критерии взаимосвязаны друг с другом и могут быть оценены количественными и качественными показателями.

Для проверки эффективности модернизации системы защиты документооборота оценивают технический эффект. Для этого необходимо вычислить риски информационной безопасности до и после модернизации системы защиты. При оценке экономического эффекта используют показатели стоимости защищаемой информации и показатели стоимости внедренных средств защиты. Стоимость средств не должна превышать величины возможного ущерба защищаемой информации. Социальный эффект понимается как совокупность социальных результатов, получаемых от реализации проекта и имеющий как положительные, так и отрицательные значения, и как последствия определенных социокультурных изменений, массовых мероприятий, и как инструмент создания благоприятных условий для всестороннего развития личности, применения гражданами своих творческих сил и способностей, который находит свое выражение в сокращении тяжелого физического труда, увеличении свободного времени, повышении материального и культурного уровня жизни народа, в охране здоровья.

Разработка концептуальной модели модернизации системы защиты документооборота позволит спланировать процесс проектирования системы защиты, разработать перечень требований для обеспечения заданного уровня безопасности, осуществить обоснование и выбор методов и средств защиты, оценить эффективность модернизации.

Список литературы

1 Бурькова, Е.В. Категорирование объектов информатизации для выбора средств физической защиты / Е.В. Бурькова // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всерос. науч.-практ. конф., - Оренбург: ОГУ, 2017. - С. 3073-3076.

2 Бурькова, Е. В. Задача оценки защищенности информационных систем персональных данных / Е.В. Бурькова // Вестник Чувашского университета, 2016. - № 1. - С. 112-118.

3 Модели информационной безопасности. Режим доступа: <http://security-corp.org/companies/google/43483-modeli-informacionnoy-bezopasnosti.html>

МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

**Бурькова Е.В., канд. пед. наук, доцент, Кулик М.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Проблема обеспечения информационной безопасности при передаче информации по каналам связи обусловлена возрастанием количества, качества и возникновением новых угроз. Основные угрозы направлены на нарушение таких свойств информации, как конфиденциальность, целостность и доступность, и реализация данных угроз приводит к значительному ущербу для обладателя информации. В настоящее время широкое распространение получили беспроводные сети передачи информации, которые отличаются от проводных рядом показателей, среди них важным является надежность передачи. Несмотря на множество преимуществ, для беспроводных сетей характерны такие недостатки как чувствительность к помехам, недостаточная безопасность, зависимость от расстояния точки доступа, высокий уровень расхода энергии устройств, возникновение сбоев, ошибок при передаче. В связи с этим задача анализа методов повышения надежности передачи информации по беспроводным сетям является актуальной и своевременной.

Надежность сети телекоммуникации - это способность обеспечивать передачу информации с сохранением значений установленных показателей качества, отражает влияние на работоспособность сети отказов любого типа, вызываемых процессами старения аппаратуры, дефектами технологии, непрофессионализмом персонала, вмешательством нарушителя.

К основным показателям надежности передачи информации относятся среднее время наработки на отказ, коэффициент готовности (отказоустойчивость), среднее время восстановления работоспособности [1]. Согласно приказу Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113 к показателям надежности функционирования сетей передачи данных относятся:

- средняя задержка передачи пакетов информации,
- отклонение от среднего значения задержки передачи пакетов информации,
- коэффициент потери пакетов информации,
- коэффициент ошибок в пакетах информации.

Если для проводных каналов связи вопрос надежности передачи данных является решенным, то для беспроводных каналов связи, ввиду большого их разнообразия, остается актуальным: применяемые методы отличаются друг от друга по уровню эффективности и применимости для определенных видов сетей. Кроме того, на надежность передачи информации влияет скорость передачи – чем выше скорость, тем выше вероятность потерь, что

подтверждено в исследованиях [3]. В статье проведена оценка влияния скорости передачи на вероятность пакетных ошибок. График зависимости показан на рисунке 1.

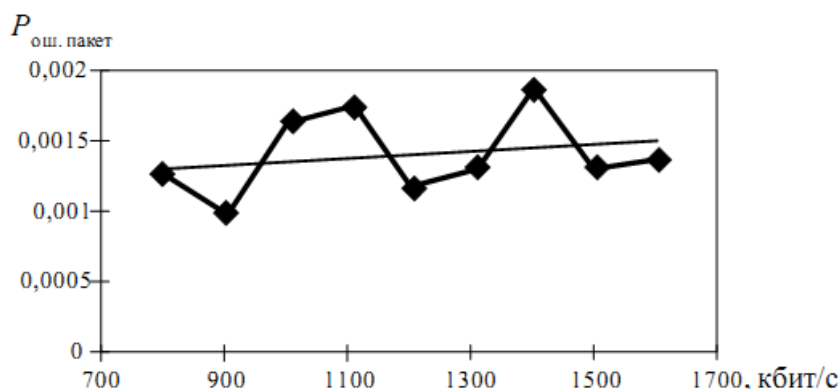


Рисунок 1— График зависимости вероятности пакетных ошибок от скорости передачи

График показывает небольшую корреляцию между вероятностью ошибки пакета и скоростью передачи. Кроме этого были зафиксированы следующие факты: вероятность ошибки пакета удваивается при каждом увеличении размера пакета на 300 байт. В таблице 1 отражена статистика эксперимента.

Таблица 1 – Результаты статистических данных

Расстояние, м	вероятность пакетной ошибки		длина ошибки		длина без ошибки	
	среднее	дисперсия	среднее	дисперсия	среднее	дисперсия
10	0,000634	0,000229	1,000	0,000	1749,59	732,72
40	0,001955	0,000725	1,848	0,227	1023,43	334,40
70	0,003271	0,001086	2,005	0,210	574,56	148,45
90	0,021822	0,010412	2,428	0,018	122,89	58,99
110	0,032171	0,014786	2,540	0,482	87,26	39,75
130	0,080431	0,037123	2,298	0,290	28,90	8,82
усреднение	0,24735	0,031554	2,054	0,564	549,37	699,39
мобильный пользователь	0,032711	0,019324	2,365	0,089	84,60	37,36

Вероятность ошибки пакетов для мобильного пользователя (со скоростью 1.5 м/сек) примерно на 30% выше средней, предположительно из-за мобильности. Средняя длина ошибки составляет от двух до трех пакетов для большинства анализируемых расстояний.

Нами были проанализированы методы повышения надежности передачи информации, классификация методов представлена на рисунке 2.

С помощью метода разбиения пакетов проводится разделение информации на отдельные блоки, после чего для каждого блока вычисляется контрольная сумма, которая передается после блока информационных данных.

Вычисление контрольной суммы обеспечивает обнаружение одиночных пакетов ошибок.

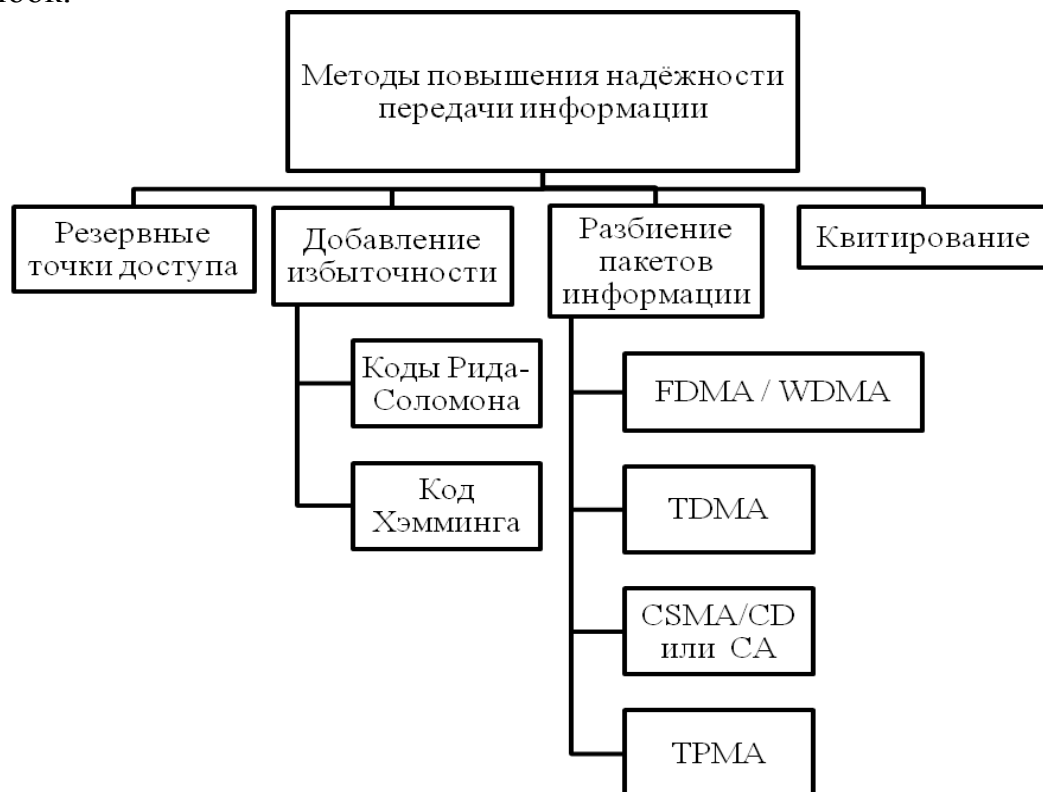


Рисунок2 - Классификация методов повышения надежности передачи информации по сетям

С целью повышения надежности сети и отдельных ее устройств, применяется резервирование. Различают общее и отдельное резервирование. Общим называется такое резервирование, при котором заменяется все отказавшие беспроводные станции. При общем резервировании надежность системы определяется формулой: $P_{общ} = 1 - (1 - \prod_{i=1}^n p_i)^m$. При отдельном

резервировании: $P_{разд.} = \prod_{i=1}^n [1 - (1 - p_i)^m]$, где P – вероятность безотказной работы элементов сети.

К методу разбиения пакетов информации относят алгоритмы, действующие как в проводных, так и беспроводных сетях – **FDMA, TDMA, TPMA, CSMA/CD или CA:**

- множественный доступ с прослушиванием несущей и разрешением коллизий (CSMA)
- множественный доступ с передачей полномочия (TPMA) или метод с передачей маркера;
- множественный доступ с разделением во времени (TDMA);
- множественный доступ с разделением частоты (FDMA) или множественный доступ с разделением длины волны (WDMA).

Многократный доступ с поддержкой несущей или CSMA - это протокол управления доступом к среде передачи (MAC), который используется для управления потоком данных на носителе передачи, так что пакеты не теряются и целостность данных сохраняется. В CSMA есть две модификации: CDMA CSMA (обнаружение столкновений) и CSMA CA (предотвращение столкновений). FDMA основан на разделении полосы пропускания канала на группу полос частот, образующих логические каналы. Метод с передачей маркера (TRMA) – это метод доступа к среде, в котором от одной рабочей станции к другой передается маркер, который выдает разрешение на передачу данных. При получении маркера рабочая станция может передавать сообщение, присоединяя его к маркеру, который переносит это сообщение по сети. TDMA основан на использовании тактового генератора [3].

Метод добавления избыточности предполагает введение кодирования пакетов информации. Для уменьшения попыток повторной передачи информации применяется прямое исправление ошибок путем использования способов помехоустойчивого кодирования: коды Рида-Соломона, код Хэмминга, модулярные корректирующие коды. Использование метода исправления ошибок на основе модулярных корректирующих кодов приводит к снижению информационной скорости передачи данных. Несмотря на это, оно оправдано при наличии помех, так как снижает количество повторных передач пакетов и, таким образом, снижает общее время, требуемое для достоверной передачи данных. Один из вариантов помехоустойчивой передачи используется в современных системах цифрового телевидения, в котором реализованы наиболее совершенные коды Рида-Соломона, требующие добавления двух проверочных символов в расчете на одну исправляемую ошибку [2].

Метод квитирования использует учет подтверждения получаемой информации по сегментам. В протоколе TCP реализована разновидность алгоритма квитирования с использованием сегментов.

Анализ методов повышения надежности передачи данных приведен в таблице 2.

Таблица 1- Анализ методов повышения надежности передачи данных

Методы	Достоинства	Недостатки
1	2	3
Методы добавления избыточности (помехоустойчивое кодирование)	Позволяет не только обнаруживать, но и исправлять ошибки. Возможность восстановления информации, исправления ошибок при передаче.	Сложность алгоритмов кодирования- декодирования, аппаратные ограничения устройств с автономным питанием, а также использование нелицензионного диапазона частот, что повышает вероятность искажения

		информационных символов.
FDMA/ WDMA	Информация передается в "реальном времени"	Недостаточная эффективность использования полосы частот, сниженная общая пропускная способность канала связи.
TDMA	Применяется в стандартах второго поколения сотовой связи (GSM), широкополосность и небольшое время передачи	Сниженная общая пропускная способность имеющегося канала связи, каждый пользователь имеет предварительно заданный тайм-слот, многоканальное искажение
CDMA	Применение в 2G и 3G	Высокая сложность и стоимость приемо-передающих устройств.
CSMA/CD или CA	Необходимы только в работе с концентраторами. Передача данных предваряется посылкой сигнала блокировки с целью захвата передающей среды в монопольное пользование.	Задержка передачи, если канал занят. При этом кадр, ожидающий освобождения канала, находится в буфере сетевого адаптера
Квитирование	Обеспечение надежной передачи данных, гарантирует доставку данных абоненту без потерь и искажения. Эффективная загрузка сетевого оборудования за счет реализации механизма скользящего окна и перераспределения потоков данных в процессе адаптивной маршрутизации	Увеличение количества пакетов в сети ведёт к снижению производительности и даже к прекращению передачи пакетов, то есть к остановке сети, что, в частности, связано с возникающими в сети блокировками.
Резервные точки доступа	Высокий уровень показателей надежности передачи данных	Затраты на избыточное оборудование сети. Потери времени на восстановления сети после отказа.

Для дальнейшего исследования был выбран метод резервирования с установкой резервных точек доступа к сети. Предполагается разработка программного средства, с использованием сервиса Яндекс Карты, на картах которого будут размещаться точки доступа к беспроводным сетям. Данные точки будут проанализированы по таким характеристикам, как мощность, охват, тип сети. В результате анализа программа генерирует графовую вероятностную модель. Данная модель учитывает показатели точек доступа, вероятность надежной передачи данных и с помощью метода кластеризации, выявит целесообразное расположение резервных каналов передачи информации, отобразив их на экране.

Список литературы

1. Бурькова, Е.В. Надежность систем физической защиты объекта информатизации / Бурькова Е. В. // Университетский комплекс как региональный центр образования, науки и культуры : материалы Всерос. науч.-метод. конф. - Оренбург : ОГУ, - 2019.- С. 1843-1847
2. Цаволык, Т.Г. Метод исправления ошибок на основе модулярных корректирующих кодов / Т.Г. Цаволык, В.В. Яцкив // Вестник Брестского государственного технического университета. Физика, математика, информатика. - 2015. - № 5 (95). - С. 36-38.
3. Асотов, Д.В. Повышение надежности передачи данных в беспроводных сетях с использованием децентрализованного режима функционирования / Д.В. Асотов, В.И. Маслов, Л.Ш. Голоскокова // Вестник Воронежского государственного технического университета - 2015. - № 3. Т. 11.- С. 126-129.

ОПЫТ ВНЕДРЕНИЯ В УЧЕБНЫЙ ПРОЦЕСС ПРЕПОДАВАНИЯ ДИСЦИПЛИН ГЕОМЕТРО-ГРАФИЧЕСКОГО ЦИКЛА ЭЛЕКТРОННЫХ КУРСОВ В СИСТЕМЕ ОБУЧЕНИЯ MOODLE

**Ваншина Е.А., канд. пед. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

В связи с переходом на новые федеральные государственные образовательные стандарты высшего образования в условиях сокращения учебных часов по таким базовым для инженерного образования геометро-графическим дисциплинам как начертательная геометрия, черчение, инженерная и компьютерная графика, преподаваемым обучающимся технических направлений подготовки всех форм обучения на первом и(или) втором курсе в первом и(или) втором семестрах [1], возникла необходимость разработки и внедрения в образовательный процесс современных информационных технологий – электронных курсов в системе обучения Moodle (<http://moodle.osu.ru>), что в переводе с английского языка "Modular Object-Oriented Dynamic Learning Environment" означает модульная объектно-ориентированная динамическая среда обучения – система управления обучением (LMS), распространяющаяся по лицензии GNU GPL[2, 3, 4], для повышения эффективности учебного процесса, объективной оценки усвоения обучающимися теоретических основ дисциплин, учебно-методического сопровождения аудиторных занятий, контроля внеаудиторной самостоятельной работы обучающихся, что является целесообразным дополнением к другим методам проверки знаний обучающихся, в том числе широко используемой в Оренбургском государственном университете Автоматизированной интерактивной системы сетевого тестирования АИССТ (<http://aist.osu.ru>) [5].

Целью разработанных нами электронных курсов в системе обучения Moodle, на примере курса «Инженерная и компьютерная графика (Начертательная геометрия и Инженерная графика и Компьютерная графика)», является приобретение обучающимися знаний теоретических основ дисциплин геометро-графического цикла, овладение обучающимися практических умений и навыков подготовки и оформления конструкторско-технологической документации, в том числе автоматизированным методом; формирование профессиональных компетенций у студентов-бакалавров 1, 2 курса всех форм обучения в 1, 2 учебных семестрах, что соответствует образовательным стандартам и программам дисциплины "Инженерная и компьютерная графика".

Целями освоения дисциплины являются приобретение обучающимися знаний теоретических основ построения проекционного чертежа как графической модели пространственных фигур, а также последующее

применение обучающимися полученных навыков в практике выполнения технических чертежей и схем с использованием компьютерной техники.

К задачам дисциплины относятся: приобретение обучающимися знаний в области теоретических основ инженерной и компьютерной графики как теоретической базы для изучения последующих дисциплин профессионального цикла; приобретение обучающимися навыков реализации теоретических знаний на практике в рамках выполнения практических заданий, лабораторных и курсовых работ, курсовых проектов с применением интерактивных методов и закреплении соответствующих компетенций.

Электронный учебный курс предназначен для учебно-методического сопровождения практических занятий, лабораторных и курсовых работ, курсовых проектов по дисциплине "Инженерная и компьютерная графика", а также эффективного контроля внеаудиторной самостоятельной работы обучающихся.

Предметный материал курса актуален, соответствует научно-техническому уровню в рассматриваемой предметной области, четко структурирован, содержит учебные материалы и ресурсы для обеспечения успешного прохождения тем дисциплины, авторские учебно-методические материалы в виде печатных изданий и интернет-ресурсов, рабочую программу дисциплины.

Учебный материал курса разделен на девять тем (первые две темы относятся к начертательной геометрии; третья, четвертая и пятая – к инженерной графике; шестая, седьмая, восьмая (состоит из двух подтем) – к компьютерной графике) для практических занятий, лабораторных и курсовых работ, курсовых проектов, а также материал для самостоятельной работы, что соответствует восьми разделам рабочей программы дисциплины.

По каждой теме курса разработаны контрольно-измерительные материалы (тесты) для текущего контроля знаний и умений студентов с фиксацией и сохранением результатов прохождения курса в журнале оценок и подведением итогов обучения студентов на курсе (итоговое тестирование). В темах курса также используются формы активного взаимодействия всех его участников (чат). Курс рассчитан на 16 часов практических занятий (лабораторных работ) и 73 часа самостоятельной работы.

Некоторые основные оконные формы электронного курса «Инженерная и компьютерная графика (Начертательная геометрия и Инженерная графика и Компьютерная графика)» представлены на рисунках 1-4.

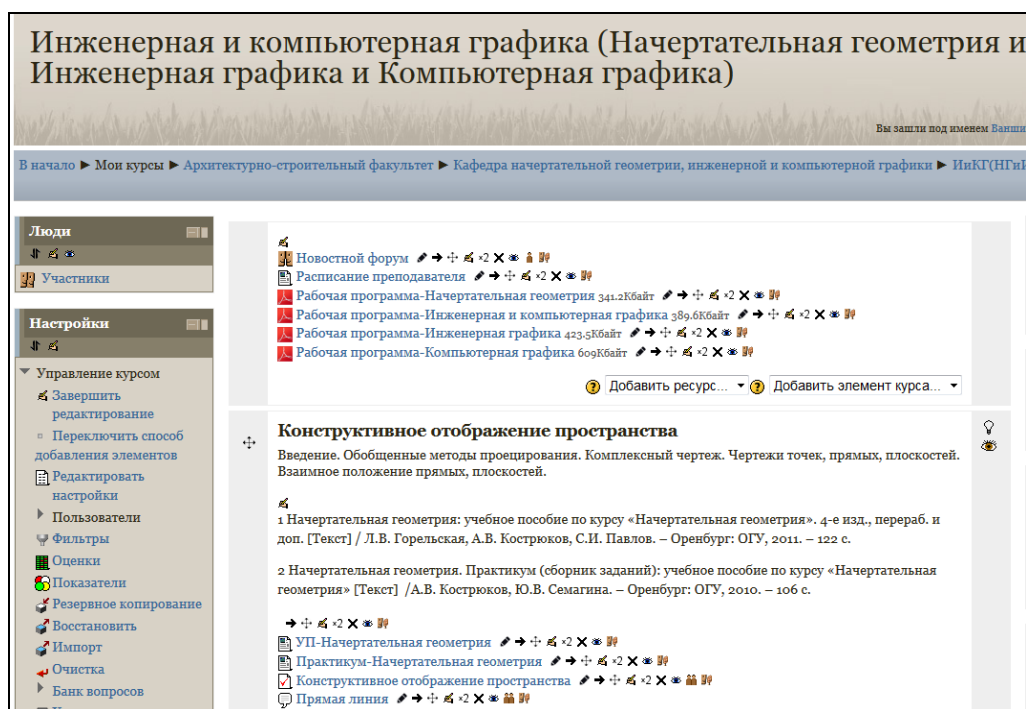


Рисунок 1 – Главное окно курса

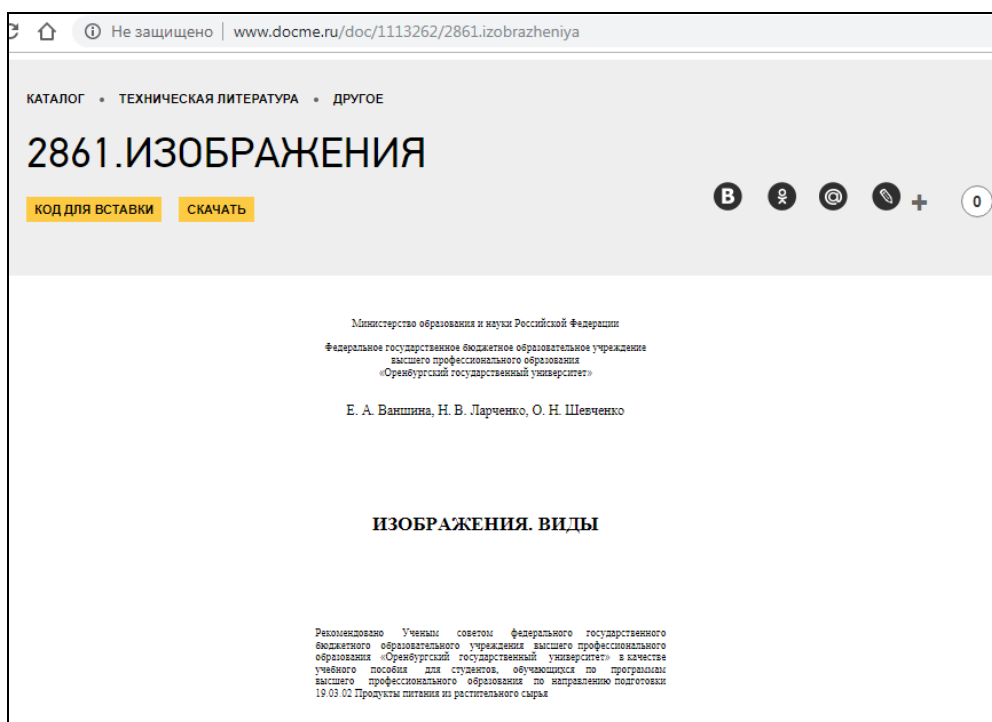


Рисунок 2 – Окно «Гиперссылка»

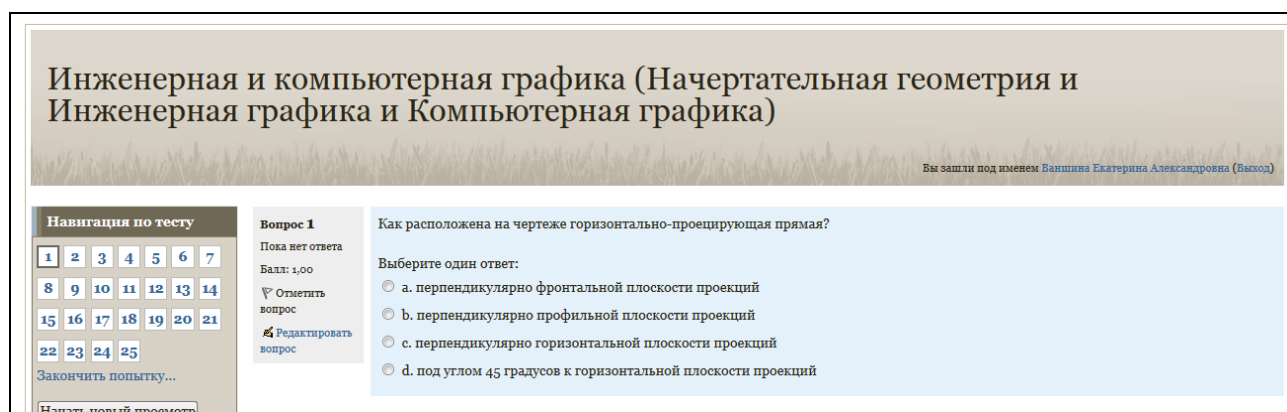


Рисунок 3 – Окно «Тест»

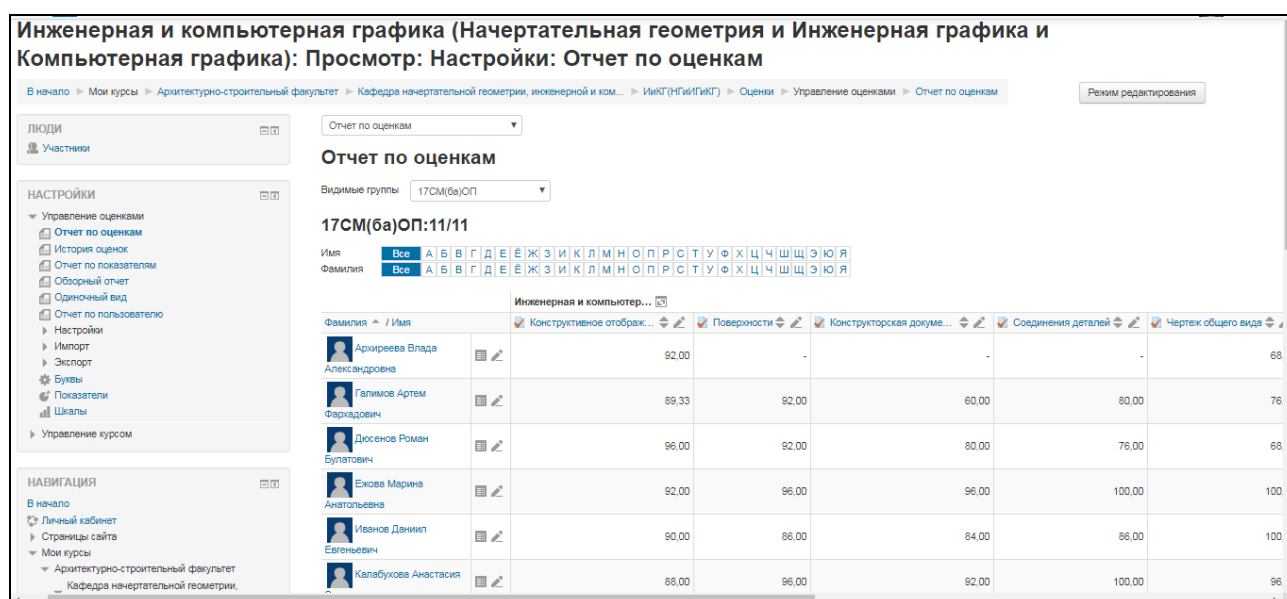


Рисунок 4 – Окно «Отчет по оценкам»

Разработка и внедрение в образовательный процесс электронных курсов "Инженерная и компьютерная графика (Начертательная геометрия и Инженерная графика и Компьютерная графика)", "Инженерная графика (Начертательная геометрия и Инженерная графика)", "Черчение" в системе электронного обучения Moodle позволяет объективно оценить уровень усвоения теоретических знаний обучающихся технических направлений подготовки всех форм обучения по дисциплинам геометро-графического цикла, при проведении компьютерного тестирования, повысить качество подготовки обучающихся за счет внедрения новых, современных форм, технологий и средств обучения, включая электронный образовательный контент и сеть Интернет, повысить качество программно-информационного обеспечения образовательных программ высшего образования, что рационально дополняет другие действующие методы проверки знаний обучающихся.

Список литературы

1. Ваншина, Е. А. Проблемы компьютеризации преподавания графических дисциплин / Е. А. Ваншина // Вестник Оренбургского государственного университета. – 2009. – №2. – С.143. – ISSN 1814-6457.
2. Ваншина, Е. А. Инженерная и компьютерная графика (Начертательная геометрия и Инженерная графика и Компьютерная графика) [Электронный ресурс]: электронный курс в системе Moodle / Е. А. Ваншина. – Оренбург: ОГУ, 2018. – 8 с., режим доступа: <http://moodle.osu.ru>
3. Ваншина, Е. А. Инженерная графика (Начертательная геометрия и Инженерная графика) [Электронный ресурс]: электронный курс в системе Moodle / Е. А. Ваншина. – Оренбург: ОГУ, 2019. – 8 с., режим доступа: <http://moodle.osu.ru>
4. Ваншина, Е. А. Черчение [Электронный ресурс]: электронный курс в системе Moodle / О. Н. Шевченко, Е. А. Ваншина. – Оренбург: ОГУ, 2019. – 8 с., режим доступа: <http://moodle.osu.ru>
5. Автоматизированная интерактивная система сетевого тестирования- АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа: <http://aist.osu.ru>.

МЕТОДИКА ИЗУЧЕНИЯ IP-КАМЕР В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КАФЕДРЫ ВУЗА

**Галимов Р.Р., канд.техн. наук, доцент, Алиев Р.М.
Федеральное государственное бюджетное учреждение
высшего образования «Оренбургский государственный
университет»**

Системы видеонаблюдения (СВН) являются одними из важнейших элементов комплексных систем защиты информации современных предприятий. Традиционные решения в данной области позволяют выполнять следующие функции:

- достоверно проводить расследования инцидентов информационной безопасности благодаря высокой информативности;
- верифицировать события от извещателей системы физической защиты для дистанционного выявления ложных срабатываний;
- оперативно реагировать на инциденты, связанные с нарушением контролируемых зон и различными нештатными ситуациями [1,2].

Кроме того, необходимо отметить профилактический характер применения систем видеонаблюдения для предотвращения нарушений.

Последними тенденциями в данной области являются использование IP-камер и применение средств видеоаналитики. Популярность IP-камер обусловлена тем, что их можно рассматривать просто как удаленные источники цифровой информации и применять стандартные методы обработки и хранения. Видеоаналитика позволяет автоматизировать процесс распознавания внештатных ситуаций без участия оператора. Данное обстоятельство актуально в контексте значительного увеличения количества камер наблюдения, когда оператор не может контролировать их с высоким качеством[3]. В связи с появлением новых методов и средства построения и эксплуатации СВН возникает необходимость в развитии навыков у студентов в данной области. Следует отметить, что наряду с большим количеством публикаций по данной тематике[4], вопросы разработки прикладных методик, учитывающих специфику конкретных условий изучения, доступных инструментальных средств лабораторного типа в литературе освещены недостаточно.

Целью данной работы является повышение эффективности изучения IP-камер как средств защиты объектов информатизации в условиях кафедры вычислительной техники и защиты информации Оренбургского государственного университета.

Для достижения поставленной цели решены следующие задачи:

- методика дистанционного мониторинга контролируемой зоны на основе IP-камер;

- методика обнаружения объектов на видеоданных IP-камер на основе глубокой нейронной сети Yolo.

Первая методика основана на дистанционном мониторинге контролируемой зоны при помощи IP-камеры. Структурная схема системы мониторинга контролируемой зоны кафедры ВУЗа на основе IP-камеры изображена на рисунке 1.

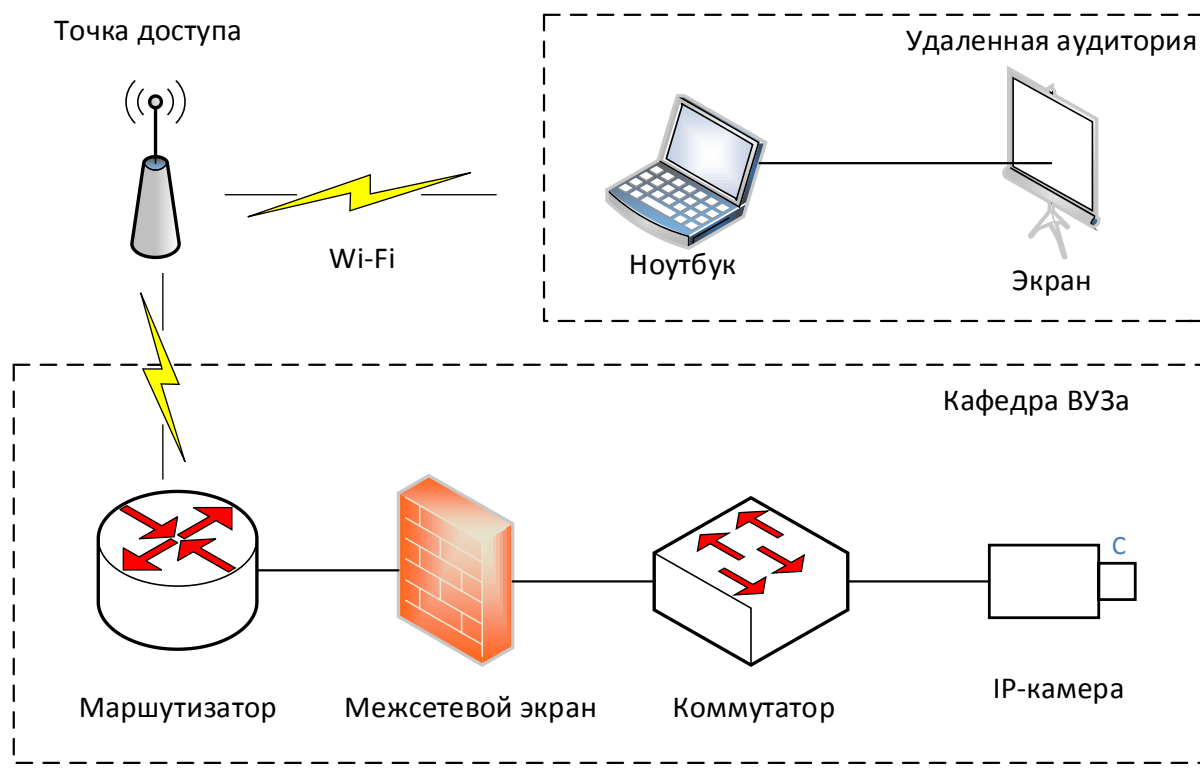


Рисунок 1 – Система мониторинга контролируемой зоны кафедры ВУЗа на основе IP-камеры

Данная система позволяет транслировать видеосигнал с IP-камеры из специализированной лаборатории кафедры в одну из удаленных лекционных аудиторий, находящаяся в другом корпусе университета. Передача видеоданных осуществляется по протоколу RTSP или HTTP на компьютер, размещенный в удаленной аудитории через ЛВС университета. Для успешного подключения необходимо добавить данное соединение в список разрешенный устройств на межсетевом экране.

Для реализации связи использованы следующие технические средства:

- 1 Ноутбук с Wi-Fi адаптером с предустановленной ОС Windows 10.
- 2 IP-видеокамера DH-HFW5431EP-Z.

Используемое программное обеспечение включает в себя:

- 1 VLC media player – программа для подключения к IP-камере по протоколу RTSP.

- 2 Плагин к браузеру Internet Explorer, предоставляемый производителем камеры.

Для подключения к IP-камере по протоколу RTSP в программе VLCmediaplayer необходимо выбрать подключение по URL и ввести сетевой адрес в формате: `rtsp://[<имя_пользователя>:<пароль>@]:<порт>/<путь_к_потoku>`.

На рисунке 2 представлены настройки для подключения к IP-камере по протоколу RTSP в лекционную аудиторию в режиме реального времени. Посредством плагина браузера удаленно изменяются следующие основные параметры IP-камеры в рамках данной методики:

- параметры видеоадреса. Задаются параметры качества трансляции и разрешения кадра;
- настройка обнаружения в контролируемой зоне. При обнаружении движения в заданной области осуществляется запись видеоданных на диск компьютера.

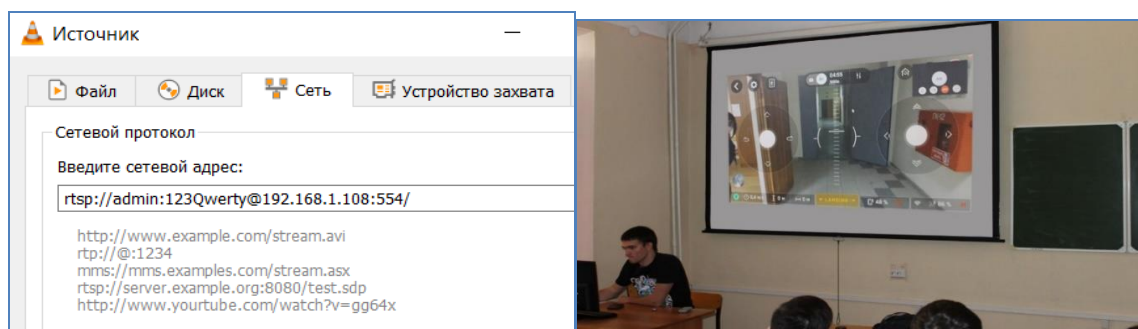


Рисунок 2 – Удаленная видеотрансляция контролируемой зоны с IP-камеры

В рамках второй методики осуществляется трансляция видеоданных с IP-камеры на удаленный компьютер для последующей обработки, в частности детектирования определенных классов объектов. На сегодняшний день для детектирования объектов на изображениях активно используют глубокие нейронные сети (ГНС), которые показывают более высокие оценки достоверности в сравнении с традиционными подходами. Основным недостатком ГНС, заключающийся в высоких требованиях к производительности вычислительных средств, которые в большинстве случаев не обеспечивают IP-камеры. Данное ограничение устранено при организации обработки на удаленных компьютерах, оборудованных видеокартами с высокими техническими характеристиками. Одним из популярных решений в области ГНС является модель YOLOv3, характеризующейся высоким значением отношения достоверность/производительность[5,6].

Схема алгоритма обнаружения объектов на видеоданных на основе глубокой нейронной сети YOLO представлена на рисунке 3.

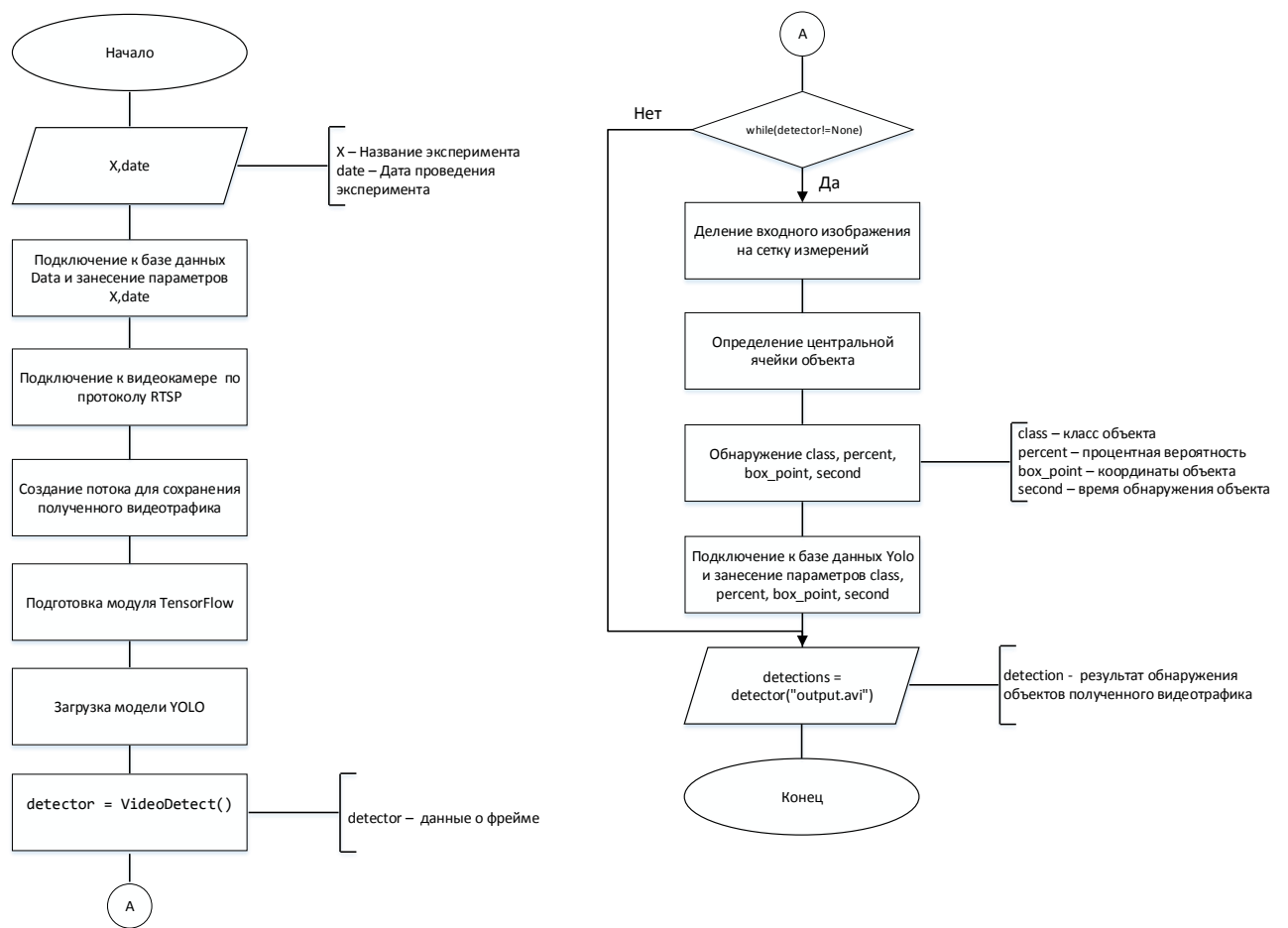


Рисунок 3 – Схема алгоритма обнаружения объектов на видеоданных на основе глубокой нейронной сети Yolo

Распознавание объектов на основе видеоданных IP-камеры реализована на языке программирования Python 3.7 с использованием модели YOLOv3, а также технологии NVIDIA CUDA. На вход программы поступают видеоданные от IP-камеры в режиме реального времени, либо в виде сохраненного видеофайла. В случае распознавания объекта выполняется SQL-запрос в базу данных на запись со следующими параметрами:

- отметки времени обнаружения объекта;
- классы, координаты и размеры обнаруженных объектов с оценками достоверности распознавания.

Результат распознавания объектов на основе полученного видеотрафика представлен на рисунке 4.

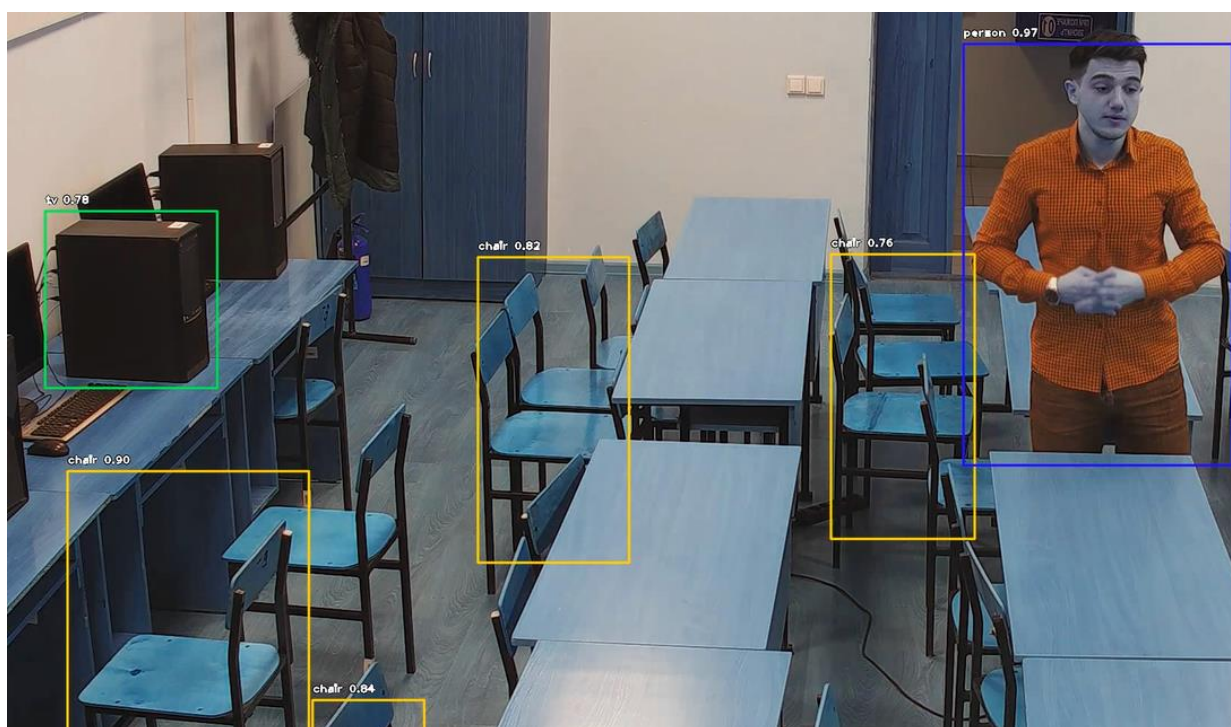


Рисунок 4 – Результат распознавания объектов на видеоданных на основе глубокой нейронной сети Yolo кафедры ВУЗа

Достоинствами данных методик являются получение навыков работы с современными технологиями в области СВН, в частности использования IP-камер при решении задач в области ИБ. Особенностью данных методик является возможность применения не только на лабораторных занятиях, но и в рамках лекционных, что позволит стимулировать интерес обучающихся на основе мультимедийных технологий.

Список литературы

1. Пескин, А.Е. Системы видеонаблюдения. Основы проектирования и эксплуатации / А.Е.Пескин. - М.: Горячая линия–Телеком, 2013. -256 с.
2. Проектирование системы видеонаблюдения на оборудовании «Болид» [Электронный ресурс]. - режим доступа: <https://bolid.ru/download/videobook.pdf/>
3. Кручинин А.Ю. Особенности защиты объектов со сложной конфигурацией в распределенных системах видеонаблюдения/ А.Ю. Кручинин, Р.Р. Галимов// ИНТЕЛЛЕКТ. ИННОВАЦИИ. ИНВЕСТИЦИИ. - 2017. - №9. – С. 64-69.
4. Ярышев С.Н. Методические указания по выполнению лабораторных работ по курсу Видеоаналитика и цифровая обработка видеосигналов. Учебно-методическое пособие. –СПб: Университет ИТМО, 2017. -92 с.
5. YOLO: Real-Time Object Detection [Электронный ресурс]. - режим доступа: <https://pjreddie.com/darknet/yolo/>.

6. Распознавание объектов в режиме реального времени на iOS с помощью YOLOv3 [Электронный ресурс]. – режим доступа: <https://temofeev.ru/info/articles/raspoznavanie-obektov-v-rezhime-realnogo-vremeni-na-ios-s-pomoshchyu-yolov3/>

АНАЛИЗ ЗАЩИЩЕННОСТИ СРЕДСТВ УДАЛЕННОГО ДОСТУПА К КОРПОРАТИВНОЙ СЕТИ

**Галимов Р.Р. канд.техн.наук, доцент, Корнейченко А.В., Мазалов Е.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
университет»**

АННОТАЦИЯ

В статье определены актуальные угрозы для систем удаленного доступа к ресурсам корпоративной сети. Проанализированы основные решения для удаленного доступа к ресурсам небольших организаций, разработаны рекомендации по их применению.

ABSTRACT

The article identifies current threats to remote access systems to corporate network resources. The main solutions for remote access to resources of small organizations are analyzed and recommendations for their application are developed.

Ключевые слова: корпоративная сеть, угроза, шифрование, удаленный доступ

Key words: remote desktop, threat, encry, remote access.

Популярной тенденцией для большинства современных предприятий является активное использование удаленной работы сотрудников, позволяющие как снизить эксплуатационные затраты офиса, так и повысить оперативность принятия решений. Так по следующим данным[8], не менее 40 % сотрудников информационных систем работают удаленно не менее 1 раза в неделю. При этом увеличивается процент рабочих процессов реализующихся на частных вычислительных устройствах служащих организации. Но при этом применение удаленного доступа к корпоративным ресурсам увеличивает риск информационной безопасности, обусловленный двумя основными причинами:

- сложностью обеспечить реализацию корпоративной политики ИБ на частных вычислительных устройствах сотрудников;
- недостаточной защищенностью шлюзов доступа к корпоративной сети.

Оценки угроз первого класса снижаются за счет применения организационных мер и применения специализированных средств защиты, таких как системы управления мобильными устройствами (MDM)[7]. Кроме того, эффективным решением для защиты от утечки конфиденциальных данных при удаленной работе на персональных устройствах является применение терминальных сессий. При этом необходимо обеспечить высокий уровень защищенности данной сессии, которая зависит как от используемых средств удаленного доступа, их настроек и области применения. В связи с

этим, существует необходимость в выявлении характеристик средств удаленного доступа для обеспечения высокого уровня защищенности.

Вопросы анализа средств удаленного доступа представлены в различных работах. В частности, в работе [9] представлен анализ средств удаленного доступа в контексте задачи дистанционного администрирования компьютеров. В статье [10] рассматриваются вопросы обеспечения безопасного удаленного доступа на основе различных виртуальных частных сетей и определяются рекомендации по их использованию. Несмотря на достоинства представленных результатов, необходимо отметить, что в них в недостаточной степени рассмотрены вопросы обеспечения информационной безопасности при использовании простых решений для небольших организаций.

Целью работы является определение оптимальных средств удаленного доступа для определенной информационной системы.

Для достижения данной цели решены следующие задачи:

- определены актуальные угрозы для ИС при использовании средств удаленного доступа;
- обоснованы критерии сравнения средств удаленного доступа;
- осуществлен анализ характеристик основных решений для удаленного доступа к ресурсам организации для небольшой организации;
- разработаны рекомендации для организации удаленного доступа к ПК организации.

Основной угрозой при использовании удаленного доступа к корпоративному компьютеру является риск НСД к ресурсам как отдельного ПК, так и всех элементов информационной системы предприятия. Уязвимость удаленного доступа определяется следующими причинами:

- для реализации удаленного доступа к ПК открывается порт на межсетевом экране с целью обеспечения возможности подключиться к корпоративной сети из Интернет;
- уязвимости протоколов сетевого взаимодействия программных средств, используемых для реализации удаленного доступа;
- не корректные настройки с точки зрения средств организации удаленного доступа к ПК корпоративной сети.

Для выбора оптимальных решений по организации удаленного доступа к ПК организации проведен анализ характеристик наиболее распространенных средств[1]:TeamViewer, AnyDesk,удаленныйрабочийстолWindows.

В качестве параметров сравнения средств удаленного доступа в данной работе выбраны следующие:

- стоимостные затраты на приобретение и эксплуатацию;
- шифрование сетевого трафика;
- схема аутентификации;
- возможность использования различных учетных записей.

TeamViewer.TeamViewer позволяет осуществлять удаленное управление различными устройствами: компьютерами, смартфонами и планшетами. Подключение осуществляется через серверы данной компании. Данный

подход позволяет удаленно подключаться к компьютерам без наличия статического IP-адреса. Отличительной чертой является простота установки и удобный интерфейс пользователя. Реализует следующие функции: удаленное управление, передача файлов и VPN-подключение.

Наиболее актуальной является функция удаленного управления ПК.

Безопасность и конфиденциальность обеспечивается следующими методами:

1. Программное обеспечение защищено цифровой подписью VeriSign. Это позволяет идентифицировать разработчика и определить целостность программы.

2. Принцип работы по сети данной архитектуры не требует открытия портов со стороны Интернета.

3. Шифрование и проверка подлинности. Защита потока данных базируется на обмене открытыми/личными ключами RSA и шифровании сеансов при помощи AES (256 бит). Данная схема гарантирует, что связанные между собой компьютеры, включая серверы маршрутизации TeamViewer, не смогут расшифровать сетевой поток.

4. Проверка идентификаторов TeamViewer. Идентификаторы автоматически генерируются на основе характеристик программного и аппаратного обеспечения. Серверы TeamViewer проверяют действительность идентификатора перед каждым соединением.

5. Защита от атаки методом перебора. Используется экспоненциальное увеличение задержки между попытками подключения[2].

6. Двухфакторная проверка подлинности. При двухфакторной проверке подлинности помимо запроса имени пользователя и пароля на мобильном устройстве создается код для входа в учетную запись TeamViewer. Для создания этого кода используется алгоритм одноразового пароля с учетом времени входа в систему (TOTP).

7. Белый список пользователей. Есть возможность разрешить доступ к удаленному компьютеру только разрешенных пользователей сервиса.

8. Возможность использовать учетные записи Windows.

Таким образом, для повышения безопасности удаленного доступа необходимо следующее:

- использовать сложный пароль. Для удобства хранения ключей нужно использовать менеджер паролей, например, KeyPass;
- не менее чем через 3 месяца менять пароль;
- настроить двухфакторную аутентификацию;
- определить «белый список» пользователей;
- при наличии нескольких клиентов использовать вход на удаленный ПК, используя учетные записи Windows.

AnyDesk. Данное решение предоставляет функционал похожий на TeamViewer. Основные режимы работы: удаленное управление и передача файлов. Отличительными особенностями данного решения являются: высокая

производительность за счет оригинального алгоритма сжатия данных. Функции шифрования трафика, белого списка аналогичны TeamViewer.

Для повышения безопасности удаленного доступа необходимо следующее:

- использовать сложный пароль. Для удобства хранения ключей нужно использовать менеджер паролей, например, KeyPass;
- не менее чем через 3 месяца менять пароль;
- определить «белый список» пользователей.

Удаленный рабочий стол. В Windows 7 (так же как и в предыдущих версиях Windows начиная с XP) присутствует возможность работы на компьютере удаленно, используя запущенную службу терминальных подключений. Для доступа к компьютеру с работающей службой, используется программа «Доступ к удаленному рабочему столу», присутствующая по умолчанию во всех версиях Windows начиная с XP.

При работе используется последняя на сегодняшний день версия протокола RDP (Remote desktop protocol v.7), в котором было сильно переработана работа с мультимедиа данными (передача видео и звука), а так же увеличена производительностью[3].

Для повышения безопасности удаленного доступа необходимо следующее:

- использовать сложный пароль для учетной записи. Для удобства хранения ключей нужно использовать менеджер паролей, например, KeyPass;
- настроить политику учетной записи: блокировать учетную запись при 5 неудачных попытках входа в систему, запретить сетевой вход с пустыми паролями;
- не менее чем через 3 месяца менять пароль;
- использовать пользовательский серверный сертификат проверки подлинности TLS[4];
- изменить стандартный порт 3389 на другой. Например, на 4678.
- разрешить подключения только компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети;
- определить «белый список» пользователей;
- для защиты от брутфорса использовать программу irban[5].

Дополнительно рекомендуется внедрить двухфакторную аутентификацию на основе программы ROHOS LOGON KEY[6].

Сравнительные характеристики средств удаленного доступа к ПК представлены в таблице 1.1.

Таблица 1 – Характеристики средств удаленного доступа

Характеристики/ решения	TeamViewer	AnyDesk	Удаленный рабочий стол Windows
----------------------------	------------	---------	--------------------------------------

Операционные системы	Windows, Mac OS, Linux, Android, Apple iOS, Windows Phone	Windows, macOS, iOS, Android, Linux, FreeBSD, Raspberry Pi, Chrome OS	Windows
Стоимость	- для личного пользования: бесплатно; - для коммерческого: 1999 руб. в месяц	- для личного пользования бесплатно; - для коммерческого: 9 евро в месяц.	Входит в состав ОС Windows, начиная с версии WindowsXP
Шифрование сетевого трафика	AES-256.	AES-256.	SSL TLS 1.0
Схема формирования сеансового ключа шифрования	На основе протокола RSA с механизмом проверки подлинности пароля.	На основе протокола RSA.	По умолчанию можно проверить только сервер на основе сертификата
Схема формирования идентификаторов	Идентификаторы автоматически генерируются на основе характеристик программного и аппаратного обеспечения. Серверы проверяют действительность идентификатора перед соединением.	Автоматическая генерация идентификатора.	Указывается вручную логин учетной записи
Защита от перебора	экспоненциальное увеличение задержки между попытками	Нет информации	Можно задать
Двухфакторная аутентификация	используется алгоритм одноразового пароля с учетом времени входа в систему (TOTP)	Нет	Нет по умолчанию
Разные учетные записи для подключения	При настройке входа с учетными записями Windows	Нет	Да
Доверенное устройство и	Да	Нет	Нет

процесс подтверждения			
«Белый список» разрешенных пользователей	Да	Да	Да
Необходимость статического ip- адреса	Нет	Нет	Да

Для повышения защищенности удаленного доступа к ПК необходимо дополнительно выполнить следующее:

- установить антивирусы: как на стороне сервера, так и клиента;
- установить сложные пароли на учетные записи.

Результаты анализа показывают, что для небольших предприятий предпочтительнее использование службы удаленного рабочего стола Windows, позволяющий настроить большее количество параметров. Основные недостатки:

- сложность настройки, требующая высокой квалификации системного администратора;
- необходимость статического «белого» IP-адреса.

Если данные требования не могут быть выполнены, то предпочтительнее применение TeamViewer.

Таким образом, современные средства удаленного доступа обеспечивают достаточно безопасный доступ к корпоративной системе при выполнении политики ИБ и выбора корректной конфигурации программного обеспечения.

Список литературы

1. Средства удаленного доступа на все случаи жизни [Электронный ресурс]. – Режим доступа: <https://xakep.ru/2013/10/31/remote-access-tools/>. – Дата доступа: 30.12.2019.

2. Центр управления безопасностью teamviewer [Электронный ресурс]. – Режим доступа: <https://www.teamviewer.com/ru/%d1%86%d0%b5%d0%bd%d1%82%d1%80-%d1%83%d0%bf%d1%80%d0%b0%d0%b2%d0%bb%d0%b5%d0%bd%d0%b8%d1%8f-%d0%b1%d0%b5%d0%b7%d0%be%d0%bf%d0%b0%d1%81%d0%bd%d0%be%d1%81%d1%82%d1%8c%d1%8e/%d0%b1%d0%b5%d0%b7%d0%be%d0%bf%d0%b0%d1%81%d0%bd%d0%be%d1%81%d1%82%d1%8c/>. – Дата доступа: 30.12.2019.

3. Подключение к Windows 7 через «Удаленный рабочий стол». [Электронный ресурс]. – Режим доступа:

<https://w7q.ru/windows7/podklyuchenie-k-windows-7-cherez-udalennyiy-rabochiy-stol/>. – Дата доступа: 30.12.2019.

4. Как заставить служб удаленных рабочих столов в Windows 7 для использования пользовательского серверного сертификата проверки подлинности TLS [Электронный ресурс]. – Режим доступа: <https://support.microsoft.com/ru-ru/help/2001849/how-to-force-remote-desktop-services-on-windows-7-to-use-a-custom-serv>. – Дата доступа: 30.12.2019.

5. Инструкция по защите RDP подключения [Электронный ресурс]. – Режим доступа: <https://neoserver.ru/help/kak-zashchitit-rdp-podklyuchenie-na-windows-server/>. – Дата доступа: 30.12.2019.

6. Rohos logon key [Электронный ресурс]. – Режим доступа: <http://www.rohos.ru/products/rohos-logon-key/>. – Дата доступа: 30.12.2019.

7. Самочадин А. В. Базовая функциональность систем централизованного управления мобильными устройствами/А. В. Самочадин, Т. Н. Самочадина, Д.А. Тимофеев, С.О. Попов // Научно-технические ведомости спбгпу. Информатика. Телекоммуникации. Управление. 2014. №4 (200). URL: <https://cyberleninka.ru/article/n/bazovaya-funktsionalnost-sistem-tsentralizovannogo-upravleniya-mobilnymi-ustroystvami> (дата обращения: 03.01.2020),

8. Удаленный доступ и утечка данных [Электронный ресурс]. – Режим доступа: http://lib.itsec.ru/articles2/Inf_security/udalenny-dostup-i-utechka-dannyh. – Дата доступа: 30.12.2019.

9. Анализ программных средств удаленного администрирования компьютеров [Электронный ресурс]. – Режим доступа: <https://docplayer.ru/73310052-Analiz-programmnyh-sredstv-udalennogo-administrirovaniya-kompyuterov.html>. – Дата доступа: 30.12.2019.

10. Удаленный доступ: в чем проблемы безопасности? [Электронный ресурс]. – Режим доступа: <http://tssonline.ru/articles2/in-ch-sec/informac-bezopasn-setey-udalen-dost>. – Дата доступа: 30.12.2019.

МЕТОДИКА ПРЕПОДАВАНИЕ ДИСЦИПЛИНЫ «ЧИСЛЕННЫЕ МЕТОДЫ» НА МАТЕМАТИЧЕСКИХ СПЕЦИАЛЬНОСТЯХ

**Джукашев К.Р., канд.физ.-мат.наук
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Математика является одним из важнейших инструментов познания окружающего мира. Она является главным методом теоретического исследования и практического применения знаний в науке и техники, без неё невозможно проводить серьёзные научные и технические расчеты. Математика как наука возникла на основе решения практических задач: вычисления расстояний, навигации, планирования и т.д. В следствии чего, изначально, да и сейчас на практике, математика была численной наукой.

Появление ЭВМ привело к новому этапу развития численного вычисления. Для исследования объектов реального мира применяется моделирования, при котором реальный объект заменяется на математическую модель. При этом аналитическим методами можно найти решения лишь для самых простых моделей, которые плохо описывают поведение реальных объектов, а более сложные модели могут не иметь аналитического решения. Поэтому кроме аналитических методов сегодня на практике используются методы, основанные на вычислениях, порой очень громоздких. В данных вычислениях активно используются вычислительные мощности современных компьютеров. Стоит отметить, что применение численных методов возможно только при совместном использовании с качественными методами, которые составляют большую часть современной математики.

Как уже отмечалось современные компьютеры оказывают незаменимую помощь при решении как задач, не имеющих аналитическое решение, так и задач, имеющих трудоемкое аналитическое решения. Поэтому в курс многих современных специальностей включен предмет «Численные методы» или «Вычислительная математика». Целью данной дисциплины является формирования готовности будущего выпускника к проведению вычислительного эксперимента. Для этого поставлены следующие задачи:

- формирование у обучающегося представлений о месте и роли вычислительного эксперимента в будущей профессиональной деятельности;
- изучение основных численных методов алгебры, математического анализа и обыкновенных дифференциальных уравнений;
- приобретение навыков реализации алгоритмов изученных методов на ЭВМ;
- приобретение навыков исследования и сопоставления методов в некотором классе задач, выборе наиболее оптимального метода для решения поставленной задачи.

В ходе изучения дисциплины рассматриваются следующие разделы и методы решения следующих задач:

- решение нелинейных уравнений и системы нелинейных уравнений;
- прямые, итерационные и параллельные методы решения СЛАУ;
- интерполирование и восстановление функции;
- численные дифференцирование и интегрирование;
- численное решение ОДУ и уравнений в частных производных.

Занятия по дисциплине «Численные методы» проводятся в форме лекций, лабораторных или практических работ, а также обучающиеся занимаются индивидуальной исследовательской работой. Весь курс поделен на разделы, где каждый раздел представляет собой или изучение методов решения отдельной задачи, или одного класса таких методов. Результатом работы обучающегося над каждым разделом является выполнение лабораторной работы с индивидуальным вариантом задания.

Основные разделы, изучаемые в курсе «Численные методы» [1,2]:

1. Введение в математическое моделирование и вычислительный эксперимент
2. Численное решение нелинейных уравнений
3. Прямые методы решения систем линейных алгебраических уравнений (СЛАУ)
4. Итерационные методы решения СЛАУ
5. Приближенное решение систем нелинейных уравнений
6. Численные методы решения проблемы собственных значений матрицы.
7. Интерполирование и восстановление функций
8. Численное интегрирование и дифференцирование
9. Численное решение задачи Коши для обыкновенных дифференциальных уравнений (ОДУ)
10. Численное решение уравнений в частных производных

В зависимости от специализации обучающихся и количества занятий некоторые из разделов могут не изучаться, либо даваться для самостоятельного ознакомления и в качестве индивидуального исследовательского проекта.

При изучении численных методов предполагается, что обучающиеся изучили разделы высшей математики, такие как математический анализ, линейную алгебру, дифференциальное и интегральное исчисление, обыкновенные дифференциальные уравнения и уравнения в частных производных. Эти разделы необходимы для полного усвоения применяемых методов и их обоснования.

В лекционных занятиях, кроме непосредственного изложения самих методов решения задач, для специальностей с математическим уклоном и при наличии достаточного времени могут даваться доказательства сходимости методов и верности полученных численных решений.

Первый раздел «Введение в математическое моделирование и вычислительный эксперимент» знакомит обучающихся с понятием численного или вычислительного эксперимента, обосновывает причины замены натурного эксперимента или аналитических вычислений на численный. В ходе изучения этого раздела обучающихся обучают схеме изучения реальных объектов и процессов по цепочке: построение математической модели – численное решение математической модели – алгоритмизация и реализация данной модели на ПК. Также обсуждается возможность применимости данных методов, условия их сходимости, корректности и адекватности.

В первом разделе также вводятся понятие погрешности и способы оценки погрешности результатов, полученных в ходе вычислительного эксперимента. Стоит отметить, что необходимо продемонстрировать обучающимся ограниченность возможностей современных ПК и возможность получить неверное решение при математически правильном методе и алгоритмически правильной его реализации.

Первый раздел в отличие от остальных разделов не предполагает выполнение лабораторной работы, однако, знания, полученные в ходе изучаемого раздела, необходимы для изучения дальнейших разделов и выполнения лабораторных работ.

Второй раздел «Численное решение нелинейных уравнений» знакомит обучающихся с численным решением уравнений вида $f(x) = 0$. В данном разделе обучающиеся знакомятся с методами отделения корней (аналитический метод, графический метод, табулирование) и методами уточнения корней (метод бисекций, метод Ньютона и его модификации, метод подвижных и неподвижных хорд, метод простых итераций), также дается обоснование и условия сходимости данных методов. В конце изучения данного раздела, обучающиеся выполняют лабораторную работу, где применяют все изученные методы и делают вывод о том, какой метод дал им лучший результат и почему, тем самым подтвердив опытным путем знания полученные на лекционных занятиях.

Третий раздел и четвертый раздел знакомит обучающихся с методами решения СЛАУ. В данных разделах обосновывается причины неприменимости на практике точных аналитических методов для решения СЛАУ (к примеру, метод Крамера). В разделах изучаются различные численные методы по решению СЛАУ, как точных (метод Гаусса и его модификации, LU-метод), так и итерационных методов. Кроме непосредственного решения СЛАУ в разделах изучается и применение данных методов для решения задач, сводящихся к решению СЛАУ (вычисление определителя и ранга матрицы, нахождение обратной матрицы).

Для изучения пятого раздела «Приближенное решение систем нелинейных уравнений» обучающиеся должны изучить и выполнить лабораторные работы предыдущих разделов, т.к. методы, используемые для

решения систем нелинейных уравнений, опираются на методы решения нелинейных уравнений и СЛАУ.

В ходе изучения разделов «Интерполирование и восстановление функций» обучающихся знакомят с понятием интерполяции и различными способами восстановления функции от самых простых (аппроксимация линейной функции) до более сложных (интерполяция сплайн-методами). В ходы выполнения лабораторной работы им предлагается интерполировать функцию используя линейную интерполяцию, метод наименьших квадратов с выбором наиболее оптимальной функции и кубический сплайн-метод.

Раздел «Численное интегрирование и дифференцирование» частично опирается на предыдущий раздел, т.к. многие методы интегрирования и дифференцирования используют аппроксимацию исходной функции функциями более низкого порядка, а для этого необходимо использовать методы интерполяции.

Разделы «Численные методы решения проблемы собственных значений матрицы», «Численное решение задачи Коши для обыкновенных ОДУ», «Численное решение уравнений в частных производных» изучаются на специальностях с математическим уклоном, т.к. задачи, решаемые в данных разделах, возникают, к примеру, при преобразовании матриц (задача о собственных значениях) или в уравнениях математической физики (обыкновенные дифференциальные уравнения и уравнения в частных производных). Данные разделы требуют знания линейной алгебры и аналитических методов решения уравнений с производными. Для изучения методов решения дифференциальных уравнений обучающиеся должны также усвоить раздел, посвященный численному дифференцированию.

Как уже отмечалось ранее каждый из разделов, за исключением первого, изучает различные методы решения поставленных задач и для лучшего усвоения и понимания работы методов, условий и границ их применимости, сходимости и выбора наиболее оптимального метода для поставленной задачи, обучающиеся выполняют лабораторную работу по каждому из разделов с индивидуальными вариантами заданий. Перед обучающимися стоит задача применить изученный метод на практике и проанализировать и сделать вывод о его сходимости (определение количества итераций для получения требуемой точности). При хорошем знании языков программирования данные работы рекомендуется выполнять, используя любой современный язык программирования, поддерживающий все необходимые структуры и операции, используемые в методе. Также можно использования методов параллельного программирования для вычислительно-затратных задач (метод Гаусса или вычисление интеграла).

Однако, если обучающийся владеет слабой подготовкой в программировании, то возможно применение любых других средств компьютерной математики, такие как математические пакеты и электронные таблицы. Главной задачей при изучении курса «Численных методов» ставится изучение методов и реализации алгоритмов изученных методов на ПК.

У реализации алгоритмов численных методов различными способами, будь то программирование или, к примеру, электронные таблицы, есть как свои достоинства, так и недостатки. Реализация методов в электронных таблицах выигрывает в скорости реализации, удобном представлении полученных данных и возможности дальнейшей их обработки. Реализация методов с помощью языков программирования требует больших ресурсов, связанных с написанием, тестированием и отладкой программы, а также с необходимостью организации ввода/вывода в форме, удобной для дальнейшей обработки.

Главными достоинствами реализации методов с помощью написания компьютерной программы являются легкая масштабируемость полученного решения и возможность быстрого изменения исходных данных решаемой задачи. Кроме того, компьютерная программа выигрывает при низкой сходимости метода, когда для получения требуемой точности необходимо провести десятки тысяч или миллион итераций.

Так как используемые методы в дальнейшем будут применяться обучающимися в профессиональной деятельности, а значит будут использоваться многократно для различного набора данных, то всё же рекомендуется написание компьютерной программы. При этом код программы желательно организовывать так, чтобы метод можно было применить к различным задачам, внося незначительные изменения в код или писать универсальную программу для данного метода.

Дисциплина «Численные методы» преподается на всех направлениях подготовки бакалавров математических специальностей. Дисциплина является естественным продолжением «классических» математических дисциплин (математический анализ, линейная алгебра, дифференциальные уравнения и пр.), позволяющая автоматизировать уже знакомые методы решения задач, а также решать численно задачи, не имеющие аналитического решения или имеющие трудоемкое аналитическое решение. В ходе изучения данной дисциплины, обучающиеся математических специальностей, закрепляют ранее полученные знания и учатся выстраивать цепочку: математическая модель – численный метод – его реализация на ПК. Данный подход является универсальным при решении множества задач в их будущей профессиональной деятельности.

В виду сложности математических моделей, описывающих реальные процессы и явления, численные методы предоставляют мощный инструмент для нахождения оптимального решения. Даже наличие аналитического решения не является причиной не использовать численные методы, из-за возможности автоматизации и решение вычислительно сложных задач в приемлемое время. Поэтому дисциплина «Численные методы» является важной при получении высшего технического или математического образования.

[1] Пименов, В. Г. Численные методы: в 2 ч. Ч. 1: [учебное пособие] / В.Г. Пименов. – М-во образования и науки РФ, Урал. федер. ун-т. – Екатеринбург: Издательство Уральского университета, 2013. – 112 с.

[2] Пименов, В. Г. Численные методы: учебное пособие: в 2 ч., Ч. 2 [учебное пособие] / Пименов В. Г., Ложников А. Б. – М-во образования и науки РФ, Урал. федер. ун-т. – Екатеринбург: Издательство Уральского университета, 2014. – 106 с.

ЭФФЕКТИВНОСТЬ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ОБУЧЕНИИ МАТЕМАТИКЕ

Калматаева Б.Б.

**PhD докторант, Международный Казахско-Турецкий Университет,
им. Х.А. Ясави, г.Туркестан, Казахстан.**

Подготовка высококвалифицированного, конкурентоспособного на рынке труда специалиста зависит от многочисленных факторов, в том числе от качества математического образования.

Использование компьютерных программ активизирует все виды деятельности человека: мыслительную, речевую, физическую, что, в свою очередь, способствует более полному усвоению материала.

Появление и широкое распространение интерактивных компьютерных технологий позволяет использовать их в качестве средства общения и воспитания. Было отмечено влияние информационных технологий на развитие личности, профессиональное самоопределение и самостановление.

Эффективность применения новых информационных технологий на уроках математики обусловлена многими факторами, в числе которых:

- разнообразие форм подачи информации;
- высокая степень наглядности;
- возможность моделировать разного вида объекты и процессы;
- высвобождение свободного времени;
- организация коллективной и индивидуальной исследовательской работы;
- дифференцирование заданий в зависимости от уровня подготовки учащихся;
- быстрый контроль и помощь со стороны преподавателя;
- возможность для ученика активно принимать участие в процессе познания.

Разумное сочетание традиционных и компьютерных форм организации учебного процесса, создает новое качество при формировании системы знаний.

Методика проведения занятий с использованием компьютерных технологий может применяться при:

- изложении нового материала;
- проверке и систематизации знаний; -решении графических задач.

Компьютерная поддержка изучения математики увлекает учащихся, облегчает осмысление сложных определений, содержащих специфическую терминологию, дает наглядное представление об основных понятиях геометрии, способствует развитию образного мышления, побуждает учащихся к исследовательской деятельности.

В процессе обучения с помощью интерактивных компьютерных технологий учащийся учится работать с текстом, создавать графические

объекты и базы данных, использовать электронные таблицы. Обучаемый узнает новые способы сбора информации и учится пользоваться ими. При использовании интерактивных компьютерных технологий на занятиях повышается мотивация учения стимулируется познавательный интерес обучающихся, возрастает эффективность самостоятельной работы. Компьютер вместе с интерактивными компьютерными технологиями открывает принципиально новые возможности в области образования, в учебной деятельности и творчестве обучаемых.

Использование информационно-коммуникационных технологий на учебных занятиях по математике способствует активизации учебно-познавательной деятельности учащихся, быстрому и эффективному усвоению ими учебного материала.

Компьютерная информационная технология – это совокупность методов, форм и средств воздействия на человека в процессе его развития.

Практическое использование компьютерной техники в учебном процессе дает возможность выбирать различные организационные формы работы – индивидуальную, групповую или коллективную, возможность показать ученикам математику с самой привлекательной стороны, вызвать в ученике радость и удовольствие от занятий умственным трудом, заинтересовать предметом.

Принцип доступности и посильности образования сводится к тому, чтобы изучаемый материал по уровню трудности был доступен, но в то же время требовал напряжения умственных и духовных сил для своего усвоения. С помощью интерактивных компьютерных технологий стало возможным дифференцировать диалоги с обучающимися в зависимости от их подготовленности, скорости и качества выполнения заданий. Современные программы позволяют генерировать задачи возрастающей сложности. При должной мотивации, работая с такой программой, ученик сам будет отбирать задачи, требующие от него умственного напряжения.

Компьютерные технологии позволяют добиться качественно более высокого уровня наглядности предлагаемого материала, значительно расширяют возможности включения разнообразных упражнений в процессе обучения, оживляют учебный процесс, способствуют повышению его динамики, что, в конечном счете, ведет к достижению главной цели обучения – формированию положительного отношения учащихся к изучаемому материалу.

С помощью компьютера появляется возможность развития критического мышления, т. е. совершенствуются умения, связанные с извлечением, переработкой и усвоением информации.

Очевидно, что использование компьютерных технологий обеспечивает оперативность, наглядность и емкость информации за короткий промежуток времени.

Можно выделить пять ключевых аспектов повышения качества обучения за счет внедрения интерактивных компьютерных методик:

1. Развитие интереса к математическим дисциплинам.

Первый этап можно назвать самым простым. Вызвав интерес к предмету, нужно удержать его, добиться, чтобы у учащегося появилось желание заниматься дальше.

2. Желание учиться.

Очень важным является этап настоящего желания достижения положительного результата. Это главный фактор успеха. Именно сейчас желательно показать возможность и доступность реализации намеченного, чтобы появилась вера в себя.

3. Вера в себя.

Этот этап может быть длительным и не простым. Учащийся видит первые свои результаты, начинает добиваться побед. Он верит в свои силы и готов преодолевать любые преграды.

4. Преодоление преград.

Преграды в виде решения и осмысления более сложных задач по принципу «от простого к сложному». Появляется уверенность, что можно достичь больших высот. «Скажи мне – и я забуду, покажи мне – и я запомню, дай мне сделать – и я пойму» (Конфуций).

Самым главным является достижение намеченного результата.

5. Положительный результат.

Все этапы ведут к определенному итогу. На протяжении всего времени учащиеся двигались вперед, к поставленной цели. Это понимание и усвоение материала в полном объеме, решение разных видов заданий и получение признания собственных знаний в виде высоких оценок.

Уч. Год курс	Кол-во студентов в группе	Успеваемость в начале учебного года			Успеваемость в конце учебного года		
		Ср.балл	Кол-во студентов	%	Ср. балл	Кол-во студентов	%
2012-2013 1-курс	23	«3»	15	65,2	«3»	10	43,4
		«4»	8	34,7	«4»	12	52,1
		«5»			«5»	1	4,3
2013-2014 2-курс	23	«3»	10	43,4	«3»	8	34,7
		«4»	12	52,1	«4»	14	60,9
		«5»	1	4,3	«5»	1	4,3

Таблица 1 - Сравнительная характеристика успеваемости студентов

В течение двух лет с 2012 по 2014 преподавала в экспериментальной группе. Группа состояла из 23 человек, состав группы не отличался от других

групп, т.е. можно говорить о репрезентативности выборки. На момент окончания школы успеваемость по математике у учащихся данной группы выглядела следующим образом: 15 студентов имели средний балл «3», 8 студентов имели средний балл «4».

Было решено проверить потенциал улучшения результатов этих студентов по математическим дисциплинам с помощью наблюдений, бесед, анкет, проблемных заданий, входного и окончательного тестирования. Уровни развития сравнивались в начале и в конце экспериментальной работы. В течение двух лет учащиеся посещали математический кружок, активно занимались в компьютерном классе. За два года обучения можно проследить тенденцию роста успеваемости студентов данной группы.

На основании представленных данных можно сделать вывод об эффективности использованных методов и приемов. По результатам эксперимента мы видим, что при систематическом посещении занятий, математического кружка и компьютерного класса у учащихся повышается интерес к математическим дисциплинам, увеличивается работоспособность, растет эффективность выполнения заданий. Таким образом, можно констатировать положительное влияние выбранных мер на качество успеваемости.

Студенты экспериментальной группы имели разный уровень базовой подготовки и включались в активный режим работы в течение всего учебного года. При этом все они ответственно относились к выполнению домашних заданий, учились с интересом и желанием. Они не только усваивали знания, которые им предлагали в рамках учебного курса, но и тянулись самостоятельно к новым.

К показателям роста достижений студентов за два года обучения можно отнести то, что в группе появился отличник, увеличилось количество студентов обучающихся на «4» на 26,2 %.

Можно с уверенностью сказать: работа проведена не зря, но не стоит останавливаться на достигнутом, ведь есть реальная возможность улучшения результатов.

Подытоживая проделанную работу можно сделать вывод, что занятия математикой стали полезными для развития интеллектуальных качеств учащихся, благоприятно влияют на логическое мышление, творческие способности, умение планировать, обобщать, находить закономерности, быстро включаться в работу.

Использование средств интерактивных компьютерных технологий повышает эффективность учебной деятельности учащихся, ИКТ используются как способ самоорганизации труда и самообразования учащихся, как способ расширения зоны индивидуальной активности учащихся. Интерактивные компьютерные технологии дают возможность реализации личностно-ориентированного подхода в обучении.

Использование средств ИКТ способствует достижению всех целей урока, эффективному закреплению материала, оперативному контролю знаний учащихся и повышению качества обучения.

Список литературы

1. Андрющенко Я.Э. Анализ педагогических технологий, используемых в процессе профессиональной подготовки магистров физико-математических специальностей в открытых образовательных ресурсах // Синергия. 2016. № 3. С. 26-30.
2. Дьяченко С.А. Интеграционное развитие профессиональных компетенций в процессе обучения математическим дисциплинам // Территория науки. 2015. № 6. С. 31-34
3. Маклаева Э.В., Фёдорова С.В. Организация продуктивной деятельности студентов средствами математики // Синергия. 2016. №2. С. 27-32.
4. Саранцев Г. И. Нужны ли интерактивные формы обучения? // Проблемы современного математического образования в вузах и школах России: Интерактивные формы обучения математике студентов и школьников. Материалы V Всеросс. науч.-методич. конф.– Киров: Изд-во ВятГГУ, 2012. – С. 42–48.
5. Суворова Н. «Интерактивное обучение: новые подходы». - М., 2005.
6. Шамин Е.А., Генералов И.Г., Завиваев Н.С., Черемухин А.Д. Сущность информатизации, ее цели, субъекты и объекты // Вестник НГИЭИ. 2015. № 11 (54). С. 99-107.

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ДЛЯ ОБРАБОТКИ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ НА ЯЗЫКЕ JAVASCRIPT

**Кобылкин Д.С., канд.тех. наук, Юсупова О.В.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

В современных условиях развития научно-технического прогресса важной задачей перед будущим выпускником высшего учебного заведения, занимающегося разработкой и обслуживанием информационных систем, является прививание знаний об основных этапах обработки, статистических методов оценивания характеристик экспериментальных данных, а также формирование умений и навыков по использованию специализированных программ для статистической обработки информации при программировании процессов обработки экспериментальных данных с использованием средств вычислительной техники;

Студентами кафедры информатики направления подготовки 09.03.02 «Информационные системы и технологии» изучается дисциплина «Обработка экспериментальных данных». Целью освоения дисциплины является изучение организационных, научных и методических основ планирования научного эксперимента, обработки его результатов, овладение современными статистическими методами исследований на основе теории эксперимента.

При изучении дисциплины студенты выполняют лабораторные работы, в ходе которых они занимаются аналитической обработкой материалов с применением возможностей современных статистических пакетов программ с овладением такой компетенции как реализация статистической обработки экспериментальных данных в информационных системах [2].

Весьма эффективным средствами при выполнении статистических исследований являются программы со встроенными средствами анализа данных: Microsoft Excel, Statistica, Deductor. Они позволяют обеспечить быстроту статистических расчетов, высокую надежность и достоверность результатов, возможность предоставления данных в аналитической, графической или табличной формах [2]. Одновременно, следует указать, что указанные программные средства должны быть установлены на определенных условиях, и пользователь должен обладать определенными знаниями и навыками работы в этих программах. Поэтому возникает потребность в разработке собственного программного продукта, позволяющего проводить многомерный статистический анализ любых данных с получением результата обработки на интуитивно понятном уровне.

При изучении дисциплины программное средство должно демонстрировать решения задач по обработке экспериментальных данных и визуализации получаемых данных. Программа должна иметь графический интерфейс. Требования, как программному, так и аппаратному обеспечению,

должны быть по возможности минимальными. Программа должна адекватно реагировать на все возникающие в процессе работы программы ситуации и обрабатывать их в соответствии с алгоритмом поставленной задачи, также надежно функционировать на ПК любой приемлемой конфигурации.

Прежде чем остановить свой выбор на каком-либо конкретном программном обеспечении, необходимо провести анализ существующего программного обеспечения (таблица 1).

Таблица 1 – Сравнение языков JavaScript и PHP

	JavaScript	PHP
Поддержка браузеров	Да	Нет
Нужен сервер	Нет	Да
Простота в использовании	Да	Нет
Нужна компиляция	Нет	Да
Работа с СУБД	Нет	Да

Таким образом для данных задач отлично подходит язык JavaScript. Не нужно устанавливать и разворачивать локальный сервер, не требуется работа с базой данных[1].

На кафедре информатики было разработано программное средство, которое предназначено для демонстрации решения задач по обработке экспериментальных данных и визуализации получаемых данных. Программное средство было реализовано как веб-приложение. Интерфейс написан с использованием языка разметки HTML. Для написания стилей приложения был использован CSS-фреймворк Bootstrap 4, предоставляющий набор готовых классов для создания дизайна приложения. «Бэкенд» приложения написан языке JavaScript с использованием библиотеки JQuery. Для вывода графиков была использована библиотека ChartJS. Все эти технологии позволяют создать качественное веб-приложение в короткие сроки, удовлетворяющее требованиям заказчика.

Основными для данного программного средства являются такие достоинства, как кроссплатформенность, то есть возможность использования приложения на любой операционной системе, так как приложение работает в браузере. Также не требуется установка, достаточно лишь запустить файл, который и запустит приложение в браузере. Наличие мобильной версии приложения. Недостаток здесь один – наличие подключения к интернету, если приложение развернуто на сервере. Если же приложение хранится локально, то и интернет здесь необязателен.

Программа состоит из 5 частей:

1. Случайная выборка
2. Проверка распределения
3. Регрессионный анализ
4. Однофакторный дисперсионный анализ
5. Двухфакторный дисперсионный анализ

Рассмотрим основные функции, используемые в разработанном программном средстве:

- функция `createData` – создает массив случайных элементов (рисунок 1);
- функция `getRandomInRange` – генерирует число в указанном диапазоне (рисунок 2);
- функция `getSumArray` – суммирует элементы массива (рисунок 3);
- функция `getAverageValue` – находит среднее значение элементов массива (рисунок 4);
- функция `getArrayDispersion` – находит дисперсию ряда (рисунок 5);
- функция `Cohren` – вычисляет критерий Кохрена (рисунок 6);
- функция `getSumsSquare` – вычисляет сумму квадратов всех наблюдений (рисунок 7).

```
function createData(max){  
    var arrayLength = parseInt($("#array-length").val());  
    var data = [];  
    for(var i=0; i<arrayLength; i++){  
        var elem = Math.floor(Math.random() * max);  
        data.push(elem);  
    }  
    return data;  
}
```

Рисунок 1 – Код функции `createData`

```
function getRandomInRange(min, max) {  
    //генерация случайного числа между min и max  
    return Math.floor(Math.random() * (max - min + 1)) + min;  
}
```

Рисунок 2 – Код функции `getRandomInRange`

```
function getSumArray(array) {  
    //получение суммы элементов массива  
    var sumArray = 0;  
    for (var i=0; i<array.length; i++) {  
        sumArray += array[i];  
    }  
    return sumArray;  
}
```

Рисунок 3 – Код функции `getSumArray`

```
function getAverageValue(array) {  
    var sumArray = getSumArray(array);  
    return sumArray / array.length;  
}
```

Рисунок 4 – Код функции getAverageValue

```
function getArrayDispersion(array, average) {  
    //получение оценки дисперсии массива  
    var numerator = 0;  
    for (var i=0; i<array.length; i++) {  
        numerator += Math.pow(array[i] - average, 2);  
    }  
    return numerator / (array.length - 1);  
}
```

Рисунок 5 – Код функции getArrayDispersion

```
function Cohren(dispersions) {  
    //получение критерия Кохрена  
    var maxDispersion = Math.max.apply(null, dispersions);  
    var sumDispersions = 0;  
    for (var i=0; i<dispersions.length; i++) {  
        sumDispersions += dispersions[i];  
    }  
    return maxDispersion / sumDispersions;  
}
```

Рисунок 6 – Код функции Cohren

```
function getSumsSquare(arrays) {  
    //получение суммы квадратов всех наблюдений  
    var sumsSquare = 0;  
    for (var i=0; i<arrays.length; i++) {  
        for (var j=0; j<arrays[i].length; j++) {  
            sumsSquare += Math.pow(arrays[i][j], 2);  
        }  
    }  
    return sumsSquare;  
}
```

Рисунок 7 – Код функции getSumsSquare

Это были основные функции, используемые в приложении. Остальные функции специфичны для каждой задачи.

Для решения задачи двухфакторного дисперсионного анализа необходимо нажать на ссылку «Двухфакторный дисперсионный анализ». Откроется страница с задачей (рисунок 8): «В химической лаборатории проверяется влияние температуры (фактор А) и катализатора (фактор В) на выход продукта химического синтеза. Полученные результаты приведены в таблице. Проведите двухфакторный дисперсионный анализ. При уровне значимости $\alpha = 0,05$ проверьте гипотезу о влиянии факторов А и В и их комбинации на указанный признак» [3]. Данная задача выбрана для демонстрации решения двухфакторного дисперсионного анализа. Для запуска решения нужно нажать на кнопку «Сгенерировать» После этого будет сгенерирована таблица значений задачи.

Двухфакторный дисперсионный анализ

Задача

В химической лаборатории проверяется влияние температуры (фактор А) и катализатора (фактор В) на выход продукта химического синтеза. Полученные результаты приведены в таблице. Проведите двухфакторный дисперсионный анализ. При уровне значимости $\alpha = 0,05$ проверьте гипотезу о влиянии факторов А и В и их комбинации на указанный признак.

Нажмите кнопку "Сгенерировать" для занесения результатов в таблицу

Сгенерировать

	B1	B2	B3
A1	25,14,16,24	13,19,20,25	25,22,19,22
A2	23,14,17,24	22,24,18,15	21,12,14,23
A3	19,10,24,11	17,20,24,19	15,14,16,21
A4	17,17,18,22	11,21,15,17	15,23,14,21

Рисунок 8 – Таблица значений задачи

После генерации таблицы будет представлено решение задачи (рисунок 9, рисунок 10).

Шаг 1 Формулировка гипотез

Гипотезы для взаимодействия:

H0: Фактор А (температура) и фактор В (катализатор) не оказывают эффекта взаимодействия на результат Y (продукт химического синтеза).

H1: Фактор А и фактор В оказывают эффекта взаимодействия на результат Y.

Гипотезы для фактора А:

H0: Для всех режимов температуры A_i нет разницы между средним результатом продукта химического синтеза Y.

H1: Для всех типов A_i существует разница между средним результатом Y.

Гипотезы для фактора В:

H0: Для всех типов катализатора B_j нет разницы между средним результатом Y.

H1: Для всех типов B_j существует разница между средним результатом Y.

Рисунок 9 – Формулировка гипотез

Шаг 2 Расчёт данных

	Yi1	Yi2	Yi3	Yi
Y1j	19.75	19.25	22	20.33
Y2j	19.5	19.75	17.5	18.92
Y3j	16	20	16.5	17.50
Y4j	18.5	16	18.25	17.58
Yj	18.4375	18.75	18.5625	18.5833

Сумма квадратов отклонений под влиянием m уровней фактора А: $Q_a = 16.04$

Сумма квадратов отклонений под влиянием k уровней фактора В: $Q_b = 0.20$

Оценка дисперсии уровней А (влияние фактора А на продукт химического синтеза): $S_a^2 = 5.35$

Оценка дисперсии уровней В (влияние фактора В на продукт химического синтеза): $S_b^2 = 0.10$

Рисунок 10 – Расчёт данных

По результатам видно, что влияние фактора А выше, чем влияние фактора В.

Для проверки правильности работы разработанной программы необходимо провести верификацию проработанного средства. В качестве проверки правильности работы программы был выбран для сравнения результатов MSExcelc установленным пакетом «Анализ данных» [4]. Рассмотрим на примере результаты верификации при проверке двухфакторного дисперсионного анализа.

1. Генерируем таблицу значений (рисунок 11).

	B1	B2	B3
A1	15,14,14,15	17,11,15,20	24,25,22,17
A2	19,13,10,19	16,18,12,14	10,18,22,14
A3	24,12,16,25	14,19,16,11	16,21,15,11
A4	17,10,15,20	24,21,19,15	20,18,18,13

Рисунок 11 – Генерация таблицы

2 Получаем таблицу средних значений (рисунок 12).

	Yi1	Yi2	Yi3	Yi
Y1j	14.5	15.75	22	17.42
Y2j	15.25	15	16	15.42
Y3j	19.25	15	15.75	16.67
Y4j	15.5	19.75	17.25	17.50
Yj	16.125	16.375	17.75	16.7500

Рисунок 12 – Таблица средних значений

3. Получаем результаты расчета программы (рисунок 13).

Сумма квадратов отклонений под влиянием m уровней фактора А: $Q_a=8.38$

Сумма квадратов отклонений под влиянием k уровней фактора В: $Q_b=6.13$

Оценка дисперсии уровней А (влияние фактора А на продукт химического синтеза): $S_a^2=2.79$

Оценка дисперсии уровней В (влияние фактора В на продукт химического синтеза): $S_b^2=3.06$

Рисунок 13– Результаты вычислений приложения

4. Копируем таблицу средних значений в Excel (рисунок 14).

8		yi1	yi2	yi3
9	y1j	14,5	15,75	22
10	y2j	15,25	15	16
11	y3j	19,25	15	15,75
12	y4j	15,5	19,75	17,25

Рисунок 14 – Построение таблицы в excel

5. Запускаем решение двухфакторного дисперсионного анализа в Excel (рисунок 15).

	A	B	C	D	E	F	G
1	Двухфакторный дисперсионный анализ без повторений						
2							
3	ИТОГИ	Счет	Сумма	Среднее	Дисперсия		
4	Строка 1	3	52,25	17,4166667	16,14583333		
5	Строка 2	3	46,25	15,4166667	0,270833333		
6	Строка 3	3	50	16,6666667	5,145833333		
7	Строка 4	3	52,5	17,5	4,5625		
8							
9	Столбец 1	4	64,5	16,125	4,520833333		
10	Столбец 2	4	65,5	16,375	5,1875		
11	Столбец 3	4	71	17,75	8,458333333		
12							
13							
14	Дисперсионный анализ						
15	Источники вариации	SS	df	MS	F	P-Значение	F критическое
16	Строки	8,375	3	2,79166667	0,363143631	0,782383592	4,757062663
17	Столбцы	6,125	2	3,0625	0,398373984	0,687939511	5,14325285
18	Погрешность	46,125	6	7,6875			
19							
20	Итого	60,625	11				

Рисунок 15 – Результаты вычислений Excel

6. Сравниваем полученные значения (рисунок 16).

Сумма квадратов отклонений под влиянием m уровней фактора А: $Q_a=8.38$
Сумма квадратов отклонений под влиянием k уровней фактора В: $Q_b=6.13$
Оценка дисперсии уровней А (влияние фактора А на продукт химического синт
Оценка дисперсии уровней В (влияние фактора В на продукт химического синт

	А	В	С	Д	Е	Ф	Г
1	Двухфакторный дисперсионный анализ без повторений						
2							
3	ИТОГИ	Счет	Сумма	Среднее	Дисперсия		
4	Строка 1	3	52,25	17,4166667	16,14583333		
5	Строка 2	3	46,25	15,4166667	0,270833333		
6	Строка 3	3	50	16,6666667	5,145833333		
7	Строка 4	3	52,5	17,5	4,5625		
8							
9	Столбец 1	4	64,5	16,125	4,520833333		
10	Столбец 2	4	65,5	16,375	5,1875		
11	Столбец 3	4	71	17,75	8,458333333		
12							
13							
14	Дисперсионный анализ						
15	Фактор	SS	df	MS	F	P-Значение	F критическое
16	Строки	8,375	3	2,791666667	0,363143631	0,782383592	4,757062663
17	Столбцы	6,125	2	3,0625	0,398373984	0,687939511	5,14325285
18	Погрешность	46,125	6	7,6875			
19							
20	Итого	60,625	11				

Рисунок 16 – Сравнение значений

Как видно из рисунка 16 все значения сходятся, следовательно двухфакторный дисперсионный анализ реализован правильно.

Разработанное приложение, наглядно демонстрирующее решения многомерного статистического анализа: формирование случайной выборки, проверка распределения по критерию Пирсона, регрессионный анализ, однофакторный и двухфакторный дисперсионный анализ. Приложение рекомендуется использовать для изучения теоретического материала по этим темам, так как в приложении используются графики и таблицы, позволяющие наглядно увидеть и проанализировать данные. Разработанное приложение возможно применять студентами, аспирантами и учеными-исследователями, занимающимися экспериментальной обработкой информации.

Список литературы

1. Гарнаев, А. Web-программирование на Java и JavaScript / А. Гарнаев, С. Гарнаев. - СПб. : БВХ-Петербург, 2005. - 1040 с. : ил. - Прил.: с. 1009-1012. - Предм. указ.: с. 1013-1021. - ISBN 5-94157-088-0.
2. Кобылкин, Д. С. Разработка программного средства для проведения исследований с параллельной статистической обработкой результатов [Электронный ресурс] / Д. С. Кобылкин, С. Г. Майер // Шаг в науку, 2019. - № 3. - С. 23-26.
3. Математические методы обработки экспериментальных данных: методическое пособие/Б.А. Шкарин. – Вологда: ВоГУ, 2014. – 55 с.

4. Цыпин, А. П. Статистика в табличном редакторе Microsoft Excel [Электронный ресурс]: лабораторный практикум: учебное пособие для студентов, обучающихся по программам высшего образования по направлению подготовки 38.03.01 Экономика / А. П. Цыпин, Л. Р. Фаизова; Минобрнауки России, Федеральное государственное бюджетное образовательное учреждение высшего образования "Оренбургский государственный университет". - Электрон. текстовые дан. (1 файл: 4.94 Мб). - Оренбург : ОГУ, 2016. - 288 с. – Режим доступа:

[http://artlib.osu.ru/site_new/index.php?option=com_find&type=getfile&name=9988_20160329.pdf&folder1=metod_all&folder2=books&no_html=1'](http://artlib.osu.ru/site_new/index.php?option=com_find&type=getfile&name=9988_20160329.pdf&folder1=metod_all&folder2=books&no_html=1)

МАТЕМАТИЧЕСКИЕ ЗАДАЧИ С ЭКОНОМИЧЕСКИМ СОДЕРЖАНИЕМ В ОБРАЗОВАНИИ

**Колобов А.Н., канд. техн. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный педагогический университет»**

В школьном курсе математики в последние годы особое внимание уделяется так называемым экономическим задачам. Это задачи, в которых содержание имеет экономический смысл, но решение требует использования математического аппарата. Экономические задачи могут быть разной степени сложности, и в их формулировках могут содержаться различные экономические понятия, такие, как процентные величины, прибыль, доход и т.п. Наиболее простые по сложности задачи имеются не только в школьных учебниках математики, но и в контрольно-измерительных материалах ЕГЭ. Самые простые из этих задач имеются в заданиях №1 и №11 в первой части ЕГЭ; их решение потребует лишь минимума познаний в области математики и не вызывает сложностей в вычислительном плане. Типичными примерами в заданиях №1 являются задачи, где описывается повышение или понижение стоимости товара в процентном отношении, и эти задачи в основном решаются очень простыми методами, например, с помощью пропорций. В заданиях №11 помимо задач с процентами встречаются задачи на производительность и совместную работу; их решение может быть осуществлено с помощью уравнений или системы уравнений.

Наиболее сложные задачи с экономическим содержанием включены во вторую часть материалов ЕГЭ. Это задания №17, которые подразделяются в основном на два типа по внутреннему содержанию: 1) задачи на банковские проценты, вклады, кредиты, выплаты; 2) задачи на оптимальный выбор. Могут быть также смешанные задачи, в которых потребуется оптимизация решений с банковскими вкладами. Задачи каждого типа решаются различными математическими методами. В задачах на банковские проценты большое значение уделяется знанию основных формул, по которым исчисляются проценты. Решение таких задач может быть сопряжено с большим вычислительным объёмом работы. Ученикам потребуются не только умения правильно анализировать задачу и составлять математическую модель, но и навыки сложных арифметических вычислений. В экономических задачах на оптимальный выбор требуется найти наилучшее решение из множества допустимых решений, то есть произвести оптимизацию. Здесь важную роль играет дифференциальное исчисление, так как с помощью производной функции можно находить наибольшее и наименьшее значения функции на промежутке. Анализ многих экономических задач приводит к составлению математической модели, в которой возможно применение производной. Решение задачи сводится к нахождению экстремума функции на заданном

промежутке, и такие задачи известны ученикам. Кроме этого, следует заметить, что многие экономические задачи на оптимизацию можно решать без привлечения дифференциального исчисления. Например, оценка эффективности принятого решения может быть осуществлена с помощью такого понятия, как доходность (эффективность). Существуют и другие типы экономических задач, в которых решение следует осуществлять по специальным алгоритмам. Модели экономических задач могут иметь специальный вид, что позволяет использовать тот или иной подход к решению. Например, задачи линейного программирования с экономическим содержанием можно решать, опираясь на сложный аппарат математического программирования; в простейших случаях допустимо решение с использованием лишь знаний школьного курса математики. В частности, умение решать системы линейных неравенств позволяет найти решение графическим методом задач линейного программирования с двумя переменными [1].

Понятие процента является одним из важнейших понятий школьного курса математики. Происхождение термина многие историки математики связывают с латинскими истоками – «pro centum» означает в переводе «сотая доля». Как экономическое понятие – это слово стали использовать в конце 19 века, и это слово стало означать выгоду, преимущество. В области финансов процент означает плату, которую одно юридическое или физическое лицо (определяемое как заёмщик) передаёт другому лицу (определяемому как кредитор). Эта плата предоставляется за услуги, связанные с временным пользованием денежными средствами, или как цена рентных доходов. При использовании термина «процент» финансисты имеют в виду также доходность ценных бумаг или акций.

В школьном курсе математики встречаются простейшие задачи с процентами нескольких видов:

1) Задачи, в которых необходимо найти указанный процент от числа.

Допустим, надо найти 20% от числа 400. Здесь можно использовать простейшие рассуждения: один процент от числа составляет одну сотую от заданного числа; значит, одному проценту соответствует величина, равная $\frac{400}{100} = 4$. Тогда 20% от числа 400 составляют величину, равную $20 \cdot 4 = 80$.

В общем случае, если требуется найти $p\%$ от числа a , то можно эту величину определить как $a \cdot \frac{p}{100}$. Например, 30% от числа 700 составляет

$$700 \cdot \frac{30}{100} = 210.$$

2) Задачи, в которых требуется найти процентное выражение одного числа от другого.

Пусть заданы два числа 200 и 160. Определим, сколько процентов составляет число 200 от 160. Проводим такие же рассуждения, что и выше: одному проценту от числа 160 соответствует величина, равная $\frac{160}{100} = 1,6$. Тогда числу 200 соответствует величина, равная $\frac{200}{1,6} = 125\%$. В общем случае,

чтобы определить, сколько процентов составляет число b от числа a , можно использовать выражение $\frac{b}{a} \cdot 100\%$. Поэтому число 200 составляет от числа 160 в процентном отношении величину, равную $\frac{200}{160} \cdot 100\% = 125\%$.

3) Задачи, в которых надо найти число, если заданы другое число и величина процентов от искомого числа.

Пусть задано некоторое число b и известно, что это число составляет $p\%$ от числа a . Тогда $\frac{b}{a} \cdot 100\% = p\%$. Значит, $a = b \cdot \frac{100\%}{p\%}$. Допустим, что число 600 составляет 80% от некоторого искомого числа a . Значит, $a = 600 \cdot \frac{100\%}{80\%} = 750$.

В школьных учебниках математики содержится большое количество задач с экономическим содержанием, в формулировках которых фигурируют проценты. Решение этих задач осуществляется с помощью простых математических выкладок с использованием минимума формул и приёмов [2]. Например, стандартные задачи, в которых стоимости товаров изменяются на некоторое число процентов, можно решать с помощью пропорций.

Задача. Прибыль предприятия составляет 150000 рублей в месяц. Определить величину прибыли, если она увеличилась на 8%.

Решение. Изначально прибыль составляла 150000 рублей, что соответствует процентной величине 100%. Так как прибыль увеличилась на 8%, то она стала составлять 108% от первоначальной прибыли. Величину соответствующей прибыли x (в рублях) мы можем найти из пропорции:

$$\frac{x}{150000} = \frac{108\%}{100\%} \Rightarrow x = \frac{150000 \cdot 108\%}{100\%} = 162000.$$

Ответ: 162000 рублей.

Задача. Костюм стоил 6000 рублей. После снижения цены он стал стоить 4920 рублей. На сколько процентов была снижена цена на костюм?

Решение. Составим пропорции:

$$\frac{6000}{4920} = \frac{100\%}{x\%} \Rightarrow x = \frac{4920 \cdot 100\%}{6000} = 82\%.$$

Следовательно, стоимость костюма после снижения составила 82% от первоначальной стоимости, и, значит, она снизилась на $100\% - 82\% = 18\%$.

Ответ: 18%.

Подобные несложные экономические задачи, содержащие процентные величины, содержатся и в контрольно-измерительных материалах ЕГЭ, а именно, в первой части в заданиях №1 или №11.

Задача. Клиент взял в банке кредит 60 000 рублей на год под 17% годовых. Он должен погашать кредит, внося в банк ежемесячно одинаковую сумму денег, и при этом через год должен выплатить всю сумму, взятую в кредит, вместе с процентами. Сколько рублей ежемесячно он должен вносить в банк?

Решение. Сначала выясним, какую сумму x клиент должен выплатить банку. Так как кредит был взят под 17% годовых, то общая сумма денег,

которые следует вернуть банку, составляет 117% от первоначальной суммы. Поэтому можно составить пропорции:

$$\frac{x}{60000} = \frac{117\%}{100\%} \Rightarrow x = \frac{60000 \cdot 117\%}{100\%} = 70200.$$

Значит, сумма возврата равна 70200 рублей. Так как клиент погашает кредит, внося в банк ежемесячно одинаковую сумму, то размер ежемесячной выплаты будет равен:

$$\frac{70200}{12} = 5850 \text{ рублей.}$$

Ответ: 5850 рублей.

Хотя эти задачи достаточно просто можно решить с помощью обычных пропорций или логических рассуждений, удобнее всё же применить простые формулы, по которым производятся расчёты величин. Здесь важнейшую роль играет формула:

$$S = S_0 \left(1 + \frac{p}{100}\right). \quad (1)$$

Эта формула связывает первоначальное значение S_0 , процентную ставку p за один расчётный период и конечное значение накопленной суммы S . Преимущество применения этой формулы по сравнению с пропорциями в том, что искомое значение можно находить путём подстановки и непосредственного вычисления по формуле. Это позволяет сократить процесс решения и избавиться от необходимости выполнения нескольких операций.

Формулу (1) можно обобщить на случай, когда проценты начисляются за несколько периодов. Пусть $p_1, p_2, \dots, p_n$ – процентные ставки за соответствующие периоды. Тогда накопленная сумма S_n за все периоды (в предположении, что никаких финансовых операций за эти периоды не выполняется) будет равна

$$S_n = S_0 \cdot \left(1 + \frac{p_1}{100}\right) \cdot \left(1 + \frac{p_2}{100}\right) \cdot \dots \cdot \left(1 + \frac{p_n}{100}\right).$$

В частности, при неизменной процентной ставке p накопленная сумма составит

$$S_n = S_0 \cdot \left(1 + \frac{p}{100}\right)^n.$$

Рассмотрим некоторые экономические задачи с процентами, решение которых основано на применении этих формул.

Задача. Акции некоторой компании подорожали в среду на некоторое число процентов, а в четверг подешевели на то же самое количество процентов. В результате они стали стоить на 4% дешевле, чем при открытии торгов в среду. На сколько процентов подорожали акции компании в среду?

Решение. Пусть S_0 – первоначальная цена акции перед открытием торгов в среду. Обозначим через p количество процентов, на которое подорожали акции в среду. Тогда цена акции после этого подорожания равна $S_0 \left(1 + \frac{p}{100}\right)$. После того, как в четверг акции подешевели на p процентов, их

стоимость составила $S_0 \left(1 + \frac{p}{100}\right) \left(1 - \frac{p}{100}\right)$. По условию задачи цена акции упала на 4% по сравнению с первоначальной ценой, поэтому их стоимость составила 96% от первоначальной цены. Следовательно, имеем соотношение:

$$S_0 \left(1 + \frac{p}{100}\right) \left(1 - \frac{p}{100}\right) = 0,96 S_0.$$

Решая это уравнение, получим:

$$\left(1 + \frac{p}{100}\right) \left(1 - \frac{p}{100}\right) = 0,96 \Rightarrow 1 - \frac{p^2}{10000} = 0,96 \Rightarrow p = 20.$$

Ответ: 20%.

Задача. Цена товара ежегодно уменьшалась на одно и то же число процентов от предыдущей цены. Определить, на сколько процентов уменьшалась ежегодно цена товара, если известно, что первоначальная цена товара, выставленного на продажу, составляла 19800 рублей, а через два года он был продан за 16038 рублей.

Решение. Обозначим через x число процентов, на которое уменьшалась цена товара ежегодно. Так как первоначальная цена была равна 19800 рублей, а после двукратного понижения на x процентов цена составила 16038 рублей, то имеем соотношение:

$$19800 \left(1 - \frac{x}{100}\right) \left(1 - \frac{x}{100}\right) = 16038.$$

Выполняя тождественные преобразования, имеем:

$$\begin{aligned} \left(1 - \frac{x}{100}\right)^2 &= \frac{16038}{19800} \Rightarrow \left(1 - \frac{x}{100}\right)^2 = 0,81 \Rightarrow \\ \Rightarrow 1 - \frac{x}{100} &= 0,9 \Rightarrow \frac{x}{100} = 0,1 \Rightarrow x = 10. \end{aligned}$$

Ответ: 10%.

Задача. Семья Петровых ежемесячно оплачивает услуги за ЖКХ, телефон и электроэнергию. Если бы услуги за ЖКХ подорожали на 50%, то общая сумма платежей увеличилась бы на 35%. Если бы электроэнергия подорожала на 50%, общая сумма платежей увеличилась бы на 10%. Определить, какой процент от общей суммы платежей приходится на телефон.

Решение. Пусть x, y, z – стоимости услуг за ЖКХ, телефон и электроэнергию соответственно. Общая сумма платежей равна $x + y + z$. Из условия задачи следует, что при подорожании услуг за ЖКХ на 50% общая сумма платежей увеличится на 35%. Значит, имеем соотношение

$$1,5x + y + z = 1,35(x + y + z).$$

Далее, при подорожании электроэнергии на 50% общая сумма платежей увеличится на 10%. Значит, выполняется равенство

$$x + y + 1,5z = 1,1(x + y + z).$$

Чтобы выяснить, какой процент от общей суммы платежей приходится на телефон, надо найти выражение

$$\frac{y}{x + y + z} \cdot 100\%.$$

Задачу можно решить алгебраически, рассматривая систему уравнений и выражая две переменные x, z через переменную y :

$$\begin{aligned} \begin{cases} 1,5x + y + z = 1,35(x + y + z) \\ x + y + 1,5z = 1,1(x + y + z) \end{cases} &\Rightarrow \begin{cases} 0,15x - 0,35y - 0,35z = 0 \\ -0,1x - 0,1y + 0,4z = 0 \end{cases} \Rightarrow \\ \Rightarrow \begin{cases} 15x - 35y - 35z = 0 \\ x + y - 4z = 0 \end{cases} &\Rightarrow \begin{cases} 3x - 7y - 7z = 0 \\ x + y - 4z = 0 \end{cases} \Rightarrow \\ \Rightarrow \begin{cases} 3x - 7y - 7z = 0 \\ x + y - 4z = 0 \end{cases} &\Rightarrow \begin{cases} 3(-y + 4z) - 7y - 7z = 0 \\ x = -y + 4z \end{cases} \Rightarrow \\ \Rightarrow \begin{cases} -10y + 5z = 0 \\ x = -y + 4z \end{cases} &\Rightarrow \begin{cases} z = 2y \\ x = -y + 4 \cdot 2y \end{cases} \Rightarrow \begin{cases} z = 2y \\ x = 7y \end{cases} \end{aligned}$$

Тогда получим:

$$\frac{y}{x + y + z} \cdot 100\% = \frac{y}{7y + y + 2y} \cdot 100\% = \frac{y}{10y} \cdot 100\% = 10\%.$$

Ответ: 10%.

Заметим, что эту задачу мы решили алгебраически, составляя математическую модель в виде системы уравнений. Но решение можно получить проще, основываясь на логических рассуждениях и применяя арифметический способ решения. Рассуждаем следующим образом. Повышение услуг ЖКХ на 50% приводит к увеличению общей суммы платежей на 35%. Следовательно, половина суммы за ЖКХ составляет 0,35 частей от общей суммы платежей, поэтому полная стоимость услуг за ЖКХ составит 0,7 доли суммарных платежей. Это означает, что услуги за ЖКХ составят 70% от общей суммы платежей. Аналогично, повышение услуг за электроэнергию на 50% приводит к увеличению общей суммы платежей на 10%. Следовательно, половина суммы за электроэнергию составляет 0,1 части от общей суммы платежей, поэтому полная стоимость услуг за электроэнергию составит 0,2 доли суммарных платежей. Это означает, что услуги за электроэнергию составят 20% от общей суммы платежей. Таким образом, на долю услуг за телефон приходится $100\% - (70\% + 20\%) = 10\%$.

Экономические задачи - это задачи, связанные с финансовой деятельностью, и, именно поэтому они есть в школьном курсе.

Ученик должен иметь представление не только о финансах, но и о грамотной их растрате. Это нужно, чтобы в последующем правильно управлять личными финансами, понимать, что такое банковское дело и инвестиции в финансовом рынке, разбираться в вопросах страхования и различать мошенничество и финансовые пирамиды, которые на Российском рынке эксперты оценивают порядком 120, действующих в Российской Федерации.

Развитие школьного финансового образования так же необходима, как трактовка проблем его содержания [3].

Если ученик сможет говорить с преподавателем «на одном языке», то есть понимать его мысли и правильно отвечать на вопросы, то и наиболее эффективнее закрепятся его знания. При взаимопонимании учитель старается

разбирать большинство тех задач, которые остались непонятными или неудачно раскрытыми.

Следовательно, предпочтительно смотреть на данную тему ежедневно, принимая во внимание, что такие задачи есть в повседневной жизни.

Список литературы

1. Колобов А.Н., Особенности изучения задач с экономическим содержанием в школьном курсе математики. / А.Н. Колобов, И.В. Прояева // Мир науки, культуры, образования. Международный научный журнал. - 2019 г.- №3.- С.175-176.

2. Колобов А.Н., Математический кружок как форма развития интереса обучающихся к математике. / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1863-1866.

3. Колобов А.Н., Роль текстовых задач в математическом образовании. / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1867-1871.

ЭКОНОМИЧЕСКИЕ ЗАДАЧИ С РАЗЛИЧНЫМИ ВИДАМИ ВЫПЛАТ В МАТЕМАТИКЕ

Колобов А.Н., канд. техн. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
педагогический университет»

Экономические задачи повышенной сложности, связанные с процентными величинами, встречаются в заданиях №17 второй части ЕГЭ по математике. Эти задачи рассматриваются как задачи с кредитами, выплатами, вкладами, причём погашение кредитов (или начисление вкладов) происходит на протяжении нескольких периодов, после каждого из которых изменяются значения накопленной суммы и возможны финансовые операции в виде внесения или изъятия некоторой части денежных средств. Решения этих задач описываются как последовательные результаты финансовых операций, и необходимо провести анализ и промежуточные расчёты в связи с изменениями параметров задачи после каждого периода времени. В подавляющем большинстве случаев необходимо построение математической модели рассматриваемой экономической задачи. Модель может иметь сложный вид и представлять собой уравнение или систему уравнений, неравенство или систему неравенств, а также могут содержаться ограничения всевозможного вида. Перейдём к рассмотрению подобных задач [1].

Задача [С – Я]. 31 декабря 2017 года Василий взял в банке 5460000 рублей в кредит под 20% годовых. Схема выплаты кредита следующая: 31 декабря каждого следующего года банк начисляет проценты на оставшуюся сумму долга (то есть увеличивает долг на 20% процентов), затем Василий переводит в банк X рублей. Какой должна быть величина X , чтобы Василий выплатил долг тремя равными платежами?

Решение. По условию имеем: $S_0 = 5460000$ – начальная сумма долга, то есть сумма, взятая в кредит; $p = 20\%$ – годовая процентная ставка. Рассмотрим величину $q = 1 + \frac{p}{100} = 1,2$. Тогда математическая модель задачи имеет вид:

$$((S_0 \cdot q - X) \cdot q - X) \cdot q - X = 0$$

Преобразуем уравнение и выразим переменную X :

$$S_0 q^3 - Xq^2 - Xq - X = 0 \Rightarrow S_0 q^3 = X(q^2 + q + 1) \Rightarrow \\ \Rightarrow X = \frac{S_0 q^3}{q^2 + q + 1}.$$

Подставив исходные значения, заданные в условии задачи, получим:

$$X = \frac{5460000 \cdot 1,2^3}{1,2^2 + 1,2 + 1} = 2592000.$$

Ответ: 2592000 рублей.

Задача. 31 декабря 2017 года Дмитрий взял в банке 7007000 рублей в кредит под 20% годовых. Схема выплаты кредита следующая: 31 декабря каждого следующего года банк начисляет проценты на оставшуюся сумму долга, затем Дмитрий переводит в банк платёж. Весь долг был выплачен тремя равными платежами. На сколько рублей меньше было бы отдано банку, если бы Дмитрий смог выплатить долг двумя равными платежами?

Решение. По условию имеем: $S_0 = 7007000$ – начальная сумма долга, то есть сумма, взятая в кредит; $p = 20\%$ – годовая процентная ставка. Рассмотрим величину $q = 1 + \frac{p}{100} = 1,2$. Обозначим через X размер выплаты в случае, когда долг выплачивается тремя равными платежами. Математическая модель задачи имеет вид:

$$((S_0 \cdot q - X) \cdot q - X) \cdot q - X = 0$$

Преобразовав уравнение, выразим неизвестное X :

$$S_0 q^3 - Xq^2 - Xq - X = 0$$

$$X = \frac{S_0 q^3}{q^2 + q + 1}$$

Подставив исходные значения, заданные в условии задачи, получим:

$$X = \frac{7007000 \cdot 1,2^3}{1,2^2 + 1,2 + 1} = 3326400.$$

Так как размер одной выплаты равен 3326400 рублей, а было произведено три равные выплаты, то общая сумма выплат равна: $3326400 \cdot 3 = 9979200$ рублей.

Рассмотрим случай, когда долг выплачивается двумя равными платежами. Обозначим через Y размер выплаты. Тогда математическая модель задачи имеет вид:

$$(S_0 q - Y)q - Y = 0$$

Преобразовав уравнение, выразим неизвестное Y :

$$S_0 q^2 - Yq - Y = 0$$

$$Y = \frac{S_0 q^2}{q + 1}$$

Подставив исходные значения, заданные в условии задачи, получим:

$$Y = \frac{7007000 \cdot 1,2^2}{1,2 + 1} = 4586400.$$

Так как размер одной выплаты равен 4586400 рублей, а было произведено две равные выплаты, то общая сумма выплат равна: $4586400 \cdot 2 = 9172800$ рублей.

Следовательно, во втором случае суммарные выплаты будут меньше на величину, равную $9979200 - 9172800 = 806400$ рублей.

Ответ: 806400 рублей.

В рассмотренных задачах предполагается, что выплаты производятся равными платежами, и это обстоятельство позволяет использовать удобную для расчётов формулу:

$$S_0 q^n = X(q^{n-1} + q^{n-2} + \dots + q + 1)$$

Но во многих задачах размеры выплат могут различаться по различным периодам, и тогда для подобных случаев требуется составлять математические модели, проводя логические рассуждения. В результате также получается уравнение, решив которое, можно найти неизвестную величину. Приведём пример.

Задача. Дмитрий взял кредит в банке на сумму 270200 рублей. Схема выплаты кредита следующая: в конце каждого года банк увеличивает на 10 процентов оставшуюся сумму долга, а затем Дмитрий переводит в банк свой очередной платёж. Известно, что Дмитрий погасил кредит за три года, причем каждый его следующий платёж был ровно втрое больше предыдущего. Какую сумму Дмитрий заплатил в первый раз?

Решение. По условию имеем: $S_0 = 270200$ – начальная сумма долга, то есть сумма, взятая в кредит; $p = 10\%$ – годовая процентная ставка. Рассмотрим величину $q = 1 + \frac{p}{100} = 1,1$. Обозначим через X размер первого платежа, тогда, исходя из условий задачи, второй платёж составит величину $3X$, а третий платёж будет равен $9X$, в результате выплат этих платежей долг будет погашен. Следовательно, математическая модель задачи имеет вид:

$$((S_0 \cdot q - X) \cdot q - 3X) \cdot q - 9X = 0$$

Преобразовав уравнение, выразим неизвестное X :

$$S_0 q^3 - Xq^2 - 3Xq - 9X = 0 \Rightarrow S_0 q^3 = X(q^2 + 3q + 9) \Rightarrow$$

$$X = \frac{S_0 q^3}{q^2 + 3q + 9}.$$

Подставив исходные значения, заданные в условии задачи, получим:

$$X = \frac{270200 \cdot 1,1^3}{1,1^2 + 3 \cdot 1,1 + 9} = 26620.$$

Ответ: 26620 рублей.

В некоторых задачах на банковские проценты математические модели могут быть достаточно сложными, и представлять собой, в частности, системы уравнений.

Задача. 31 декабря 2018 года Алексей взял в банке некоторую сумму в кредит под некоторый процент годовых. Схема выплаты кредита следующая: 31 декабря каждого следующего года банк начисляет проценты на оставшуюся сумму долга (то есть увеличивает долг на $p\%$), а затем Алексей переводит очередной транш (то есть производит выплату). Если он будет платить каждый год по 2073600 рублей, то выплатит долг за 4 года. Если же будет платить по 3513600 рублей, то выплатит долг за 2 года. Под какой процент Алексей взял деньги в кредит?

Решение. Обозначим через S_0 – сумму, взятую в кредит. Пусть $p\%$ – годовая процентная ставка. Положим $q = 1 + \frac{p}{100}$. Для удобства расчётов и анализа задачи введём обозначения заданных в условии выплат: $X_1 = 2073600$; $X_2 = 3513600$. Известно из условий задачи, что если

выплачивать ежегодно платёж в размере X_1 , то долг будет погашен за 4 года. Следовательно, имеем уравнение:

$$\left(((S_0 q - X_1)q - X_1)q - X_1 \right) q - X_1 = 0. \quad (*)$$

Преобразуем это уравнение и запишем в следующем виде:

$$S_0 q^4 - X_1 q^3 - X_1 q^2 - X_1 q - X_1 = 0.$$

Если выплачивать ежегодно платёж в размере X_2 , то долг будет погашен за 2 года. Следовательно, имеем уравнение:

$$(S_0 q - X_2)q - X_2 = 0. \quad (**)$$

Преобразовав уравнение, получим:

$$S_0 q^2 - X_2 q - X_2 = 0.$$

Математическая модель задачи представляет собой систему двух уравнений с двумя переменными:

$$\begin{cases} S_0 q^4 - X_1 q^3 - X_1 q^2 - X_1 q - X_1 = 0 \\ S_0 q^2 - X_2 q - X_2 = 0 \end{cases}$$

Эта система содержит две переменные S_0 и q . Выразим из второго уравнения неизвестное S_0 :

$$S_0 = \frac{X_2(q+1)}{q^2}.$$

Подставим это выражение в первое уравнение:

$$\begin{aligned} \frac{X_2(q+1)}{q^2} q^4 - X_1 q^3 - X_1 q^2 - X_1 q - X_1 &= 0 \Rightarrow \\ \Rightarrow X_2(q+1)q^2 - X_1(q^3 + q^2 + q + 1) &= 0 \Rightarrow \\ \Rightarrow X_2(q+1)q^2 = X_1(q^3 + q^2 + q + 1) &\Rightarrow \\ \Rightarrow X_2(q+1)q^2 = X_1(q^2 + 1)(q+1) &\Rightarrow \\ \Rightarrow X_2 q^2 = X_1(q^2 + 1) \Rightarrow X_2 q^2 - X_1 q^2 - X_1 &= 0 \Rightarrow \\ \Rightarrow (X_2 - X_1)q^2 = X_1 \Rightarrow q^2 = \frac{X_1}{X_2 - X_1}. \end{aligned}$$

Подставив известные значения $X_1 = 2073600, X_2 = 3513600$, получим:

$$q^2 = \frac{2073600}{3513600 - 2073600} = 1,44.$$

Следовательно, $\begin{cases} q = 1,2 \\ q = -1,2 \end{cases}$. Учитывая, что значение q должно быть

положительным, получим $q = 1,2$. Тогда $1 + \frac{p}{100} = 1,2 \Rightarrow p = 20$.

Ответ: 20%.

Перейдём к рассмотрению задач с дифференцированными платежами. Они отличаются от предыдущих задач тем, что сами платежи не указаны, и их размеры не определены. Составление модели задачи происходит исходя из специальных условий относительно размеров долга после выплат за каждый период времени. Например, погашение кредита может происходить так, что размеры основного долга после каждого периода понижаются равномерно [2].

Задача. Василий взял в банке кредит в размере 10000 рублей на срок 5 месяцев. По договору он должен вносить в банк часть денег в конце каждого

месяца. В начале каждого месяца общая сумма долга возрастает на 10%, а затем уменьшается на сумму, уплаченную Василием банку в конце месяца. Суммы, выплачиваемые Василием, подбираются так, чтобы сумма долга уменьшалась равномерно, то есть на одну и ту же величину каждый месяц. Какую сумму Василий выплатит банку в течение всего срока кредитования?

Решение. Из условия задачи вытекает, что погашение долга должно происходить так, чтобы каждый месяц основной долг понижался равномерно на одну и ту же величину. Так как кредит должен погашаться в течение 5 месяцев, то в конце каждого месяца основной долг должен понижаться на 2000 рублей. В начале первого месяца после взятия кредита накопленный долг составит величину, равную $10000 \cdot \left(1 + \frac{10}{100}\right) = 10000 \cdot 1,1 = 11000$ рублей, а в конце этого месяца долг должен быть $10000 - 2000 = 8000$ рублей. Следовательно, выплата за первый месяц составит $11000 - 8000 = 3000$ рублей.

Аналогично, в начале второго месяца долг составит $8000 \cdot 1,1 = 8800$ рублей, а в конце второго месяца долг должен остаться в размере $8000 - 2000 = 6000$ рублей. Выплата за второй месяц составит $8800 - 6000 = 2800$ рублей.

Проводя такие же рассуждения, получим:

В начале третьего месяца долг составит $6000 \cdot 1,1 = 6600$ рублей, а в конце третьего месяца долг должен остаться в размере $6000 - 2000 = 4000$ рублей. Выплата за третий месяц составит $6600 - 4000 = 2600$ рублей.

В начале четвёртого месяца долг составит $4000 \cdot 1,1 = 4400$ рублей, а в конце четвёртого месяца долг должен остаться в размере $4000 - 2000 = 2000$ рублей. Выплата за четвёртый месяц составит $4400 - 2000 = 2400$ рублей.

Наконец, в начале пятого месяца долг составит $2000 \cdot 1,1 = 2200$ рублей, а в конце пятого месяца долг должен быть в размере $2000 - 2000 = 0$ рублей, то есть он должен быть полностью погашен. Выплата за последний месяц составит 2200 рублей.

Таким образом, в течение всего срока кредитования банку будет выплачена сумма, равная сумме ежемесячных платежей:

$$3000 + 2800 + 2600 + 2400 + 2200 = 13000 \text{ рублей.}$$

Ответ: 13000 рублей.

В рассмотренной задаче мы по каждому месяцу определяли размер платежа, исходя из условия равномерного погашения долга. Процесс решения подобным образом может сильно усложняться, если кредит берётся на большое количество месяцев. Для упрощения расчётов и уменьшения громоздкости рассуждений предложим решение с помощью расчётной таблицы следующего вида:

Период (месяц)	Долг до выплаты	Долг после выплаты	Выплата
1	$10000 \cdot 1,1 = 11000$	8000	$11000 - 8000 = 3000$
2	$8000 \cdot 1,1 = 8800$	6000	$8800 - 6000 = 2800$

3	$6000 \cdot 1,1 = 6600$	4000	$6600 - 4000 = 2600$
4	$4000 \cdot 1,1 = 4400$	2000	$4400 - 2000 = 2400$
5	$2000 \cdot 1,1 = 2200$	0	$2200 - 0 = 2200$

Тогда из последнего столбца, сложив все найденные значения, получим искомый результат.

Решение банковских задач с дифференцированными платежами удобно проводить не в алгебраической форме, как показано в вышерассмотренном примере, а описывая выражение для суммы выплат в общем виде и устанавливая закономерности, проявляющиеся при нахождении искомой величины[3]. Приведём для наглядности следующий пример.

Задача. 15-го января планируется взять кредит в банке на 18 месяцев. Условия его возврата таковы:

- 1-го числа каждого месяца долг возрастает на 2% по сравнению с концом предыдущего месяца;
- со 2-го по 14-е число каждого месяца необходимо выплатить часть долга;
- 15-го числа каждого месяца долг должен быть на одну и ту же величину меньше долга на 15-е число предыдущего месяца.

Сколько процентов от суммы кредита составляет общая сумма денег, которую нужно выплатить банку за весь срок кредитования?

Решение. Обозначим через S_0 начальную сумму, то есть сумму, взятую в кредит. По условию задачи месячная процентная ставка составляет 2%, поэтому положим $q = 1 + \frac{p}{100} = 1 + \frac{2}{100} = 1,02$. Кроме того, долг по условию понижается равномерно, после каждого месяца на величину, равную $\frac{1}{18}$ части основного долга. Составим расчётную таблицу:

Долг (месяц)	Сумма долга до выплаты	Сумма долга после выплаты
1	$S_0 q$	$\frac{17}{18} S_0$
2	$\frac{17}{18} S_0 q$	$\frac{16}{18} S_0$
3	$\frac{16}{18} S_0 q$	$\frac{15}{18} S_0$
...	...	...
16	$\frac{3}{18} S_0 q$	$\frac{2}{18} S_0$
17	$\frac{2}{18} S_0 q$	$\frac{1}{18} S_0$
18	$\frac{1}{18} S_0 q$	0

Общая сумма денег, которую нужно вернуть банку за весь срок кредитования, равна сумме ежемесячных выплат, то есть она определяется как сумма разностей значений долга до выплат и значений после выплат по

каждой строке. Очевидно, что такой способ подсчёта является очень громоздким. И здесь эффективным методом решения является следующий метод, основанный на том, что сумма разностей элементов второго и третьего столбцов равна разности между суммой всех элементов второго столбца и суммой всех элементов третьего столбца. Учитывая, что соответствующие столбцы имеют общие множители, выражение для конечной суммы выплат может быть записано в достаточно компактной форме. В нашем случае общая сумма платежей представляет собой выражение:

$$S = S_0 q \left(1 + \frac{17}{18} + \frac{16}{18} + \dots + \frac{3}{18} + \frac{2}{18} + \frac{1}{18} \right) - S_0 \left(\frac{17}{18} + \frac{16}{18} + \frac{15}{18} \dots + \frac{2}{18} + \frac{1}{18} \right).$$

Преобразуем это выражение:

$$S = S_0 q \frac{18 + 17 + 16 + \dots + 3 + 2 + 1}{18} - S_0 \frac{17 + 16 + \dots + 2 + 1}{18}.$$

$$S = S_0 q \frac{1}{18} (18 + 17 + 16 + \dots + 3 + 2 + 1) - S_0 \frac{1}{18} (17 + 16 + \dots + 2 + 1).$$

Выражения в скобках представляют собой сумму членов арифметической прогрессии, и для вычисления значений выражений в этих скобках воспользуемся формулой суммы n первых членов арифметической прогрессии:

$$S_n = \frac{a_1 + a_n}{2} \cdot n$$

Здесь n – число членов; a_1 и a_n – первый и последний члены арифметической прогрессии. Применив эту формулу, запишем выражение для суммы выплат:

$$S = S_0 q \frac{1}{18} \cdot \frac{18 + 1}{2} \cdot 18 - S_0 \frac{1}{18} \cdot \frac{17 + 1}{2} \cdot 17$$

Упростим это выражение:

$$S = S_0 q \cdot \frac{19}{2} - S_0 \cdot \frac{17}{2} = S_0 \left(\frac{19}{2} q - \frac{17}{2} \right).$$

Подставляя значение $q = 1,02$, получим:

$$S = S_0 \cdot \left(\frac{19}{2} \cdot 1,02 - \frac{17}{2} \right) = S_0 \cdot 1,19.$$

Это означает, что общая сумма выплат в 1,19 раз превышает сумму, взятую в кредит. То есть общая сумма денег, которую нужно выплатить банку за весь срок кредитования, составляет 119 процентов от суммы кредита.

Ответ: 119 %.

Задачи с дифференцированными платежами, в которых погашение кредита происходит в соответствии с условиями предыдущей задачи (то есть после каждого периода основной долг уменьшается равномерно) встречаются очень часто в материалах ЕГЭ. Могут быть некоторые различия в постановке задачи. Но тем не менее можно использовать алгоритм решения, основанный на применении расчётной таблицы, предложенный в предыдущем примере.

Список литературы

1. Колобов А.Н., Особенности изучения задач с экономическим содержанием в школьном курсе математики. / А.Н. Колобов, И.В. Прояева // Мир науки, культуры, образования. Международный научный журнал. - 2019 г.- №3.- С.175-176.

2. Колобов А.Н., Математический кружок как форма развития интереса обучающихся к математике. / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1863-1866.

3. Колобов А.Н., Факультативные курсы по математике как форма развития математических способностей / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1872-1876.

ЭЛЕМЕНТЫ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ И ДИФФЕРЕНЦИАЛЬНОГО ИСЧИСЛЕНИЯ ПРИ РЕШЕНИИ ЭКОНОМИЧЕСКИХ ЗАДАЧ В МАТЕМАТИКЕ

Колобов А.Н., канд. техн. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
педагогический университет»

Для решения многих экономических задач можно применять элементы дифференциального исчисления. Это те задачи, в которых анализ приводит к необходимости составления математической модели, в которой требуется найти оптимальное значение некоторой функции при наличии ограничений на переменные. При этом исследуемая функция должна быть дифференцируемой. Как известно из школьных учебников математики старших классов, если функция одной переменной является дифференцируемой на некотором промежутке, то задача сводится к нахождению наибольшего (или наименьшего) значения функции, и решение задачи осуществляется с помощью методов дифференциального исчисления. Подобные задачи входят в блок заданий №17 профильного уровня ЕГЭ. Рассмотрим некоторые из них[1].

Пример 1 [*]. У фермера есть два поля, каждое площадью 10 гектаров. На каждом поле можно выращивать картофель и свеклу, поля можно делить между этими культурами в любой пропорции. Урожайность картофеля на первом поле составляет 400 ц/га, а на втором - 300 ц/га. Урожайность свеклы на первом поле составляет 300 ц/га, а на втором – 400 ц/га. Фермер может продавать картофель по цене 5000 рублей за центнер, а свеклу – по цене 6000 рублей за центнер. Какой наибольший доход может получить фермер?

Решение. Проанализируем сначала, влияет ли структура посева на одном поле на то, каким образом будет засеиваться другое поле. Из условий задачи очевидно, что прямой связи между полями нет. Значит, доход, получаемый фермером на каждом поле, не зависит от дохода, получаемого на другом поле. Поэтому можно рассмотреть для каждого поля в отдельности наибольший возможный доход, и полученные значения сложить.

Приступим к построению математической модели задачи. Введём в рассмотрение некоторую переменную x – площадь первого поля, засеянного картофелем; тогда $(10 - x)$ – площадь, засеянная свеклой на первом поле (эти площади измеряются в гектарах). Значит, доход, полученный фермером на первом поле, будет равен

$$\begin{aligned} F(x) &= x \cdot 400 \cdot 5000 + (10 - x) \cdot 300 \cdot 6000 = \\ &= 2000000x + 18000000 - 1800000x = 200000x + 18000000; x \in [0; 10]. \end{aligned}$$

Продифференцируем функцию:

$$F'(x) = 200000 > 0, \forall x \in [0; 10].$$

Так как производная на всём промежутке положительна, то функция возрастает, следовательно, наибольшее значение достигается на правом конце отрезка, то есть в точке $x = 10$: $F_{\text{наиб}} = F(10) = 20000000$.

Аналогично, введём в рассмотрение переменную y – площадь второго поля, засеянного картофелем; тогда $(10 - y)$ – площадь, засеянная свеклой на втором поле. Значит, доход, полученный фермером на втором поле, будет равен

$$F(y) = y \cdot 300 \cdot 5000 + (10 - y) \cdot 400 \cdot 6000 = \\ = 1500000y + 24000000 - 2400000y = -900000y + 24000000, y \in [0; 10].$$

Производная функции имеет вид: $F'(y) = -900000 < 0; \forall y \in [0; 10]$.

Так как производная на всём промежутке отрицательна, то функция убывает, следовательно, наибольшее значение достигается на левом конце отрезка, то есть в точке $x = 0$: $F_{\text{наиб}} = F(0) = 24000000$.

Итак, суммарный доход фермера будет равен сумме значений дохода на двух полях: $F_{\text{наиб}} = 20000000 + 24000000 = 44000000$.

Ответ: 44000000 рублей - наибольший доход, который получит фермер.

Пример 2 [*]. В бассейне проведены три трубы. Первая труба наливает 40 м^3 воды в час, вторая труба наливает в час на $2k \text{ м}^3$ меньше, чем первая ($0 < k < 20$), третья труба наливает в час на $10k \text{ м}^3$ больше первой. Сначала первая и вторая трубы, работая вместе, наливают $0,2$ части бассейна, а затем все три трубы, работая вместе, наливают оставшиеся 80% бассейна. При каком значении k бассейн быстрее всего наполнится указанным способом?

Решение. Пусть для определённости объём бассейна равен единице. По условию первая труба наливает 40 м^3 воды в час, вторая труба - $(40 - 2k) \text{ м}^3$, а третья - $(40 + 10k) \text{ м}^3$. Работая вместе, первая и вторая трубы наливают $(40 + 40 - 2k) = (80 - 2k) \text{ м}^3$ воды в час. Работая вместе, все три трубы наливают $40 + (40 - 2k) + (40 + 10k) \text{ м}^3 = (120 + 8k) \text{ м}^3$ воды в час. Первая и вторая трубы наливают $0,2$ части бассейна, и, работая вместе, они затратят $\frac{0,2}{80-2k}$ часов. Так как 80% составляет $0,8$ части бассейна, то оставшиеся $0,8$ части бассейна три трубы, работая вместе, заполнят за $\frac{0,8}{120+8k}$ часов.

Весь бассейн будет наполнен за $\left(\frac{0,2}{80-2k} + \frac{0,8}{120+8k}\right)$ часов.

Задача сводится к нахождению такого значения k , при котором значение функции $t(k) = \frac{0,2}{80-2k} + \frac{0,8}{120+8k}$, ($0 < k < 20$) будет наименьшим. Исследуем функцию и найдём стационарную точку:

$$t'(k) = \frac{0,4}{(80-2k)^2} - \frac{6,4}{(120+8k)^2} = \frac{0,4 \cdot (120+8k)^2 - 6,4 \cdot (80-2k)^2}{(80-2k)^2 \cdot (120+8k)^2}.$$

$$t'(k) = 0 \Rightarrow \begin{cases} 0,4 \cdot (120 + 8k)^2 - 6,4 \cdot (80 - 2k)^2 = 0, \\ 80 - 2k \neq 0, \\ 120 + 8k \neq 0, \\ 0 < k < 20 \end{cases}$$

$$(120 + 8k)^2 - 16 \cdot (80 - 2k)^2 = 0 \Rightarrow$$

$$\Rightarrow 14400 + 1920k + 64k^2 - 102400 + 5120k - 64k^2 = 0 \Rightarrow$$

$$\Rightarrow 7040k = 88000 \Rightarrow k = 12,5; 12,5 \in (0; 20).$$

Данная стационарная точка является внутренней точкой промежутка; найдём знаки производной на интервалах. Получим следующее:

$$t'(k) < 0 \text{ при } k < 12,5 \text{ и } t'(k) > 0 \text{ при } k > 12,5, \text{ значит, } k = 12,5 -$$

точка минимума функции $t(k)$. Так как функция имеет на промежутке единственную точку минимума, то в ней она принимает своё наименьшее значение. Таким образом, быстрее всего бассейн наполнится при $k = 12,5$.

Ответ: При $k = 12,5$ бассейн наполнится быстрее всего.

Пример 28. Алексей является владельцем двух заводов в разных городах. На заводах производятся абсолютно одинаковые приборы. Если рабочие на одном из заводов трудятся суммарно t^2 часов в неделю, то за эту неделю они производят t единиц товара. За каждый час работы на заводе, расположенном в первом городе, Алексей платит рабочему 250 рублей, а на заводе, расположенном во втором городе, - 200 рублей. На оплату труда рабочих планируется выделять 900000 рублей в неделю. Какое наибольшее количество приборов можно произвести за неделю на этих двух заводах?

Решение. Обозначим через x и y количества приборов, которые производятся на первом и втором заводах соответственно. Тогда выражение $F(x; y) = x + y$ означает общее количество производимых за неделю приборов. Для их производства требуется количество времени, равное $x^2 + y^2$ часов. С учётом того, что производится оплата за каждый час работы на каждом заводе, нужно выделить $250x^2 + 200y^2$ рублей, и по условию максимальное количество выделяемых финансов составляет 900000 рублей. Итак, имеем ограничение $250x^2 + 200y^2 = 900000$. Аналогично, как и в предыдущих примерах, выразим одну переменную через другую. Например, выразим переменную y :

$$200y^2 = 900000 - 250x^2 \Rightarrow y^2 = 4500 - 1,25x^2 \Rightarrow y = \sqrt{4500 - 1,25x^2}.$$

Подставив это равенство в выражение $F(x; y)$, получим функцию одной переменной:

$$f(x) = x + \sqrt{4500 - 1,25x^2}; x \in [0; 360].$$

Продифференцировав функцию и приравняв к нулю, найдём стационарную точку $x = 40$, которая является внутренней точкой промежутка; аналогично показывается, что она является точкой максимума, и в ней функция принимает наибольшее значение. Следовательно,

$$f_{\text{наиб}} = f(40) = 40 + \sqrt{4500 - 1,25 \cdot 40^2} = 40 + 50 = 90.$$

Ответ: Наибольшее количество производимых приборов составляет 90 единиц.

Задача. Анатолий является владельцем двух заводов в разных городах. Допустим, что на этих заводах производятся абсолютно одинаковые приборы, но на втором заводе используется более совершенное технологическое оборудование. В результате, если рабочие на заводе, расположенном в первом городе, трудятся суммарно $4t^3$ часов в неделю, то за эту неделю они производят t приборов; если рабочие на заводе, расположенном во втором городе, трудятся суммарно t^3 часов в неделю, то они производят t приборов.

За каждый час работы на каждом из заводов Анатолий платит рабочему 1000 рублей. За неделю по плану необходимо произвести 20 приборов. Какую наименьшую сумму придётся потратить владельцу заводов еженедельно на оплату труда рабочих?

Решение. Составим математическую модель задачи. Введём переменную x – число приборов, производимых на первом заводе. Тогда, исходя из условий задачи, на втором заводе необходимо произвести $20 - x$ приборов. Для производства x приборов на первом заводе потребуется $4x^3$ часов, а для производства $(20 - x)$ приборов на втором заводе потребуется $(20 - x)^3$ часов. И так как за каждый час работы выплачивается 1000 рублей, то суммарные выплаты для производства всех приборов определяются выражением:

$$f(x) = 1000 \cdot 4x^3 + 1000(20 - x)^3.$$

Учитывая, что $x \in [0; 20]$, получим задачу условной оптимизации, представляющую собой задачу нахождения наибольшего значения функции на заданном отрезке.

Продифференцируем функцию $f(x)$ и найдём стационарные точки.

$$f'(x) = 1000(12x^2 + 3(20 - x)^2 \cdot (-1)) = 1000(12x^2 - 3(20 - x)^2) = \\ = 1000(12x^2 - 1200 + 120x - 3x^2) = 1000(9x^2 + 120x - 1200).$$

$$f'(x) = 0 \Rightarrow 9x^2 + 120x - 1200 = 0 \Rightarrow \begin{cases} x = \frac{20}{3} \\ x = -20 \end{cases}.$$

Значение $x = -20$ не удовлетворяет условию задачи, и его можно не рассматривать. Значение $x = \frac{20}{3} \in [0; 20]$. Проверкой выявляем, что эта точка является точкой минимума, значит, в ней функция принимает наименьшее значение. Но значение x должно быть целым по условию, поэтому найденное значение $x = \frac{20}{3} = 6\frac{2}{3}$ не подходит. Поэтому функция будет принимать своё наименьшее значение в одной из двух точек, соответствующих целым числам: либо в точке $x = 6$, либо в точке $x = 7$. Сравним значения функции в этих точках:

$$f(6) = 1000 \cdot 4 \cdot 6^3 + 1000(20 - 6)^3 = 864000 + 2744000 = 3608000;$$

$$f(7) = 1000 \cdot 4 \cdot 7^3 + 1000(20 - 7)^3 = 1372000 + 2197000 = 3569000.$$

Сравнивая эти значения, выбираем наименьшее, то есть $f(7) = 3569000$. Следовательно, на первом заводе должно выпускаться 7 приборов, а на втором – 13 приборов; при этом выплаченная за неделю сумма окажется наименьшей и составит 3569000 рублей.

Ответ: 3569000 рублей.

Рассмотрим экономические задачи, в том числе на оптимизацию, которые могут быть решены без привлечения дифференциального исчисления или некоторого другого сложного математического аппарата. Для обоснования метода решения введём понятие «доходности». Доходность характеризует эффективность вкладываемых ресурсов на единицу некоторой меры [2]. Допустим, что предприниматель купил две квартиры для сдачи в аренду. Однокомнатную квартиру он приобрёл за 1 млн. рублей и сдаёт в аренду за 10000 рублей в месяц, а двухкомнатную квартиру купил за 2 млн. рублей и сдаёт в аренду за 15000 рублей в месяц. Очевидно, что прибыль в абсолютном исчислении от двухкомнатной квартиры выше на 5000 рублей, но эффективность вложений в однокомнатную квартиру выше. Действительно, потратив 1 млн. рублей, ежемесячно будем получать 10000 рублей; то есть каждый вложенный рубль в однокомнатную квартиру приносит ежемесячно $\frac{10000}{1000000} \cdot 100\% = 1\%$ прибыли. Эта величина и характеризует доходность вкладываемых ресурсов. Потратив 2 млн. рублей на двухкомнатную квартиру, ежемесячно получаем прибыль 15000 рублей; то есть каждый вложенный рубль приносит ежемесячно $\frac{15000}{2000000} \cdot 100\% = 0,75\%$ прибыли. Этот пример показывает различие между понятиями «доход» (прибыль) и «доходность». Доходность может определяться по отношению к единице ресурсов (это могут быть или финансовые ресурсы, или материальные ресурсы в другом исчислении); к единице времени, затрачиваемой для выпуска продукции; к единице производственных мощностей и т.п.

Отметим, что в некоторых случаях задачи, решение которых может быть получено методами дифференциального исчисления, могут быть решены и с привлечением понятия доходности. Рассмотрим разобранный выше пример 1.

Определим доходность каждой засеиваемой культуры на каждом поле в отдельности на единицу площади. На первом поле каждый гектар площади, засеиваемой картофелем, приносит 400 центнеров, в денежном эквиваленте мы получим $400 \cdot 5000 = 2000000$ рублей. Каждый гектар площади, засеиваемой свеклой, приносит 300 центнеров, и в денежном эквиваленте это составит $300 \cdot 6000 = 1800000$ рублей. Таким образом, каждый гектар на первом поле приносит больше дохода, если площадь засеивается картофелем. Следовательно, для получения максимальной прибыли первое поле нужно засеять только картофелем. Площадь первого поля составляет 10 га, значит, прибыль составит $10 \cdot 2000000 = 20000000$ рублей.

Рассмотрим теперь второе поле и проведём аналогичные рассуждения. На этом поле каждый гектар площади, засеиваемой картофелем, приносит 300 центнеров, в денежном эквиваленте мы получим $300 \cdot 5000 = 1500000$ рублей. Каждый гектар площади, засеиваемой свеклой, приносит 400 центнеров, и в денежном эквиваленте это составит $400 \cdot 6000 = 2400000$ рублей. Таким образом, каждый гектар на втором поле приносит больше дохода, если вся площадь засеивается свеклой. Следовательно, для получения максимальной прибыли второе поле нужно засеять только свеклой. Площадь второго поля составляет 10 га, значит, прибыль составит $10 \cdot 2400000 = 24000000$ рублей. Тогда суммарный доход фермера составит $20000000 + 24000000 = 44000000$ рублей.

Заметим, что метод решения, основанный на понятии доходности, существенно проще, чем в случае, когда используется дифференциальное исчисление. Но есть определённый недостаток, состоящий в отсутствии математической модели рассматриваемой задачи. Но многие оптимизационные задачи с экономическим содержанием в школьном курсе математики, в том числе и входящие в материалы ЕГЭ, невозможно решить методами дифференциального исчисления, так как оптимизируемая функция не является гладкой. Даже если применение производной теоретически возможно, это может привести к очень громоздким преобразованиям, и в этом случае следует применять альтернативные методы решения.

Задача. Предприниматель купил здание и собирается открыть в нем отель. В отеле могут быть стандартные номера площадью 30 квадратных метров и номера «люкс» площадью 40 квадратных метров. Общая площадь, которую можно отвести под номера, составляет 940 квадратных метров. Предприниматель может поделить эту площадь между номерами различных типов, как хочет. Обычный номер будет приносить отелю 4000 рублей в сутки, а номер «люкс» — 5000 рублей в сутки. Какую наибольшую сумму денег сможет заработать в сутки на своем отеле предприниматель?

Решение. Определим доходность каждого типа номера на единицу площади. Прибыль на один квадратный метр составит для стандартного номера $\frac{4000}{30} = \frac{400}{3}$ рублей, а для номера «люкс» — $\frac{5000}{40} = \frac{500}{4}$ рублей. Следовательно, доходность стандартного номера выше, и поэтому выгоднее строить стандартные номера. Максимальное число стандартных номеров не превысит величины $\frac{940}{30} = 31\frac{1}{3}$, то есть оно равно 31. На первый взгляд, мы и получим искомое оптимальное решение, которое состоит в том, чтобы построить 31 стандартный номер. Но подобное суждение может быть ошибочным. Покажем это, проведя тщательный анализ задачи. Пусть x — число стандартных номеров; y — число номеров «люкс». По условию имеем ограничение на занимаемую площадь: $S = 30x + 40y \leq 940$. Доход предпринимателя за сутки определяется выражением: $F = 4000x + 5000y$.

Проведём анализ всевозможных комбинаций числа номеров с помощью следующей таблицы:

x	y	$S = 30x + 40y$	$F = 4000x + 5000y$
31	0	930(10)	124000
30	1	940(0)	125000
29	1	910(30)	121000
28	2	920(20)	122000
...	...	...	...

Из таблицы видно, что если построить 30 стандартных номеров и 1 номер «люкс», то прибыль составит 125000 рублей. При этом вся выделяемая площадь будет полностью задействована. Если проводить дальнейший анализ комбинаций номеров, то обнаружится, что ни одна из остальных комбинаций не даст лучшего решения, чем то, которое мы обнаружили. Эти рассуждения не имеют строгого математического обоснования, но их можно принимать в качестве решения задачи. Можно было бы привести более строгие решения в рамках построения математической модели, но они будут достаточно сложными для учеников старших классов.

Существуют классы оптимизационных экономических задач, которые имеют особую структуру, и анализ которых приводит к так называемым задачам линейного программирования. Это задачи, в которых оптимизируемая функция является линейной, то есть представляет собой линейную комбинацию переменных, и все ограничения описываются линейными равенствами или неравенствами. Задачи линейного программирования (ЗЛП) в общем виде могут быть очень сложными, и для их решения могут понадобиться специальные алгоритмы. Применительно к школьному курсу можно рассмотреть лишь частный случай задач линейного программирования, в которых возможно решение, основанное на геометрических построениях [3]. Так как построения возможны лишь в плоскости, то число переменных должно быть равно двум. Модель ЗЛП с двумя переменными имеет вид:

[illegible]

Здесь $F(x_1, x_2)$ – функция, для которой нужно найти максимальное или минимальное значение; числа c_1 и c_2 являются коэффициентами при переменных; следовательно, функция $F(x_1, x_2)$ является линейной. В системе ограничений числа a_{ij} являются также коэффициентами при переменных, в правых частях неравенств также содержатся числа; значит, все ограничения являются линейными неравенствами (вообще говоря, в системе могут быть и равенства, и неравенства). Структура модели ЗЛП позволяет применить геометрический способ решения. Действительно, целевая функция

определяется как семейство параллельных прямых (так называемых линий уровня); в системе ограничений каждое равенство определяет на плоскости прямую, а каждое неравенство определяет полуплоскость. Таким образом, пересечение всех полуплоскостей можно изобразить геометрически на плоскости, это пересечение определяет область допустимых решений (ОДР). И выбирая положение линии уровня, можно найти максимальное или минимальное значение функции с учётом всех ограничений.

Список литературы

1. Колобов А.Н., Особенности изучения задач с экономическим содержанием в школьном курсе математики. / А.Н. Колобов, И.В. Прояева // Мир науки, культуры, образования. Международный научный журнал. - 2019 г.- №3.- С.175-176.
2. Колобов А.Н., Математический кружок как форма развития интереса обучающихся к математике. / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1863-1866.
3. Колобов А.Н., Факультативные курсы по математике как форма развития математических способностей / В сборнике: Университетский комплекс как региональный центр образования, науки и культуры. Материалы Всероссийской научно-методической конференции. 2019. С. 1872-1876.

ПОДХОДЫ К ОРГАНИЗАЦИИ СИСТЕМЫ БЕЗОПАСНОСТИ СЕТЕЙ IOT-УСТРОЙСТВ

**Кузнецова Л.Ю., Парфёнов Д.И., кан. тех. наук,
Болодурина И.П., д-р техн. наук, проф., Парфёнов А.И., Забродина Л.С.**

**Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
университет»**

Объем услуг, предоставляемых провайдерами с использованием общедоступных сетей передачи данных, ежегодно увеличивается. Современная архитектура "сетей без границ" (Borderless Network Architecture) является основной для организации работы технологии Интернета вещей (IoT). В свою очередь сети IoT позволяет связать каждый объект или устройство с сетевыми возможностями. На сегодняшний день устройства, входящие в такую сеть, могут иметь совершенно различное назначение, начиная от бытовых предметов и видеокамер, заканчивая системами автоматизации, датчиками, медицинским оборудованием, и другими жизненно важными системами реального времени [1].

Особенностью IoT сетей является наличие множества разнородных IoT устройств, которые используют разнообразные протоколы передачи данных. Каждый протокол имеет собственные механизмы и меры безопасности. Тем не менее комплексного решения, обеспечивающего из единой точки механизм для организации защиты такого большого количества устройств на сегодняшний день не существует.

Традиционные подходы к безопасности, такие как системы обнаружения атак и системы предотвращения вторжений, а так же межсетевые экраны как правило направлены на организацию защиты от внешних атак. Но в случае IoT сетей, особенностью которых является бесшовный и безграничный доступ к сети, контроль становится сложнее. В рамках настоящего исследования мы обсуждаем текущее состояние и подходы к организации безопасности в IoT сетях.

Обеспечение безопасности, надёжности, устойчивости и стабильности приложений и услуг в сетях IoT имеет критически важное значение для доверия и использования интернета. Пользователям важно быть уверенными в том, что сеть передачи данных, к которой подключено IoT устройство, его приложения и подключённые к нему устройства имеют достаточно высокую степень безопасности.

Основными критериями сетевой безопасности выступают:

- конфиденциальность – неразглашение информации, обрабатываемой по сети, внешним факторам;
- целостность – сохранение структуры сообщения при его передаче по сети;

– доступность – сеть должна быть всегда доступна при любых обстоятельствах.

При создании, развёртывании или оценке IoT-технологий необходимо понимать и учитывать связанные с Интернетом вещей проблемы безопасности. Так, международная некоммерческая организация OWASP (Open Web Application Security Project) выделила следующие TOP-10 IoT-уязвимостей:

- 1) слабый, угадываемый или жёстко заданный пароль (Weak, Guessable, or Hardcoded Passwords);
- 2) небезопасные сетевые сервисы (Insecure Network Services);
- 3) небезопасные интерфейсы системы (Insecure Ecosystem Interfaces);
- 4) отсутствие безопасных механизмов обновления (Lack of Secure Update Mechanism);
- 5) использование небезопасных или устаревших компонентов (Use of Insecure or Outdated Components);
- 6) недостаточная защита конфиденциальности (Insufficient Privacy Protection);
- 7) небезопасная передача и хранение данных (Insecure Data Transfer and Storage);
- 8) ограниченные возможности управления устройством (Lack of Device Management);
- 9) небезопасные настройки по умолчанию (Insecure Default Settings);
- 10) недостаточная физическая безопасность (Lack of Physical Hardening)

Тем самым, обеспечение безопасности продуктов и услуг IoT является основным приоритетным направлением в данной отрасли.

Выделяют следующие отличия обеспечения безопасности IoT-систем от традиционных систем.

Системы IoT ограничены с точки зрения вычислительных возможностей, объёма памяти, времени автономной работы и пропускной способности сети. Следовательно, невозможно развернуть существующие традиционные решения по обеспечению безопасности, которые часто требуют значительных ресурсов.

– Системы IoT являются сильно распределёнными и неоднородными системами. Таким образом, централизованное традиционное решение может оказаться непригодным. Кроме того, распределённый аспект IoT добавляет больше трудностей и ограничений в их защите.

– Системы IoT развёрнуты в физической среде, которая непредсказуема. Таким образом, к списку традиционных угроз безопасности добавляются физические атаки.

– Системы IoT подключены к Интернету, поскольку каждое устройство имеет доступ со своим IP-адресом. Следовательно, существует ещё одна группа угроз, связанных с сетью передачи данных.

– Системы IoT состоят из большого количества ограниченных объектов, которые генерируют огромное количество данных. В связи с этим,

используя ограниченную пропускную способность сетей, можно легко вызвать отказ в обслуживании и атаковать эти небольшие устройства.

– Системы IoT охватывают большое количество разнородных протоколов и технологий в одной системе. Следовательно, предлагаемое решение безопасности IoT должно учитывать разнообразие этих протоколов и технологий в одном предложении.

По мере постоянного увеличения числа устройств, подключенных к сети интернет, возникают новые потенциальные уязвимые места. В связи с чем, IoT-устройства подвержены сетевым, физическим и программным атакам, а также утечке конфиденциальной информации.

Выделим следующие угрозы безопасности IoT-устройств.

1) DoS-атаки (Denial of Service, атака типа «отказ в обслуживании»)

Во время этой атаки злоумышленники переполняют целевой сервер избыточными запросами, чтобы прервать пользователям доступ к услугам IoT-устройств [2]. Один из наиболее опасных типов DoS-атак – это DDoS-атаки (Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»), которые используют тысячи адресов интернет-протоколов для запроса услуг IoT, что затрудняет серверу возможность отличить законные устройства IoT от злоумышленников. Эта атака влияет на сетевые ресурсы, пропускную способность, процессор и т.д. Распределенные IoT-устройства с лёгкими протоколами безопасности особенно уязвимы для DDoS-атак [3].

2) Помехи (Jamming). Вид атаки, при которой злоумышленники посылают поддельные сигналы для прерывания текущих радиопередач IoT-устройств и дальнейшего истощения пропускной способности, энергии, центральных процессоров (ЦП) и ресурсов памяти IoT-устройств или датчиков во время их неудачных попыток связи [4].

3) Спуфинг (Spoofing). Узел спуфинга маскируется под легальное IoT-устройство с его идентификатором, таким, как адрес управления доступом к среде (MAC) и RFID-метка, чтобы получить незаконный доступ к IoT-системе. Тем самым, этот узел может в дальнейшем запускать атаки типа DoS и Man-in-the-middle [5].

4) Атака Man-in-the-middle. Вид атаки, когда злоумышленник, находящийся посередине, посылает сигналы помех и спуфинга с целью тайного мониторинга, прослушивания и изменения связи между двумя IoT-устройствами, которые считают, что общаются непосредственно друг с другом [2].

5) Hello Flood Attack. В IoT-сети протокол маршрутизации транслирует приветственное сообщение, чтобы сообщить о своём присутствии соседним узлам. Злоумышленник может подделать такое сообщение и отправить его на устройство. Узел, который принимает сообщение приветствия, может распознать, что устройство находится в пределах досягаемости (т. е. в пределах своего диапазона связи), и добавить его в список соседних узлов.

6) Программные атаки (Software attacks). К таким атакам относятся мобильные вредоносные программы, такие как трояны, черви и вирусы,

которые могут привести к утечке конфиденциальности, экономическим потерям, истощению мощности и снижению производительности сети IoT-систем [6].

7) Утечка конфиденциальных данных (Privacy Leakage). Примерно 90% устройств собирают ту или иную персональную информацию о владельце без его ведома. Однако, некоторые из разработчиков устройств могут использовать собранные персональные данные не для улучшения работы устройств, а для продажи другим компаниям с целью прибыли. Также злоумышленники могут получить доступ к этой информации, используя «дыры» в защите систем. Носимые устройства, которые собирают личную информацию пользователя, такую, как информация о местоположении и здоровье, неоднократно подвергались утечке личной информации пользователей [7].

Подходы обнаружения вторжения в Интернет вещей подразделяются на четыре типа в зависимости от механизма обнаружения.

1) Подходы на основе сигнатур. В таких подходах системы обнаружения вторжений (Intrusion Detection Systems, IDS) выявляют атаки, когда поведение системы или сети совпадает с сигнатурой атаки, хранящейся в собственных базах данных IDS. Если какая-либо активность системы или сети совпадает с сохранёнными шаблонами / сигнатурами, то будет выдано предупреждение. Системы обнаружения вторжений на основе сигнатур точны в выявлении известных угроз, а их методика проста для понимания. Однако этот подход неэффективен для обнаружения новых атак и других вариантов известных атак, поскольку совпадающая сигнатура для этих атак всё ещё не установлена.

2) Подходы, основанные на аномалиях. Системы обнаружения вторжений, основанные на аномалиях, мгновенно сравнивают действия системы с профилем нормального поведения и выдают сигнал тревоги всякий раз, когда отклонение от нормального поведения выходит за пределы порогового значения. Этот подход эффективен для обнаружения новых атак, в частности, тех атак, которые связаны со злоупотреблением ресурсами. Тем не менее, всё, что не соответствует нормальному поведению, считается вторжением, и изучение всего объёма нормального поведения является достаточно трудоёмкой задачей. Тем самым, этот метод обычно имеет высокий уровень ложных срабатываний. Чтобы построить нормальный профиль поведения, учёные обычно используют статистические методы или алгоритмы машинного обучения, которые могут быть слишком тяжёлыми для узлов IoT-сетей, имеющих низкую пропускную способность. Следовательно, методы обнаружения вторжений на основе аномалий должны учитывать эту особенность IoT-сетей.

3) Подходы, основанные на спецификациях. Спецификация – это группа правил и пороговых значений, которые определяют ожидаемое поведение для сетевых элементов, таких, как узлы, протоколы и таблицы маршрутизации. Подходы, основанные на спецификации, выявляют вторжения, когда

поведение сети отклоняется от определений спецификации. Следовательно, обнаружение на основе спецификаций имеет ту же цель, что и на основе аномалий: выявление отклонений от нормального поведения. Однако есть одно важное различие между этими методами: в подходах, основанных на спецификациях, специалист-человек должен вручную определять правила каждой спецификации. Спецификации, определённые вручную, обычно обеспечивают более низкий уровень ложных срабатываний по сравнению с обнаружением на основе аномалий. Кроме того, системам обнаружения на основе спецификаций не требуется этап обучения, поскольку они могут начать работать сразу после настройки спецификации. Однако определённые вручную спецификации могут не адаптироваться к различным средам и могут занимать много времени и быть подвержены ошибкам.

4) Гибридные подходы. Такие подходы используют идеи обнаружения на основе сигнатур, спецификаций и аномалий, чтобы максимизировать преимущества этих подходов и минимизировать их недостатки.

Таким образом обнаружение атак в сетях IoT относится к процедуре проверки и анализа событий, происходящих в системе, для выявления ненормального (вредоносного) поведения. Процесс обнаружения вторжения включает в себя выявление ряда действий, которые ставят под угрозу безопасность системы.

Обнаружение вторжений можно рассматривать как одну из следующих задач машинного обучения.

1) Задача прогнозирования (предсказания). Данная задача направлена на предсказание будущих возможностей и тенденций. Зная характер развития событий в будущем, можно принимать более обоснованные решения. Одним из основных методов прогнозирования является регрессионный анализ, с помощью которого можно предсказать возможность атаки. Регрессионный анализ позволяет предсказывать подобное поведение из собранных логов атак.

2) Классификация. Подобные задачи направлены на разделение на классы объектов (поведение сети) согласно определённым и заданным заранее признакам. Классификация позволяет выделить всё то, что не вписывается в стандартные классы, т. е. выявить вторжение. Тем самым, классификация помогает администратору безопасности определить направление защиты и анализа. Для решения задачи классификации используются методы обучения с учителем.

3) Кластеризация. Для решения данных задач применяются методы обучения без учителя. Задача кластеризации направлена на разбиение набора данных на группы, имеющие одинаковые свойства (т. н. кластеры). Кластеризация разделяет набор данных на несколько групп (кластеров) таким образом, что сходство внутри группы (кластера) больше, чем между группами (кластерами). Задача кластеризации сходна с задачей классификации, но её отличие заключается в том, что классы изучаемого набора данных заранее не предопределены. Отметим, что процедуры кластеризации также подходят для сжатия данных.

4) Задача поиска ассоциативных правил. Данная задача направлена на выявление скрытых отношений между данными. Отношение из потока времени называется правилом последовательности. При обнаружении закономерностей в таких последовательностях можно с некоторой долей вероятности предсказывать появление событий в будущем, что позволяет принимать более правильные решения. Этот метод анализа может определять ненормальное поведение сети путём анализа поведения пользователя или работы устройств сети.

Актуальной задачей является разработка моделей и механизмов обеспечения безопасности IoT-сети. Для этого необходимо разработать модель идентификации атак на IoT-сеть, использующую поведенческий анализ, основанный на мониторинге характеристик (признаков) поведения сети. Под поведением сети будем понимать совокупность характеристик (признаков) сети в определенный момент времени.

Идентификация подразумевает сопоставление текущего поведения сети с известным поведением (нормальное поведение, поведение под атакой). Тем самым, задача идентификации атак сводится к задаче классификации поведения сети.

В рамках данной работы задача классификации может быть сформулирована следующим образом.

Пусть дано множество классов поведения IoT-сети C (нормальное поведение, поведение под атакой); множество признаков поведения IoT-сети K ; множество исследуемых поведений IoT-сети X_c .

Из множества признаков поведения сети K выделим подмножество $K_I \subseteq K$ – множество наиболее информативных признаков. То есть каждое поведение представлено вектором признаков K_I размерностью k .

Положим, X_{cK_I} – множество исследуемых объектов, представленные вектором признаков K_I , $|K_I| = k$. Пусть с помощью некоторого правила R построена обучающая выборка – набор маркированных вектор-признаков

поведения IoT-сети, т. е. $\Psi_{X_c^L} = \left\{ (x_i', \bar{c}) \right\}_{i=0}^M = \bigcup_{C_i \in C} \bigcup_{x \in C_i \cap X_c^L} (x, \lambda(C))$, где

$X_c^L \subseteq X_c$ – множество обучающих векторов, а $x_i' \in C_{i\bar{c}_i}$ – отношение принадлежности.

Отсюда следует, что для решения задачи идентификации атак на IoT-сеть требуется решить следующую оптимизационную задачу на основе обучающей выборки $\Psi_{X_c^L}$.

Для этого дополнительно введём множество $G = \{K_{I_1}, \dots, K_{I_k}\}$, где $K_{I_i} \subseteq K_I$, $|K_{I_i}| = i$, а также вспомогательную функцию $\psi: G \rightarrow \{X_{C_{K_{I_1}}}, \dots, X_{C_{K_{I_k}}}\}$, где $X_{C_{K_{I_i}}}$ – исследуемые IoT-устройства, представленные вектором длиной i .

Требуется при заданном уровне эффективности идентификации σ минимизировать количество используемых признаков $k \in K_I$, т. е.

$$\Lambda(a, X_c, \sigma) = \left\{ |K_{I_i}| \mid K_{I_i} \in G, \Omega(a, \psi(K_{I_i})) \geq \sigma \right\} \rightarrow \min_{i \in 1, k},$$

где $\Lambda(a, X_c, \sigma)$ – функция оценки минимального набора признаков поведения; σ – некоторое заданное положительное число.

В дальнейшем для реализации идентификации и классификации атак на IoT сети будут использована построенная модель. Кроме того, необходимо провести дополнительные исследования для подбора методов прогнозирования угроз и сбора данных об инцидентах в IoT сети.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 18-37-00400, № 18-07-01446, № 19-47-560011, № 20-07-01065, а так же гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-860.2019.9).

Список литературы

- 1 Болодурина И. П., Парфёнов Д. И. Моделирование обеспечения надежности функционирования объектов сетевой инфраструктуры киберфизической системы //Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. – 2018. – Т. 18. – №. 4. – С. 41-51.
- 2 Andrea I., Chrysostomou C., Hadjichristofi G. Internet of Things: Security vulnerabilities and challenges //2015 IEEE Symposium on Computers and Communication (ISCC). – IEEE, 2015. – С. 180-187.
- 3 Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed internet of things //Computer Networks. – 2013. – Т. 57. – №. 10. – С. 2266-2279.
- 4 Han G., Xiao L., Poor H. V. Two-dimensional anti-jamming communication based on deep reinforcement learning //2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). – IEEE, 2017. – С. 2087-2091.
- 5 Xiao L. et al. PHY-layer spoofing detection with reinforcement learning in wireless networks //IEEE Transactions on Vehicular Technology. – 2016. – Т. 65. – №. 12. – С. 10037-10047.

6 Xiao L. et al. Cloud-based malware detection game for mobile devices with offloading //IEEE Transactions on Mobile Computing. – 2017. – T. 16. – №. 10. – C. 2742-2750.

7 Yan Z., Zhang P., Vasilakos A. V. A survey on trust management for Internet of Things //Journal of network and computer applications. – 2014. – T. 42. – C. 120-134.

АЛГОРИТМЫ ФОРМИРОВАНИЯ ДИСКОВЫХ ОБРАЗОВ ДЛЯ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА К УДАЛЕННЫМ РАБОЧИМ ОКРУЖЕНИЯМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Легашев Л.В., канд.техн.наук, Полежаев П.Н.,
Коннов А.Л., канд.техн.наук, доцент, Грибович И.О, Матвеев А.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
университет»

Мультиоблачный центр коллективного доступа к удаленным рабочим окружениям может быть использован в образовательном процессе [1, 2] для совместного доступа к программному обеспечению и вычислительным ресурсам нескольких образовательных организаций. Одной из важнейших задач, решаемых в рамках проекта по созданию мультиоблачного центра коллективного доступа, является создание дисковых образов для обслуживания данного центра.

Приведем математическую формализацию данной задачи. Пусть $F = \{f_1, \dots, f_m\}$ - набор доступного для установки или удаления программного обеспечения. Пусть $S_{install}(f_i)$ и $S_{delete}(f_i)$ – соответственно средняя стоимость установки и удаления программного обеспечения f_i . Каждый дисковый образ F_{flav}^i , используемый в виртуальных машинах мультиоблачного центра коллективного доступа, представляет собой, по сути, некоторое подмножество $F_{flav}^i \subseteq F$. Размер дискового образа берется достаточным, или он может динамически меняться специальными инструментами для работы с образами и файловыми системами. Также каждый дисковый образ включает в себя операционную систему (ОС), которая для простоты считается уже установленной (или устанавливается первой).

Пусть ориентированный граф $G = (V, E)$ представляет собой граф дисковых образов и операций по их формированию. Его вершинами $V = 2^F$ выступают все возможные дисковые образы (множество всех подмножеств множества F), а каждая дуга $e = (u, v) \in E$ соответствует операции (автоматической установки или удаления) для получения дискового образа v из образа u . Для определения типа операции, ассоциированной с дугой e может быть использована следующая индикаторная функция:

$$type(e) = \begin{cases} 1, & \text{если установка ПО,} \\ 0, & \text{иначе.} \end{cases}$$

Пусть $software(e) \in F$ представляет собой программный пакет, установка или удаления которого ассоциирована с дугой e , $cost(e)$ - стоимость данной операции:

$$\text{cost}(e) = \begin{cases} S_{\text{install}}(\text{software}(e)), & \text{если } \text{type}(e) = 1, \\ S_{\text{delete}}(\text{software}(e)), & \text{иначе.} \end{cases}$$

Следует заметить, что ориентированный граф G - представляет собой m -й гиперкуб с экспоненциальным числом вершин. Поэтому временная сложность большинства алгоритмов для данного графа (даже простого обхода всех вершин в некотором порядке) будет экспоненциальной.

Рассмотрим задачу формирования набора терминальных дисковых образов $R = \{r_k\}_{k=1, N_R} \subseteq 2^F$ из пустого дискового образа $\emptyset \in 2^F$. Необходимо найти такой подграф $T = (V_T, E_T) \subseteq G$, для которого верны одновременно следующие утверждения:

а) $\emptyset \in V_T, R \subseteq V_T$;

б) для любого терминального дискового образа $r_k \in R$ в T существует единственный путь $\text{Path}(r_k)$, соединяющий $\emptyset$ с r_k ;

в) $\bigcup_{r_k \in R} \text{Path}(r_k) = E_T$ – объединение всех путей формирует множество дуг

данного подграфа;

г) $\text{cost}(T) = \text{cost}(E_T) = \sum_{e \in E_T} \text{cost}(e) \rightarrow \min$ – стоимость подграфа T , она же

суммарная стоимость всех дуг такого подграфа, должна быть наименьшей.

Очевидно, что данный подграф T представляет собой ориентированное дерево с выделенным корнем $\emptyset$ – дерево Штейнера минимального веса.

В общем случае решение данной задачи даже для графа с полиномиальным числом вершин является экспоненциальным. Поэтому для нахождения субоптимального приближения дерева Штейнера минимального веса необходимо использовать метаэвристические алгоритмы, причем они не могут просматривать все вершины ориентированного графа $G = (V, E)$, т.к. их количество экспоненциально.

Основной идеей ранее предложенных авторами алгоритмов [2] (при наличии только операции установки программного обеспечения) является применение алгоритма муравьиной колонии, при котором муравьи расставляются в терминальные дисковые образы по одному и двигаются в сторону пустого дискового образа в корне в направлении противоположном ориентации дуг, пока не дойдут до него или до пути другого муравья. Полученное дерево является аппроксимацией дерева Штейнера минимального веса и используется для расчета оставленного каждым муравьем феромона.

Другим вариантом алгоритма (Prim's AntColonyOptimization (PACO)) [2] является движение всех муравьев до корня с последующим объединением всех посещенных муравьями вершин. После чего к объединенным вершинам добавляются все возможные дуги из исходного графа, которые их соединяют и в получившемся конечном графе запускается алгоритм Прима из пустой вершины. При этом для него ориентация дуг не важна, т.к. они все будут ориентированы в порядке просмотра и обратных дуг не будет. Минимальное

покрывающее дерево, которое он находит и является аппроксимацией дерева Штейнера минимального веса. Данный подход оказался лучшим согласно ранее проведенным экспериментальным исследованиям с помощью симулятора [2].

В рамках данной работы рассматривается усложненный вариант задачи, в котором программное обеспечение можно автоматически удалять, если оно было установлено в дисковый образ. Данный подход больше соответствует реальной ситуации, когда программные пакеты не только устанавливаются, но и удаляются. В связи с тем, что поддерживается удаление ПО, муравьи могут бесконечно долго перемещаться по графу G , не дойдя до пустого дискового образа, поэтому надо их перемещение ограничить как по количеству пройденных дуг, так и по повторному посещению ранее пройденных вершин. В первом случае при достижении ограничения по количеству пройденных дуг муравей двигается непосредственно к пустому дисковому образу, используя только дуги установки ПО, не смотря на множество табу. Во-втором случае используется множество табу для хранения ранее посещенных вершин, чтобы не заходить в них повторно.

Рассмотрим алгоритм решения задачи построения аппроксимации дерева Штейнера минимального веса, который основан на метаэвристике муравьиной колонии.

Алгоритм 1 – Алгоритм муравьиной колонии для нахождения аппроксимации дерева Штейнера минимального веса

Шаг 1. Инициализировать количество итераций $t = 1$ и лучшее решение $T_{best} = \emptyset$, $cost(T_{best}) = +\infty$.

Шаг 2. Муравьи распределяются по терминальным вершинам (по одному на вершину). Пусть $Ants = \{ant_k\}_{k=1, \overline{N_R}}$ – список муравьев, ant_k помещается в вершину, соответствующую терминальному дисковому образу r_k .

Шаг 3. Пока $t \leq T_{max}$ (не превышено максимальное количество итераций) выполняются следующие действия:

Шаг 3.1. инициализируем список активных муравьев $M = Ants$, которые могут продолжать двигаться;

Шаг 3.2. для каждого муравья $ant_k \in M$ зададим пустой список $P_k = \emptyset$ пройденных дуг ориентированного графа G , $Tabu_k = \{r_k\}$ – множество вершин, запрещенных для перехода муравью, V'_k – множество посещенных вершин, $mode_k = 1$ – режим поиска пустого дискового образа;

Шаг 3.3. пока $M \neq \emptyset$ (есть муравьи, которые еще не дошли до стартовой вершины), случайно равномерно выбираем муравья $ant_k \in M$ и для него выполняем следующие вложенные шаги:

Шаг 3.3.1. пусть u_k – текущая вершина ориентированного графа G , в которой находится муравей ant_k , добавляем ее в множество посещенных вершин $V'_k = V'_k \cup \{u_k\}$;

Шаг 3.3.2. если $u_k = \emptyset$ (муравей достиг пустого дискового образа), то удаляем его из списка активных муравьев $M = M \setminus \{ant_k\}$ и переходим на следующую итерацию цикла шага 3.3;

Шаг 3.3.3. иначе, если $u_k \neq \emptyset$, то:

Шаг 3.3.3.1. необходимо определить $L_k(t, u_k, mode_k)$ – множество рассматриваемых для перехода вершин муравьем ant_k в момент времени t , когда он находится в вершине u_k в режиме $mode_k$. Если $mode_k = 1$, то рассматриваются вершины, не содержащие в $Tabu_k$, из которых исходят дуги, соответствующие установке или удалению одного ПО. Иначе, если $mode_k = 0$, то не смотря на $Tabu_k$ выбор производится среди только тех вершин, из которых исходят дуги, соответствующие установки ПО. $L_k(t, u_k, mode_k)$ вычисляется по формуле:

$$L_k(t, u_k, mode_k) = \begin{cases} \{v \in V \setminus Tabu_k \mid (v, u_k) \in E\}, & \text{если } mode_k = 1, \\ \{v \in V \mid (v, u_k) \in E \ \& \ type((v, u_k)) = 1\}, & \text{иначе;} \end{cases}$$

Шаг 3.3.3.2. если $L_k(t, u_k, mode_k) = \emptyset$ (муравей окружен вершинами из множества табу), то возвращаемся по последней пройденной в обратном направлении дуге (u_k, w_k) из P_k назад в вершину w_k , а также удаляем эту дугу из пути $P_k = P_k \setminus \{(u_k, w_k)\}$, а вершину u_k – из множества посещенных вершин $V'_k = V'_k \setminus \{u_k\}$;

Шаг 3.3.3.3. иначе, если $L_k(t, u_k, mode_k) \neq \emptyset$, то:

Шаг 3.3.3.3.1. случайно выбираем следующую вершину v_k , в которую может перейти муравей в графе G при движении в противоположном ориентации дуг. Вероятности выбора вершин определяется вероятностями выбора соответствующих дуг согласно формуле:

$$P_{(v_k, u_k)}(t) = \frac{(\tau_{(v_k, u_k)}(t))^\alpha (\eta_{(v_k, u_k)}(t))^\beta}{\sum_{v_k \in L_k(t, u_k, mode_k)} (\tau_{(v_k, u_k)}(t))^\alpha (\eta_{(v_k, u_k)}(t))^\beta}, \quad (1)$$

где $\tau_{(v_k, u_k)}(t)$ – текущий уровень феромона на дуге (v_k, u_k) на итерации t (в начале он равен τ_0 , а затем обновляется муравьями), а

$\eta_{(v_k, u_k)}(t) = \frac{1}{cost((v_k, u_k))}$ – величина, обратная стоимости дуги, $\alpha, \beta \geq 0$ –

весовые коэффициенты, соответственно отражающие степень важности феромона (предыдущего совместного опыта муравьев) и текущего окружения муравья;

Шаг 3.3.3.3.2. добавить выбранную дугу к пути муравья $P_k = P_k \cup \{(v_k, u_k)\}$, обновить список табу $Tabu_k = Tabu_k \cup \{v_k\}$. Если $mode_k = 1 \& |P_k| = P_{\max}$, то $mode_k = 0$ - включить режим движения муравья только по дугам установки ПО;

Шаг 3.3.4. перейти на следующую итерацию цикла на шаге 3.3;

Шаг 3.4. сформировать ориентированный граф $G' = (V', E')$, в котором $V' = \bigcup_{k=1, N_k} V'_k$ - множество посещенных муравьями вершин, а множество дуг формируется путем включения всех дуг из графа G , соединяющих вершины $E' = \{(u, v) | u, v \in V' \wedge (u, v) \in E\}$;

Шаг 3.5. запустить на ориентированном графе G' с использованием весовой функции $cost$ из пустой вершины $\emptyset$ алгоритм Чу Йонджина и Лю Цзенхонга [3] для нахождения ориентированного минимального покрывающего дерева $T_{MST} = (V_{MST}, E_{MST})$ с выделенным корнем в вершине $\emptyset$;

Шаг 3.6. удалить из T_{MST} все ребра и вершины, которые не лежат на путях, ведущих к терминальным дисковым образам R , оставшиеся вершины и дуги образуют искомый граф $T = (V_T, E_T)$ - аппроксимацию дерева Штейнера минимального веса;

Шаг 3.7. вычислить стоимость $cost(T)$ полученного дерева T , если $cost(T_{best}) > cost(T)$, то $T_{best} = T$ (обновляем лучшее найденное решение);

Шаг 3.8. каждый муравей $ant_k \in M$ двигается по дугам пути P_k от пустого дискового образа $\emptyset$ до его стартового терминального образа r_k и обновляет феромон по следующей формуле:

$$\tau_{(v_k, u_k)}(t+1) = \tau_{(v_k, u_k)}(t)(1 - \rho) + \frac{1}{cost(T)} \rho,$$

где $\rho \in [0, 1]$ - скорость испарения феромона.

Шаг 3.9. Увеличить номер итерации $t = t + 1$ и перейти на шаг 3.

Шаг 4. Вернуть T_{best} в качестве лучшей аппроксимации дерева Штейнера минимального веса.

Обратим внимание на особенности данного алгоритма. На шаге 3.3.3.3.1 выбор следующей вершины для перехода муравьем происходит с учетом противоположной ориентации дуг графа G , чтобы потом получившиеся деревья Штейнера имели правильную ориентацию дуг и отражали реальную последовательность установки программ. На рисунке 1 проиллюстрированы возможные вершины для перехода муравьем в режиме 1, это две группы вершин, не входящих в множество табу, — те, в которые ставится одно ПО, чтобы получилась текущая вершина муравья, и те, из которых удаляется один программный пакет. Выбор вершины для перехода происходит стохастически с вероятностями, заданными формулой (1).

Т.к. дисковые образа представляют собой множества программных пакетов, то для их кодирования и хранения удобно использовать двоичное векторное представление. Пусть муравей стоит в вершине, соответствующей текущему дисковому образу $u = [u_1, u_2, \dots, u_m]$, где $u_i = 1$, если программный пакет $f_i \in u$, и $u_i = 0$ иначе. Тогда дисковые образа $v = [v_1, v_2, \dots, v_m]$, в которые ставится ПО, будут отличаться ровно одним, скажем j -м компонентом вектора, причем $v_j = 0$, а $u_j = 1$. Аналогично, дисковые образа $v = [v_1, v_2, \dots, v_m]$, из которых удаляется ПО, также будут отличаться ровно одним, пусть j -м компонентом вектора, причем $v_j = 1$, а $u_j = 0$.

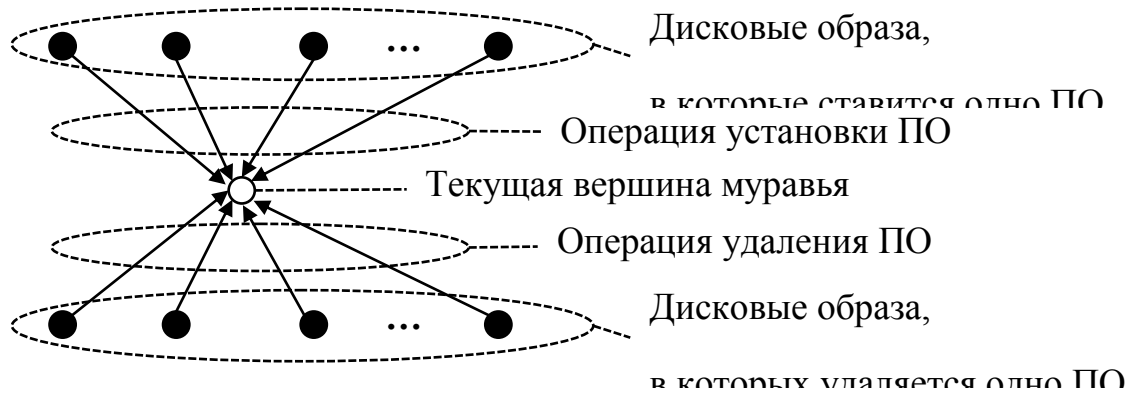


Рисунок 1 – Выбор следующей вершины для перехода муравья

Сформулируем задачу формирования набора опорных дисковых образов $S \subseteq F$. Набор опорных дисковых образов может быть использован для обработки запросов на формирования терминальных дисковых образов путем их копирования и установки/удаления необходимого программного обеспечения. Эффективный набор опорных образов может значительно сократить время на обработку запросов на формирования терминальных образов в сравнении с использованием только пустого дискового образа.

Если имеется набор опорных дисковых образов $S \subseteq F$, то для обработки запроса на формирование терминальных дисковых образов $R = \{r_k\}_{k=1, \overline{N_R}} \subseteq 2^F$ достаточно изменить ориентированный граф G так, чтобы получить граф $G_S = (V, E_S)$, в котором тоже самое множество вершин, а множество дуг дополнено дугами $(\emptyset, r_k)$, соединяющими пустой образ с каждым опорным:

$$E_S = E \cup \bigcup_{r_k \in R} \{(\emptyset, r_k)\}.$$

При этом $type((\emptyset, r_k)) = 1$ (установка) и $cost((\emptyset, r_k)) = 0$ (стоимость установки нулевая, т.к. образы подготовлены заранее). Тогда стоимость обработки запроса R будет равна стоимости аппроксимации дерева Штейнера минимального веса $cost(G_S, R)$, построенного с помощью модифицированного алгоритма 1 на графе G_S .

Для поддержки работы с опорными образами алгоритм 1 должен быть модифицирован в части поиска пустого дискового образа – теперь муравей останавливается, когда находит любой опорный дисковый образ. Также в режиме 0 (превышен максимальный размер пути) муравей начинает двигаться стохастически не до пустого образа, а до ближайшего опорного.

В общем случае задачу формирования набора опорных дисковых образов можно сформулировать в виде оптимизационной проблемы следующим образом:

$$S = \arg \min_{\substack{S \in 2^F, \\ |S| \leq K}} \sum_{R \in 2^F} p(R) \cdot \text{cost}(G_S, R), \quad (2)$$

где $K > 0$ – максимальное количество опорных дисковых образов, причем $K = O(m)$, $p(R)$ – вероятность появления запроса R .

Формула (2), по сути, минимизирует математическое ожидания стоимости выполнения случайного запроса R . Также заметим, что ограничение K на количество опорных дисковых образов необходимо, т.к. без него в формуле (2) минимум будет достигаться при $S = 2^F$ (все образы создать заранее и сделать опорными), что недопустимо, т.к. мы хотим обеспечить полиномиальную временную сложность для алгоритма формирования опорных дисковых образов. Аналогично, с этой же целью требуется, чтобы количество опорных образов было линейным от m .

Основным недостатком данной оптимизационной задачи является экспоненциальная временная сложность ее решения, т.к. в формуле (2) происходит перебор подмножеств множества всех программных пакетов под знаком минимума и суммы.

Для его преодоления сформулируем оптимизационную задачу другим способом. Пусть $Q = \{R_i\}_i$ – множество эталонных запросов на формирование терминальных дисковых образов, причем его размер $|Q| = O(P(m))$ – полиномиален от количества программных пакетов. Рассмотрим задачу (2), которая является упрощением (2):

$$S = \arg \min_{\substack{S \in 2^F, \\ |S| \leq K}} \sum_{R \in Q} \text{cost}(G_S, R). \quad (2)$$

Решение оптимизационной задачи (3) по-прежнему требует экспоненциальной временной сложности, т.к. остался перебор подмножеств программных пакетов под знаком суммы.

Заметим, что обычная очевидная жадная стратегия, которая начинает с первого опорного дискового образа и добавляет образа по одному, на каждом шаге обеспечивая локальный минимум целевой оптимизируемой функции относительного очередного выбираемого дискового образа, имеет экспоненциальную временную сложность и также эффективно работать не будет.

Предложим несколько вариантов алгоритмов, которые рассматривают ограниченные подмножества множества пакетов программного обеспечения:

а) Алгоритм, основанный на подсчете статистики использования дисковых образов. Пусть $count_R(F_{flav}^i)$ – количество терминальных дисковых образов запроса R , которые были из него получены алгоритмом, т.е. $count_R(F_{flav}^i) = 0$, если F_{flav}^i не принадлежит аппроксимации дерева Штейнера для запроса R , иначе $count_R(F_{flav}^i)$ равно количеству листьев в дереве, достижимых из F_{flav}^i . Определим ранг образа, как среднее количество таких терминальных образов на множестве эталонных запросов Q :

$$rank(F_{flav}^i) = \frac{1}{|Q|} \sum_{R \in Q} count_R(F_{flav}^i).$$

Алгоритм выбирает в качестве опорных K дисковых образов с максимальными значениями $rank(F_{flav}^i)$.

б) Модификация предыдущего алгоритма, в которой множество опорных дисковых образов дополняется максимальным образом, содержащим все программное обеспечения в установленном виде.

в) Алгоритм, основанный на оценке полезности дисковых образов. Рассмотрим терминальные образы запроса $R = \{r_k\}_{k=1, \overline{N_R}} \in Q$, из них составляются все возможные попарные пересечения и объединения: $\forall i = \overline{1, N_R - 1}, \forall j = i + 1, \overline{N_R}, \sigma_{ij} = r_i \cup r_j$ и $\eta_{ij} = r_i \cap r_j$, а при наличии времени:

- пересечения и объединения троек терминальных образов;
- пересечения и объединения четверок терминальных образов.

Сами терминальные образы, а также составленные из них образы, упорядочиваются по полезности $utility(F_{flav}^i)$ и из них выбирается K с максимальным значением. Полезность может быть вычислена по формуле:

$$utility(F_{flav}^i) = \frac{1}{|Q|} \sum_{R \in Q} cost(G_{F_{flav}^i}, R).$$

В рамках исследований были разработаны алгоритмы для формировать опорных дисковых образов и динамической обработки запросов по созданию дисковых образов с их помощью на основе алгоритма муравьиной колонии.

Исследования проведены при финансовой поддержке РФФИ (проект 18-37-00460 мол_а) и гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9).

Список литературы

1. Bolodurina I., Legashev L., Polezhaev P., Shukhman A., Ushakov Yu. Ant Colony Algorithm for Building of Virtual Machine Disk Images Within Cloud Systems //International Conference on Remote Engineering and Virtual Instrumentation. - Springer, Cham, 2018. - P. 701-706.
2. Polezhaev, P. Simulation Modeling of Virtual Machine Based Services in Multi-Cloud Shared Access Centers / Polezhaev P., Legashev L. Shukhman A.,

Bolodurina I. // Advances in Intelligent Systems Research, volume 166, 2019. - P. 219-224.

3. С.Ю. Пименов, Г. А. Корнеев, А.А. Шалыто. Алгоритм Чу Йонджина и Лю Цзенхонга построения кратчайшего корневого дерева в ориентированном графе [Электронный ресурс]// Санкт-Петербург, 2004. – Режим доступа: <http://is.ifmo.ru/vis/ctree/doc.pdf>

ИССЛЕДОВАНИЕ АЛГОРИТМОВ РАБОТЫ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА К УДАЛЕННЫМ РАБОЧИМ ОКРУЖЕНИЯМ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

**Легашев Л.В., канд.техн.наук, Полежаев П.Н.,
Коннов А.Л., канд.техн.наук, доцент, Грибович И.О., Матвеев А.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Оренбургский государственный
университет»**

Мультиоблачный центр коллективного доступа к удаленным рабочим окружениям может быть использован в образовательном процессе для совместного доступа к программному обеспечению и вычислительным ресурсам нескольких образовательных организаций. Аналогично он может быть использован компаниями, которые с целью экономии денежных средств хотят пользоваться тонкими клиентами.

Ранее в рамках проводимого исследования были разработаны теоретические модели[1]: структурная модель мультиоблачной системы коллективного доступа, структурная модель сервисов виртуальных рабочих окружений DaaS, имитационная модель мультиоблачной системы коллективного доступа, а также алгоритмические решения [2, 3]: алгоритм оценки и прогнозирования характеристик потока заявок пользователей для получения доступа к виртуальным рабочим окружениям, алгоритм эффективного масштабирования и распределения нагрузки на пулы виртуальных машин, используемых для размещения контейнеров с виртуальными рабочими окружениями, с учетом прогнозируемых характеристик потока заявок пользователей, алгоритма миграции контейнеров с виртуальными рабочими окружениями между виртуальными машинами пулов, алгоритм формирования опорных дисковых образов виртуальных машин, алгоритм динамического формирования набора дисковых образов виртуальных машин для обслуживаемых заявок пользователей на основе опорных образов.

Для исследования данных алгоритмов был разработан симулятор мультиоблачной системы коллективного доступа, который был реализован на языке программирования Python. Он моделирует генерацию и обработку заявок пользователей на запуск сервисов, а также их работу внутри сервисов. В частности, для DaaS-сервисов моделируется работа пользователей с приложениями в рамках их виртуальных окружений.

Рассмотрим основные метрики, анализируемые в рамках данного исследования:

а) Средняя загрузка вычислительных ядер виртуальных машин:

$$\overline{U}^{cpu} = \frac{1}{M} \sum_{j=1}^M \overline{U}_j^{cpu},$$

$$\bar{U}_j^{cpu} = \frac{1}{(t_n - t_0)} \sum_{k=1}^n ((t_k - t_{k-1}) u_j^{cpu.vm}(t_k)) \cdot 100\%,$$

где M – количество анализируемых виртуальных машин, $\bar{U}_j^{cpu}$ – средняя загрузка вычислительных ядер процессоров виртуальной машины Vm_j за весь период наблюдения, n – количество замеров загрузки ядер виртуальных машин, $t_0, t_1, t_2, \dots, t_n$ – моменты времени, в которые проводились замеры, $u_j^{cpu.vm}(t_k)$ – средняя загрузка всех ядер процессоров виртуальной машины в момент времени t_k .

б) Индекс сбалансированности загрузки вычислительных ядер виртуальных машин вычисляется по формуле:

$$\sigma_{cpu} = \sqrt{\frac{\sum_{j=1}^M (\bar{U}_j^{cpu} - \bar{U}^{cpu})^2}{M - 1}}.$$

в) Среднее время выполнения запроса на запуск DaaS-сервиса:

$$\bar{T}^{start} = \frac{1}{N} \sum_{j=1}^N T_j^{start},$$

где N – количество запросов, T_j^{start} – время выполнения j -го запроса.

Значения данных метрик усреднялись по результатам 20 запусков на случайно сгенерированных заявках и активностей пользователей.

В ходе исследования алгоритмов с помощью симулятора рассматривалось три сценария:

а) Сценарий А – 1 провайдер, 5 пулов со стартовым количеством виртуальных машин 3.

б) Сценарий В – 2 провайдера, 5 пулов со стартовым количеством виртуальных машин 3 в каждом.

г) Сценарий С – 3 провайдера, 5 пулов со стартовым количеством виртуальных машин 3 в каждом.

Пулы виртуальных машин отличаются друг от друга шаблонами используемых виртуальных машин, а также дисковыми образами. Провайдеры облачных услуг различаются временными показателями по выполнению операций над виртуальными машинами. Сценарий В отличается от А добавлением еще одного провайдера с чуть более быстрой инфраструктурой, аналогичным образом сценарий С отличается от В.

Разработанный алгоритм оценки и прогнозирования характеристик потока заявок пользователей для получения доступа к виртуальным рабочим окружениям исследовался совместно с алгоритмом эффективного масштабирования и распределения нагрузки на пулы виртуальных машин (обозначим его в качестве PredScaler). Исследование проводилось в сравнении с алгоритмом масштабирования, основанном на пороговых правилах

(минимальной и максимальной загруженности ресурсов), который не использует прогнозные значения (ThreshScaler).

На рисунках 1 и 2 показаны соответственно графики метрик загруженности вычислительных ядер виртуальных машин и индекса их сбалансированности. Значения метрик исследовались в зависимости от коэффициента нагрузки, определяемого интенсивностью появления заявок пользователей на запуск виртуальных рабочих окружений. Первые 20 минут симуляции значения метрик не учитывались.

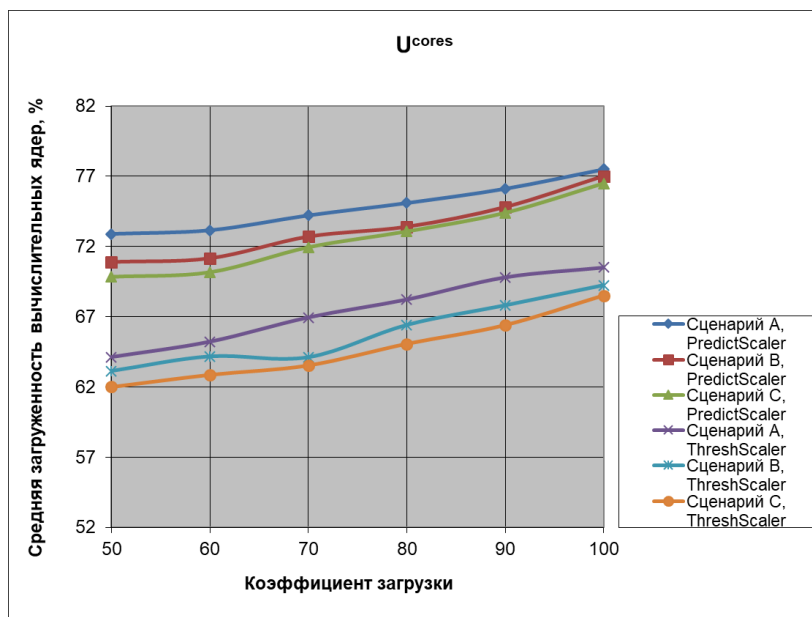


Рисунок 1 – Графики средней загруженности вычислительных ядер

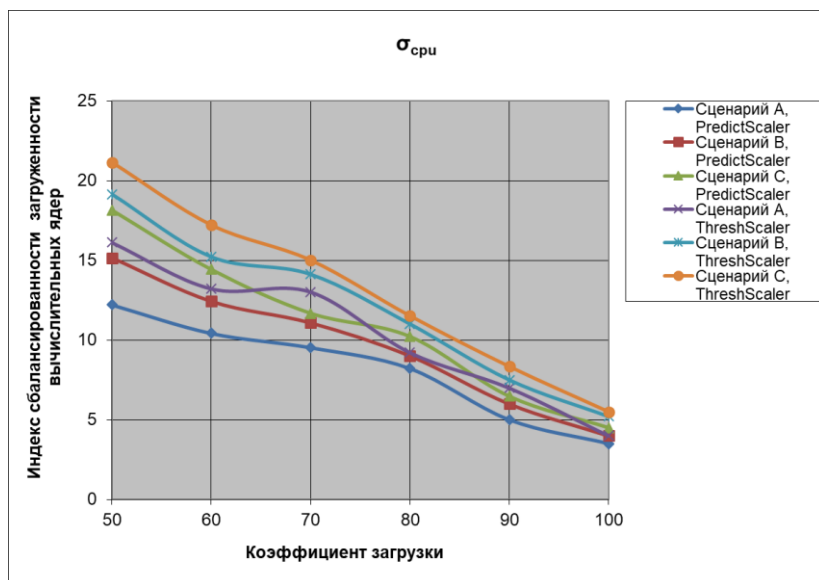


Рисунок 2 – Графики индекса сбалансированности загруженности вычислительных ядер для исследуемых алгоритмов масштабирования

Анализ графиков показывает, что предложенный алгоритм PredScaler демонстрирует большую эффективность, чем ThreshScaler по всем сценариям.

PredScaler увеличивает загруженность ядер процессоров на 6.3-8.8% для сценария А, на 7-8.6% для В и 7.3-8.4% для С в абсолютном выражении. При этом в среднем дисбаланс загрузки ядер у PredScaler меньше.

На рисунке 3 приведены графики среднего времени выполнения запросов на запуск DaaS сервисов для обоих алгоритмов масштабирования. Для алгоритма PredictScale в сценариях А, В и С среднее время запуска соответственно составляет 11.47, 10.34 и 9.10 мин., что соответственно на 19%, 20% и 21% быстрее алгоритма TreshScale в относительном выражении.

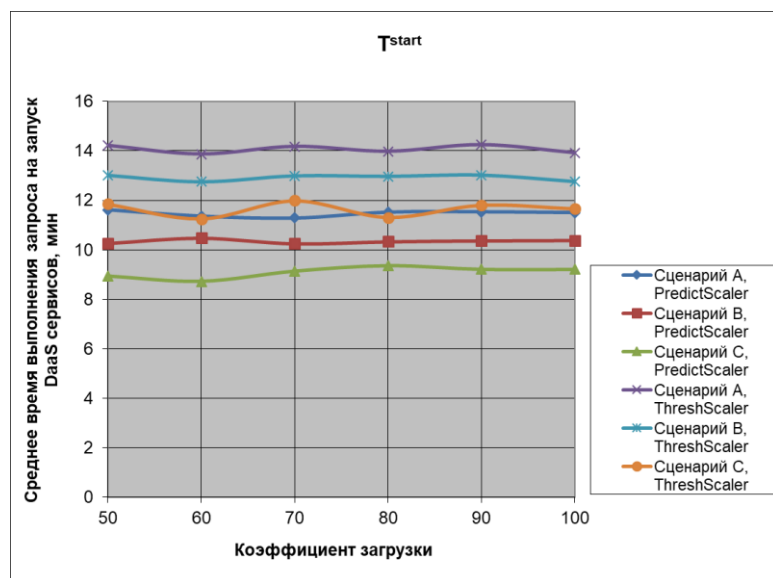


Рисунок 3 – График среднего времени выполнения запросов пользователей на запуск DaaS сервисов

Также видно, что среднее время стабилизировалось для всех сценариях практически независимо от коэффициента нагрузки.

Рассмотрим влияние разработанного алгоритма миграции контейнеров с виртуальными рабочими окружениями между виртуальными машинами пулов на индекс сбалансированности загруженности вычислительных ядер (см. рисунок 4) в сочетании с алгоритмом PredictScale дает в среднем улучшение от 4 до 18% для разных сценариев в относительном выражении.

В 2016 году в рамках проекта по созданию «Методического электронного образовательного центра Министерства образования Оренбургской области и Оренбургского государственного университета» была развернута облачная система коллективного доступа, которая называется «Ресурсный центр» [4]. В данном исследовании чтобы не реализовывать с нуля прототип мультиоблачного центра коллективного доступа к удаленным рабочим окружениям и программному обеспечению за основу был взят ресурсный центр, его инфраструктурные модули были модифицированы и дополнены с целью реализации разрабатываемых алгоритмических решений.

Ресурсный центр развернут с использованием ресурсов частного облака Оренбургского государственного университета (сервера IntelXeonE5, 64 Гб RAM), а также публичного провайдера 1Cloud (сервера Cisco B200 (3

GHz), Cisco B200-M4 (2.2 GHz)). Конфигурации пулов развернутых виртуальных машин приведены в таблице 1.

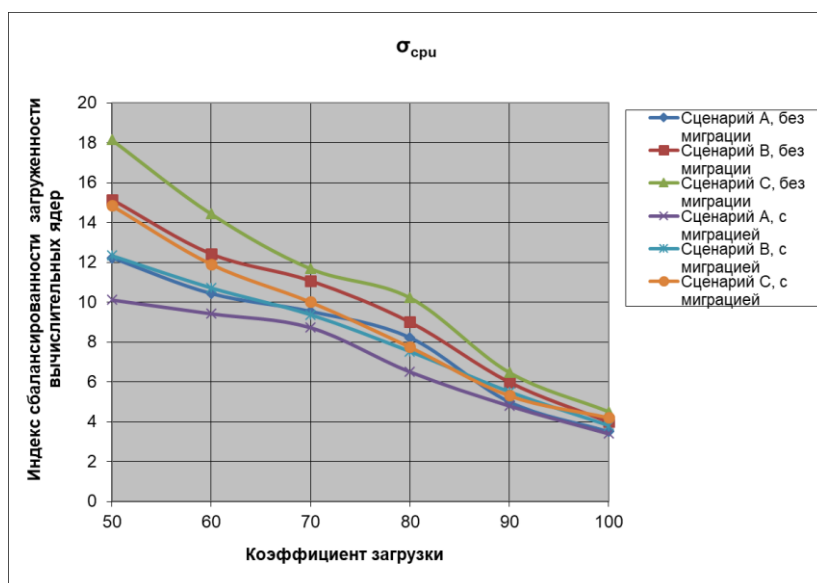


Рисунок 4 – Графики индекса сбалансированности загрузки вычислительных ядер для случаев с алгоритмом миграции и без него

Таблица 1 – Конфигурации пулов развернутых виртуальных машин

№ Пула	Расположение	Конфигурация	Первоначальное количество виртуальных машин
1	Приватное облако	4 vCPU, 16 Гб RAM, 256 Гб HDD	3
2	Приватное облако	2 vCPU, 8 Гб RAM, 256 Гб HDD	3
3	Публичное облако	24 vCPU, 120 Гб RAM, 1000 Гб SSD	3
4	Публичное облако	12 vCPU, 60 Гб RAM, 500 Гб SSD	3

Исследование проводилось с использованием 4х готовых дисковых образов виртуальных машин со всем предустановленным программным обеспечением.

Также дополнительно для экспериментальных исследований было разработано два инструмента: генератор заявок пользователей на запуск рабочих инструментов через REST-интерфейс и набор скриптов для имитации активности пользователей по работе с программами внутри окружений.

На рисунке 5 приведены графики зависимости средней загрузки вычислительных ядер для новой (со всеми разработанными алгоритмами) и

старой версий ресурсного центра. Средняя загрузка вычислительных ядер увеличилась до 6% в абсолютном выражении за счет разработанных алгоритмов.

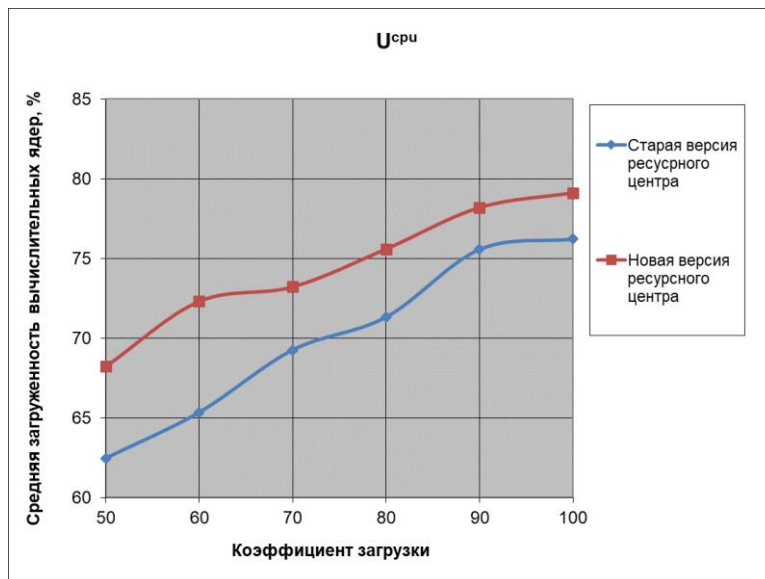


Рисунок 5 – Графики средней загрузки вычислительных ядер для старой и новой версии ресурсного центра

Графики индекса сбалансированности загрузки вычислительных ядер приведены на рисунке 6. Очевидно небольшое улучшение данной метрики для новой версии ресурсного центра.

Среднее время выполнения запроса на запуск DaaS-сервисов для новой версии ресурсного центра составило 11.47 мин., что быстрее старой версии на 14.4%.

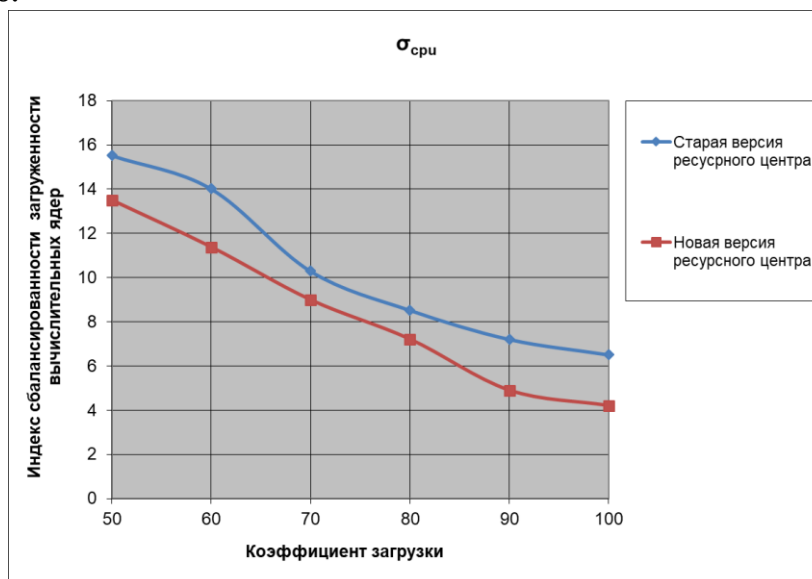


Рисунок 6 – Графики индекса сбалансированности загрузки вычислительных ядер для старой и новой версии ресурсного центра

Проведенные экспериментальные исследования разработанных алгоритмов работы мультиоблачного центра коллективного доступа к удаленным рабочим окружениям и программному обеспечению показывают улучшение его работы по метрикам производительности и сбалансированности. Результаты, полученные с помощью симулятора, согласуются с результатами прототипа.

Исследования проведены при финансовой поддержке РФФИ (проект 18-37-00460 мол_а) и гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9).

Список литературы

1. Полежаев П.Н., Легашев Л.В. Моделирование мультиоблачного центра коллективного доступа к удаленным рабочим окружениям и программному обеспечению // Сборник трудов VIII Всероссийской научно-практической конференции «Современная техника и технологии: проблемы, состояние и перспективы». – 2018. – С. 185-191

2. Полежаев П.Н., Легашев Л.В. МАСШТАБИРОВАНИЕ ОБЛАЧНЫХ СЕРВИСОВ ДЛЯ МУЛЬТИОБЛАЧНОГО ЦЕНТРА КОЛЛЕКТИВНОГО ДОСТУПА // Университетский комплекс как региональный центр образования, науки и культуры [Электронный ресурс]: материалы Всероссийской научно-методической конференции; Оренбург. гос. ун-т. - Электрон. дан. - Оренбург: ОГУ, 2019. С. 1882-1888.

3. Polezhaev P., Legashev L. Shukhman A., Bolodurina I. Simulation Modeling of Virtual Machine Based Services in Multi-Cloud Shared Access Centers // Advances in Intelligent Systems Research, volume 166, 2019. - P. 219-224

4. Shukhman A., Bolodurina I., Polezhaev P., Ushakov Yu., Legashev L. Creation of regional center for shared access to educational software based on cloud technology // Selected Papers of the XI International Scientific-Practical Conference Modern Information Technologies and IT-Education (SITITO 2016). CEUR Workshop Proceedings (CEUR-WS.org). Online Proceedings for Scientific Conferences and Workshops. - Vol-1761. - PP. 180-188

АКТИВИЗАЦИЯ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ МАТЕМАТИКИ

Максименко Н.В.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

В течение многих лет исследователи, говоря об учебной деятельности и ее успешности, в первую очередь имели в виду ведущую роль интеллектуального развития личности. Без сомнения, значение этого момента недооценивать нельзя. Но некоторые экспериментальные исследования заставляют взглянуть по-другому на задачу соответствия мотивационного и интеллектуального факторов. Например, в результате одного из экспериментов Реана А.А. были обнаружены интересные факты. Изучив по шкале общего интеллекта группу студентов – будущих педагогов и сравнив результаты тестирования с данными о степени учебной успеваемости, было обнаружено, что никакой явной взаимосвязи интеллекта с успеваемостью ни по общеобразовательным дисциплинам, ни по специальным предметам нет. Этот удивительный результат получил подтверждение и в трудах Якунина В.А. и Мешкова Н.И. Обнаружена еще одна важная закономерность: выяснилось, что «сильные» и «слабые» студенты действительно отличаются друг от друга. Но не по интеллектуальному уровню, а по качеству, силе и виду мотивации учебной деятельности. Сильным студентам присуща внутренняя мотивация: им необходимо овладеть профессией на значительном уровне, они ориентируются на приобретение прочных специальных знаний и практических умений. Если взять слабых учащихся, то их мотивы чаще всего внешние, обусловленные ситуацией: для таких студентов прежде всего необходимо уйти от осуждения и наказания за плохую учебу, не лишиться стипендии и т.п.

Данные исследования позволяют с уверенностью заявлять, что высокая положительная мотивация может компенсировать отсутствие особых способностей или ограниченный запас знаний, умений и навыков, играя роль компенсаторного фактора. Но в обратную сторону компенсаторный механизм не действует, т. е. каким бы талантливым ни был студент, без стремления к учебе успехов он не добьется.

Я формирование мотивации осуществляю в ходе организации учебной работы, перехода с одного вида деятельности на другой, обучения студентов навыкам самостоятельной постановки задач и их решения в условиях затруднений за счет привлечения учащихся к оценивающей деятельности – самооценке и самоконтролю. При формировании целенаправленной учебной деятельности важно учитывать, что задания повышенной трудности могут блокировать деятельность студентов, поэтому ее помехоустойчивость лучше отрабатывать шаг за шагом. Я стараюсь не ограничиваться только

положительным подкреплением учебной работы, т.к. переживания неудачи может подводить студентов к самостоятельному получению решения, к постановке обязательных целей, к обсуждению их практичности. Очень важно при формировании положительной мотивации учения не просто излагать научную информацию и эпизодически применять проблемные методы, а добиваться, чтобы кроме усвоения знаний у студентов формировалось мировоззрение, чтобы у будущих специалистов развивались творческие способности и навыки самостоятельного добывания и применения знаний в профессиональной деятельности и в жизни. Для этого нужно выделить важнейшие методы, формы, средства и критерии качества обучения, обеспечивающие условия для выявления творческого потенциала личности.

Чтобы все эти сложные дидактические проблемы решались, необходимо активизировать самостоятельную работу учащихся. Поэтому каждый преподаватель должен быть технологом, руководителем творческой самостоятельной работы студентов, на базе которой идет формирование их профессиональной деятельности, которая осуществляется по собственному побуждению, наблюдается развитие рефлексии, принимает регулярный характер процесс самовоспитания.

В педагогике вузов самостоятельная работа студентов рассматривается как особая форма специально организованной учебной деятельности. К тому же, она определяется как компонент учебно-профессиональной деятельности, которая имеет соответствующую мотивацию, цель, предмет, условия и систему воплощения: когда самостоятельная работа учащегося занимает значительную часть его подготовки как специалиста, он может научиться при определенной ее организации разбирать проблемные ситуации, излагать задачу, обнаружить и разъяснить алгоритм ее решения, реализовывать его. Поэтому самостоятельную работу студентов я стараюсь организовать так, чтобы у них возникли мотивы, стимулирующие к преумножению приобретенных знаний, способствующие активизации и развитию мышления, интеллектуального ресурса. Динамика и выражение интеллекта возможны лишь в определенной деятельности, в которой процессы интеллектуального развития и обучения по применению знаний являются прочно связанными и совместно обусловленными.

Необходимо уделить внимание информационно-деятельностному подходу к профессиональной подготовке и развитию личности студента. Основным его смыслом является организация учебно-профессиональной деятельности с учетом двойственной природы мышления. Главное в том, что преподаватель, организуя самостоятельную работу, должен не просто сообщать учебный материал, а сосредотачивать внимание учащихся на отличительных чертах передаваемой информации и давать советы по углублению знаний, организовывать получение навыков по их использованию. К примеру, определение производной функции – одно из ключевых понятий математики. К сожалению, у учащихся создается мнение о том, что в любом случае производная – это скорость движения. Но это не так.

Производную можно рассматривать как скорость, но скорость изменения функции относительно ее аргумента.

В данных случаях самостоятельную работу студентов стараюсь пополнить особыми задачами на нахождение разного рода скоростей (движения, роста стоимости во времени, относительно затрат и т.д.). В итоге растет точность знаний, и учащиеся получают необходимые навыки их практического применения. Я использую задания, организующие изучение разных способов решения задач. В связи с этим можно говорить о получении необходимого умения самостоятельного поиска знаний, развитии обобщенных представлений о соответствующей методологии.

Другим приемом формирования положительной мотивации учения является организация совместной учебной деятельности. У студента есть возможность осуществить свое взаимодействие с партнерами по коллективной работе, чтобы овладение знаниями, умениями прошло наиболее плодотворно. Непосредственно нацеленность на взаимодействие с партнерами указывает на присутствие у студентов мотивации совместной учебной работы. Преподаватель должен создать условия для возникновения учебной ситуации: потребности студентов в совместной деятельности и содержание обучения. Третья составляющая, без которой невозможно разрешение учебной ситуации, – преподаватель. Без взаимодействия с ним стремление студентов к овладению способами совместной работы не будет осуществлено и через какое-то время интерес к коллективному выполнению учебных задач исчезнет и у самых мотивированных к этому типу деятельности студентов. При совместной активной деятельности повышается творческая активность студентов, которая проявляется в стремлении освоить новые виды деятельности[1].

Предпосылками развития творческой активности являются преобладание активного познавательного интереса в мотивационной структуре личности учащегося и творческий характер учебно-познавательной деятельности. Первое условие выполняется, если старания педагога и студента направлены на формирование внутренних мотивов познавательной деятельности, которые стимулируют умственные способности и взаимодействия с ними, активизируют и выход за рамки заданного. Второе условие гарантируется ориентацией участников процесса обучения на творчество. В этом случае необходимые репродуктивные действия являются частью по сути творческого процесса, который в обучении трактуется не только как познание механизмов деятельности, но и как развитие нужных для творчества качеств личности.

Условиями созидательной активности студентов являются: выражение интеллектуальной инициативы; присутствие оптимальной мотивации, степень формирования творческих способностей и умений; демонстрация самостоятельности и способности к самоорганизации в учебно-познавательной деятельности. Преподавателю необходимо просчитывать эффективность своей работы по формированию мотивации, подводить ее

итоги. Плоды этой работы лучше всего оценивать по действенности отношения студентов к учению. Сопоставление начальных данных с изменениями в мотивации, которые появились в результате воздействия, характеризует плодотворность развития мотивационной сферы. На основе данных и выводов об эффективности работы по формированию мотивации преподаватель ставит задачи последующего учебно-воспитательного процесса.

Результаты диагностики первокурсников в начале учебного года выявили слабую мотивацию учебной деятельности, низкий уровень знаний, недостаточный навык самостоятельной деятельности, отсутствие у большинства творческого отношения к работе и стремление к саморазвитию.

Постоянное стимулирование самостоятельности и творческого отношения к изучению математики содействует осознанию студентами скрытых возможностей, разработке собственного метода усвоения учебной информации и способности оценить значимость этого события в своей познавательной деятельности. К концу учебного года у студентов повысился уровень познавательной мотивации, обозначились сдвиги в самоорганизации и саморегуляции труда, студенты стали более активными и инициативными на занятиях. Мне стало легче организовывать выполнение заданий в микрогруппе, так как у студентов улучшились коммуникативно-творческие способности.

Список литературы

1. Максименко, Н.В. Проблемы актуализации мотивации академических достижений студентов как факторы повышения качества обучения в университете [Электронный ресурс] / Н.В. Максименко // Вестник ОГУ. – 2018. – №6 (218). – С. 40-46. Режим доступа: http://vestnik.osu.ru/2018_6/7.pdf

МЕТОДЫ КЛАСТЕРИЗАЦИИ ПОИСКОВЫХ ЗАПРОСОВ

Морковина Э.Ф., канд. пед. наук, доцент, Ходырева Д.В.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет»

В современном обществе многие социальные, культурные, экономические явления и процессы представляются в глобальном информационном пространстве, что ведет к росту количества информационных ресурсов в сети. В подобных условиях увеличивается конкуренция среди информационных источников в сети Интернет, и уже недостаточно быть представленным в сети, необходимо иметь высокий рейтинг ресурса, в том числе в поисковых системах, что особенно актуально для коммерческих продуктов.

Решением этой проблемы является оптимизация веб-сайта не только для потенциального конечного пользователя, но и для поисковой машины, которая будет проводить ранжирование и присваивать Интернет-ресурсу определенную позицию на странице результатов поиска.

Поисковая оптимизация веб-сайта (Search Engine Optimization, SEO), включает в себя комплекс технологий, методов и приемов, позволяющих поднять рейтинг веб-ресурса в процессе ранжирования поисковой системы по определенным запросам.

Для максимально грамотного и эффективного продвижения сайта специалистами по оптимизации используется семантическое ядро.

Семантическое ядро сайта – это упорядоченный набор слов, их морфологических форм и словосочетаний, которые наиболее точно характеризуют вид деятельности, товары или услуги, предлагаемые данным ресурсом. Семантическое ядро имеет центральное ключевое слово, как правило, высокочастотное, а все остальные ключевые слова в нём ранжируются по мере убывания частоты совместного использования с центральным запросом в общей коллекции документов.

Кластеризация запросов семантического ядра – это группировка поисковых запросов на основе поисковой выдачи. В сущности, это автоматическое деление ключевых слов на группы.

Правильно составленное семантическое ядро – это основа SEO-оптимизации и гарантия того, что сайт будет на первых страницах выдачи поисковых систем. Работа любого SEO-оптимизатора начинается с оценки и составления грамотного семантического ядра. Все это определяет актуальность изучения данной темы.

В поисковой оптимизации при кластеризации поисковых запросов семантического ядра сайта сортировка поисковых запросов часто выполняется вручную, однако эту задачу вполне можно решить за меньшее время с применением специальных методов.

Постановка научной задачи: дан набор поисковых запросов, необходимо найти группы семантически похожих документов, то есть провести кластеризацию текстовых документов по тематике.

Для этого целесообразно выполнить следующие шаги:

- 1) векторное представление поисковых запросов (векторизация);
- 2) применение к полученным векторам методов кластеризации, основанных на расстоянии между ними;
- 3) моделирование тематики документов (тематическое моделирование);
- 4) визуализация кластеров.

Кластеризация документов – это процесс обнаружения естественных групп в коллекции документов. Задачу кластеризации можно представить так – дано множество объектов, в которой необходимо найти группы похожих объектов. Есть две основные проблемы: заранее неизвестно количество кластеров и неизвестны истинные кластеры, которые нужно выделять [3]. Поэтому задача решается очень тяжело – здесь невозможно оценить качество решения. Кластерный анализ занимает одно из центральных мест среди методов анализа данных, и представляет собой совокупность методов, подходов и процедур, разработанных для решения проблемы формирования однородных классов в произвольной проблемной области. Зачастую проблемная область представляет собой огромный массив текстовой информации, что делает невозможным его кластеризацию с помощью экспертов. Помимо этого, экспертная разбивка текстов на кластеры может быть субъективной и отражать лишь мнение конкретного эксперта [3].

В основе кластеризации текстов лежит способность сравнивать документы и определять их сходство. Документы, похожие друг на друга объединяются в группы, которые описывают темы и закономерности внутри корпуса. Эти закономерности могут быть дискретными (когда группы вообще не пересекаются) или нечеткими (когда документы настолько схожи, что их трудно различить). В любом случае, получающиеся группы представляют собой модель содержимого всех документов, которая позволяет легко отнести новые документы к той или иной группе.

Группы формируются только на основе попарной схожести описаний документов, и никакие характеристики этих групп не задаются заранее, в отличие от классификации документов, где категории задаются заранее [1].

В общем случае задача кластеризации текста распадается на две:

- техническая задача преобразования в некоторую матричную, векторную или любую другую модель;
- математическая задача кластеризации.

На первом этапе текстовые представления документов по определенным правилам переводят в векторные представления. На втором этапе необходимо применить к полученным векторам методы кластеризации, основанные на расстоянии между ними.

Этапы кластеризации поисковых запросов и методы, применяемые на данных этапах, представлены в таблице 1.

Чтобы выполнить машинное обучение на тексте, нужно преобразовать документы в векторные представления, к которым можно применить численное машинное обучение. Этот процесс называется извлечением признаков, или просто векторизацией, и является первым шагом на пути к анализу естественного языка.

Таблица 1 – Методы кластеризации поисковых запросов

№	Этапы кластеризации поисковых запросов	Методы
1	Векторизация поисковых запросов	– Частотные векторы – Прямое кодирование – Метод кодирования TF-IDF – Распределенное представление (word2vec, RusVectōrēs)
2	Кластеризация векторов	– Метод k-средних (k-means) – Иерархическая кластеризация
3	Тематическое моделирование	– Латентное размещение Дирихле (Latent Dirichlet Allocation, LDA); – Латентно-семантический анализ (Latent Semantic Analysis, LSA); – Неотрицательное матричное разложение (Non-Negative Matrix Factorization, NNMF).
4	Визуализация кластеров	– Метод t-распределенного стохастического вложения соседей (t-distributed Stochastic Neighbor Embedding, t-SNE) – Сингулярное разложение (Singular Value Decomposition, SVD) – Метод главных компонент (Principal Components Analysis, PCA)

Следующий этап – кластеризация полученных векторов. Данная задача решается с помощью обучения без учителя. Обучение без учителя затруднительно из-за отсутствия надежного способа оценить качество модели. Тем не менее, существуют методы, позволяющие количественно оценить сходство документов, которые могут быстро и эффективно обрабатывать большие корпуса и представлять интересную и актуальную информацию.

Метод *k-средних* – это эффективный и универсальный метод кластеризации, который хорошо масштабируется для обработки больших корпусов, особенно если кластеров не очень много и геометрия не слишком

сложна. В случаях с большим количеством кластеров и менее равномерно распределенными данными хорошей альтернативой может оказаться агломеративная кластеризация [4].

Для эффективного обобщения корпуса документов без меток часто требуется не только предварительная классификация, но и метод описания категорий. Это можно реализовать на этапе тематического моделирования с помощью метода латентного размещения Дирихле, латентно-семантического анализа или неотрицательного матричного разложения.

Оценить модели кластеризации в случае обучения без учителя не так просто, как в обучении с учителем, когда есть преимущество знания правильных и неправильных ответов. В кластеризации нет количественной оценки – успех модели зависит от того, насколько благополучно она обнаруживает закономерности, различимые и значимые для человека. Поэтому применение методов визуализации для оценки приобретает особую важность.

При применении алгоритмов кластеризации, оценка модели оказывается не такой простой, как в случае машинного обучения с учителем, когда имеются знания правильных и неправильных ответов. В кластеризации нет количественной оценки – относительный успех модели обычно зависит от того, насколько благополучно она обнаруживает закономерности, различимые и значимые для человека. По этой причине применение методов визуализации для оценки приобретает особую важность.

С помощью диаграмм плотности можно исследовать степень сходства документов по всем признакам. Для этой цели используется популярный метод распределенного стохастического вложения соседей *t*-distributed Stochastic Neighbor Embedding, *t*-SNE).

Метод *t*-SNE способен сгруппировать схожие документы путем разложения векторных представлений документов с большим числом измерений в два измерения (с использованием распределений вероятностей из оригинальной и разложенной размерностей). Разложением на два или на три измерения можно построить диаграммы рассеяния.

Объект *TSNEVisualizer* можно также использовать для визуализации кластеров при использовании его совместно с алгоритмом кластеризации. С помощью этого приема можно оценить эффективность разных методов кластеризации [2].

Оценить эффективность данных методов можно, применив их к задаче кластеризации поисковых запросов семантического ядра с помощью языка программирования Python с использованием библиотек *Scikit-Learn*, *NLTK*, *Gensim*, *spaCy*, *NetworkX* и *Yellowbrick*.

Описанные выше техники кластеризации могут являться базой для построения более эффективных кластеризаторов, будучи скомбинированы с разнообразными методами уменьшения размерности пространства признаков.

1. Безверхий, О. А. Самохвалова, С. Г. Кластеризация большого объема текстовых поисковых запросов [Электронный ресурс]. – Режим доступа: <http://pnu.edu.ru/ejournal/pub/articles/1331/>
2. Бенгфорт Бенджамин, Прикладной анализ текстовых данных на Python. Машинное обучение и создание приложений обработки естественного языка / Бенгфорт Бенджамин, Билбро Ребекка, Охеда Тони / – СПб.: Питер, 2019. – 368 с. ISBN 978-5-4461-1153-4. Гроховский, Л. SEO для бизнеса / Л. Гроховский, О. Хохловский, О. Шестаков, Р. Рзаев // М: Топ Эксперт. – 2015. – 200 с.
3. Елизаров, С. И. Разработка и Исследование методов и алгоритмов кластеризации для систем анализа данных / С. И. Елизаров [Электронный ресурс]. – Режим доступа: <http://www.eltech.ru/education/aspir/SIElizarov.doc> – 11.09.2016
4. Черникова, Д.А. Алгоритм кластеризации поисковых запросов / Д.А. Черникова / Евразийский Научный Журнал №12, 2017. [Электронный ресурс]. – Режим доступа: <http://journalpro.ru/articles/algorithm-klasterizatsii-poiskovykh-zaprosov/>

РАЗРАБОТКА САЙТА И МЕТОДЫ ЗАЩИТЫ БАЗЫ ДАННЫХ

Мухтубаева С.Н.

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Разрабатываемый сайт предназначен для ознакомления людей с теоретическими и практическими сведениями о криптографии. Целевая аудитория сайта – пользователи, привыкшие искать информацию в сети Интернет. Одна из задач сайта – это предоставление нужной информации посетителям, а также возможность оставить комментарии. Исходя из поставленных задач, Web-сайт должен предоставлять следующие возможности:

- при первом посещении сайта пользователь должен понять, для чего служит данный сайт, составить общее впечатление о нём, выяснить свои потребности в отношении сайта;
- если в дальнейшем пользователю не понравилась информация о выбранном им разделе, он может оставить свой комментарий.

Дизайн сайта играет важную роль в создании самого сайта. Web-сайт включает в себя: цветовое оформление, элементы навигации по сайту, текстовую информацию. Оформление сайта должно соответствовать следующим требованиям:

- внешний вид сайта должен соответствовать выбранной тематике;
- навигация по сайту должна быть удобной для пользователя;
- главные материалы, предложения и категории услуг должны быть расположены на первом плане, чтобы заинтересовать посетителя.

В верхней части страницы помещается название сайта, отражающее его тему. Название сайта находится на каждой странице и не изменяется в зависимости от местонахождения на сайте. Меню предназначается для навигации по сайту, в нём отображаются ссылки на все страницы сайта. Главная страница – страница, отображающаяся при первом входе на сайт. Её оформление и содержание даёт пользователю первое представление о сайте.

Любой Web-сайт создаётся с конкретной целью, он «заточен» под какие-то определённые функции. Основная функция сайта – информационная: пользователи приходят в сеть за информацией. Популярность любого проекта зависит от того, как полно и содержательно он её предоставит, насколько материалы Web-ресурса актуальны, как часто обновляются.

Жизненный цикл программного обеспечения – это непрерывный процесс, который начинается с момента принятия решения о необходимости создания ПО и заканчивается в момент его эксплуатации. Существует несколько видов жизненного цикла. Выбор каскадной модели заключается в том, что происходит последовательное выполнение этапов в строгом порядке.

Также такая модель жизненного цикла позволяет оценивать качество продукта на каждом этапе.

Этап 1 – Анализ

Постановка задачи: требуется реализовать сайт по криптографии, с постоянным обновлением задач и возможностью общения.

Цель создания сайта: ознакомление с задачами по криптографии, размещение данных о программах и конференций, проводимых для улучшения навыков, взаимодействие с аудиторией.

Этап 2 – Проектирование

Проектирование сайта включает 4 этапа:

- сбор информации;
- информационное пополнение;
- разработка структуры сайта;
- создание схемы сайта.

Этап 3 – Реализация

Программа должна быть написана на языке PHP с привязкой базы данных. Дизайн и структура сайта должны отвечать требованиям пользователей, а также креативность решения и его функциональность. Создание удобных и полезных сервисов для целевой аудитории. Разработка среды общения (форумы, блоги, доски объявлений). Создания опросов, тестирования. Качество и полнота контента, его соответствие лексике аудитории и принципам воспринимаемости контента на сайтах.

Этап 4 – Тестирование

Данный сайт должен соответствовать всем стандартам и правилам проектирования. Все элементы интерфейса программного продукта необходимо выполнить в размеренном стиле, где каждый элемент имеет своё определённое место на главном окне, не перекрывая элементы, находящиеся поблизости.

На Web-странице может находиться большое количество информационных элементов, поэтому для упрощения восприятия и различимости Web-разработчику необходимо производить их группировку. Разработка структуры Web-сайта является одним из ключевых моментов его создания, который в большой степени определяет эффективность его функционирования в будущем. С технической точки зрения структура сайта – это не что иное, как все его страницы, расположенные в порядке их значимости для пользователей, то есть иерархии. Исходя из этого можно выделить модули сайта.

Модуль	Описание
Управление контентом	Основной модуль сайта, позволяющий управлять его структурой и содержанием. Процесс создания разделов и подразделов прост и интуитивно понятен.

	Редактирование страниц максимально приближено к процессу работы в текстовом редакторе. Редактор отличается расширенными возможностями работы с таблицами и стилями сайта. Данный модуль позволяет управлять новостной лентой. В модуль встроена система разграничения прав доступа.
Файловый архив	Данный модуль предназначен для хранения и размещения на страницах сайта файлов разных типов.
Новости	Модуль предназначен для публикации новостей на сайте. Позволяет разделить новости на тематические и подгруппы.
Форум	Данный модуль позволяет владельцам ресурса организовать дискуссию на определённые темы, создав один или несколько форумов. В рамках выбранного форума зарегистрированные пользователи могут заводить новые темы и участвовать в обсуждении тем, заведённых другими участниками.
Вопрос-ответ	Модуль предназначен для приёма вопросов посетителей сайта. В определённых разделах сайта пользователю предоставляется возможность отправить вопрос по содержанию раздела Администратору. Сами вопросы и ответы на них публикуются на той же странице.
Письма с сайта администратору	Модуль предназначен для автоматической отправки писем на E-mail адреса со страниц сайта, без использования почтовых программ.
Поиск по сайту	Данный модуль предназначен для быстрого поиска текстовых материалов на страницах сайта. Поиск осуществляется по ключевому слову. Результаты поиска выдаются на специальной странице сайта в удобном и понятном для пользователя виде. При клике на ссылку пользователь попадает на соответствующую страницу.
Регистрация/авторизация	Модуль предназначен для регистрации новых пользователей и последующей авторизации для входа на закрытую часть

сайта. По уникальному логину и паролю происходит идентификация пользователя.
--

Существует множество средств для создания Web-сайтов, но лишь некоторые из них способны предоставить разработчикам инструменты для решения подавляющего большинства стоящих перед ним задач. При разработке Web-сайта из всех современных Web-технологий, позволяющих создавать интерактивные Web-страницы, необходимо выбрать наиболее подходящие для выполнения поставленных на первоначальном этапе задач.

Наряду с выбором средств для создания Web-сайта существуют и проблемы защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом. Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность. Под конфиденциальностью понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности. Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами.

Обычно в процессе обсуждения защиты баз данных на первый план невольно выходит риск их взлома и утраты конфиденциальной информации. Представляется колоссальных масштабов трагедия: поврежденная репутация сайта, необратимые финансовые потери и долгий реабилитационный период. Далее выстраивается цепочка возможных мер, своевременное принятие которых позволило бы предотвратить случившееся, начинается тщательный анализ неучтенных уязвимостей во избежание будущих ошибок.

Классическая схема защиты баз данных (БД) подразделяется на следующие обязательные процедуры:

- **Разграничение доступа** - каждый пользователь, включая администратора, имеет доступ только к необходимой ему согласно занимаемой должности информации.

- **Резервное копирование**, позволяющее восстанавливать данные на случай аппаратных или программных сбоев. Необходимо настроить регулярное резервное копирование базы данных и хранить файлы не только на жестком диске компьютера, но также дублировать их на ленту или жесткий диск другого компьютера в сети.

- **Контрольный след** позволяет регистрировать детальные сведения обо всех операциях пользователей с БД. Данная сохраненная информация играет весьма существенную роль в обнаружении несанкционированного вмешательства в базу данных, выявлении уязвимостей в системе защиты, а также устранении каких-либо внесенных искажений данных.

- **Шифрование данных** - шифровать необходимо как передаваемые в сети данные для защиты от перехвата, так и данные, записываемые на

носитель, для защиты от кражи носителя и несанкционированного просмотра/изменения не средствами системы управления БД (СУБД).

- **Аудит доступа к данным** - действия с критичными данными должны протоколироваться. Доступ к протоколу не должны иметь пользователи, на которых он ведется. В случае приложений, использующих многозвенную архитектуру, приведенные функции защиты также имеют место, за исключением защиты данных на носителе - эта функция остается за БД.

Таким образом, защита баз данных должна осуществляться поэтапно, начиная с принятия базовых мер. Описанные выше методы способны в определенной степени обеспечить конфиденциальность и целостность данных, однако их использование не гарантирует полной безопасности данных. Для повышения уровня сохранности информации в базе данных рекомендуется использование комплексных мер, включая интеграцию СУБД со специальными программными продуктами для защиты информации.

Список литературы

- 1 Веллинг, Л. Разработка веб-приложений с помощью PHP и MySQL [Текст] / Л. Веллинг, Л. Томсон. - Вильямс 2010 - 848 с.
- 2 Влацкая, И.В. Технология разработки программного обеспечения: методические указания к лабораторным и самостоятельным работам студентов / И.В. Влацкая, Н.А. Заельская, Н.С. Шамсутдинова. – Оренбург: ГОУ ОГУ. – 2008. – 58 с.
- 3 Уорд П. Метод 360 градусов / П. Уорд: ГИППО, 2006 ISBN 978-5-7410-1573-5.
- 4 Subtotal [Электронный ресурс]. – Режим доступа: <http://start.vsubtotal.ru>
- 5 Фримен, Э. Изучаем HTML, XHTML и CSS [Текст] / Э. Фримен. - СПб.: Питер, 2012. - 656 с.

РЕШЕНИЕ ЗАДАЧИ КАТЕГОРИАЛЬНОЙ РЕГРЕССИИ С ПОМОЩЬЮ НЕЙРОННЫХ СЕТЕЙ И ГРАДИЕНТНОГО БУСТИНГА ДЛЯ ПРОГНОЗИРОВАНИЯ УСПЕВАЕМОСТИ ОБУЧАЮЩИХСЯ МАССОВЫХ ОТКРЫТЫХ ОНЛАЙН-КУРСОВ

**Нигматулин Г.А., Парфёнов Д.И., канд. техн. наук,
Болодурина И.П., д-р техн. наук, проф., Запорожко В.В., канд. пед. наук
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

В настоящее время динамические процессы, протекающие в экосистеме массовых открытых онлайн-курсов, требуют постоянной объективной оценки, своевременной корректировки и управления [1]. Вследствие сложности и самостоятельности обучения в условиях образовательной онлайн-платформы, составление прогноза развития тех или иных событий, более известное как задача регрессии, и оценка достигнутых результатов, являются важной задачей для практического решения. Инструментами, позволяющими решить поставленную задачу, являются нейросети и градиентный бустинг.

Образовательный анализ данных используется для прогнозирования при решении разных образовательных задач, в частности, при реализации массовых открытых онлайн-курсов.

В рамках исследования М. Vitiello и его коллег рассмотрены онлайн-курсы, которые стартовали многократно. Авторы предложили извлечь важные характеристики для выявления группы учащихся, которые могут не завершить начатый курс. В последствие была предложена модель прогнозирования, основанная на расширенных деревьях принятия решений. Приняв такой подход, авторы добились точности вычислений в 80% [2].

Ученые из Китая имели другой взгляд на проблему: рассматривали явление отсева обучающихся с курсов как проблему временных рядов, и предложили прогностическую модель, основанную на рекуррентной нейронной сети (RNN) с ячейками кратковременной памяти. Данная модель обеспечила точность результатов на уровне 88,1% [3].

В работе [4] была предложена модель прогнозирования, которая основана на свёрточных нейронных сетях, объединяющих в одной структуре как извлечение, так и отбор признаков, а также классификацию обучающихся. Модель обеспечила точность, составляющую 86,75% [4].

Таким образом, авторы разработали модели прогнозирования, основанные на методах интеллектуального анализа данных, и выявили их точность. Однако данные методы были реализованы на ограниченном числе предсказательных признаков, которые оставались относительно похожими. В настоящее время остро стоит вопрос о необходимости проводить аналитику больших образовательных данных на основе обширного количества разнородных признаков и осуществлять их мониторинг в режиме реального

времени. В связи с этим авторы предложили решение задачи категориальной регрессии с помощью нейронных сетей разной типологии и градиентного бустинга для прогнозирования успеваемости обучающихся массовых открытых онлайн-курсов.

Решение поставленной задачи с помощью нейронной сети сводилось к выполнению следующей последовательности шагов: сбору данных для обучения, подготовке и нормализации данных, выбору количества слоев, обучению – настройке параметров сети, в основе которой лежит многоэкстремальная невыпуклая задача оптимизации функции ошибок, проверке адекватности обучения, окончательному обучению и сохранению нейронной сети.

Исходные данные для решения искомой задачи были получены из открытой базы наборов данных «Open University Learning Analytics Dataset». Данная база представляла собой анонимизированный набор больших данных образовательной аналитики Открытого университета (OULAD). В структуре данного набора содержались данные о курсах, сведения об обучающихся их взаимодействии с онлайн-курсами. Для построения модели был выбран курс, который перезапускался четыре раза, а количество оценочных средств которого составило 12 заданий. Нами были извлечены данные по тем обучающимся, которые сдали все оценочные задания в курсе. Количество полученных наборов данных составило 38192 записей.

Описание задачи

Каждый обучающийся онлайн-платформы определялся рядом фактических характеристик, значения которых являлись входными значениями для нейронной сети, решающей искомую задачу регрессионного анализа:

X_1 – пол обучающегося: М – мужской, Ж – женский;

X_2 – уровень высшего образования при изучении курса;

X_3 – возрастная группа, к которой относился обучающийся: от 0 до 35 лет включительно, от 35 лет до 55 лет, старше 55 лет;

X_4 – показатель, характеризующий наличие инвалидности у обучающегося: Y – Да, N – Нет;

X_5 – оценка за предыдущий (i-1) этап обучения (i>1), (баллов);

X_6 – срок сдачи оценочного задания (i-1) этапа оценивания (i>1), (дней).

По завершении обучения были предложены следующие признаки:

Y_1 – прогнозируемая оценка по результатам предыдущих (i) этапов обучения (i>1), (баллов);

Y_2 – прогнозируемый срок сдачи оценочного задания (i) очередного этапа обучения (i>1), (дней);

где $X_5, Y_1 \in [0, 100]$ (баллов), $X_6, Y_2 \in [0, 124]$ (дней).

На основе данных, описанных выше, были реализованы следующие способы решения задачи категориальной регрессии для прогнозирования

успеваемости обучающегося и планирования индивидуального срока обучения на каждом очередном этапе освоения онлайн-курса:

1) с использованием двух отдельных нейронных сетей для прогнозирования каждого показателя отдельно;

2) с применением одной нейронной сети для одновременного прогнозирования обоих показателей;

3) при помощи модели градиентного бустинга.

Реализация предложенных моделей

Опишем гиперпараметры каждой модели.

В случае построения двух отдельных нейронных сетей у каждой сети на входном слое располагались 14 перцептронов, равных количеству исходных признаков после проведения dummy-кодирования. Далее следовал скрытый слой, в котором была реализована активационная функция гиперболического тангенса, и в конце – выходной слой, представляющий из себя один перцептрон, прогнозирующий один из показателей: для первой нейронной сети – оценку (в баллах), а для второй – срок сдачи (в днях). Для реализации нейронных сетей использовалась библиотека Keras – библиотека нейронных сетей с открытым исходным кодом, написанная на языке Python. Параметрами нейронных сетей являлись следующие: количество нейронов в скрытом слое, функция активации, целевая функция, алгоритм оптимизации параметров, количество эпох обучения нейронной сети.

Для реализации второго случая – когда задача категориальной регрессии решалась с помощью одной нейронной сети с одновременным прогнозированием обоих показателей – использовался аналогичный подход, однако вместо одного выходного нейрона использовалось два – для каждого из прогнозируемых признаков.

При реализации третьего способа использовался метод градиентного бустинга из библиотеки CatBoost, эффективно работающей с категориальными признаками и использующей деревья решений. Функцией ошибки в данной модели являлась средняя абсолютная ошибка прогнозирования. Параметрами данной модели были установлены максимальное количество итераций и глубина деревьев. При этом большое значение имел коэффициент скорости обучения – параметр градиентных алгоритмов, позволяющий управлять величиной коррекции весов на каждой итерации.

Результаты вычислительных экспериментов

Используя приведенные выше модели, нами были проведены серии экспериментов по прогнозированию успеваемости и срока сдачи запланированных оценочных средств. Полученные результаты показали (таблицы 1 и 2), что предложенные алгоритмы обладали высокой эффективностью по критерию средняя абсолютная ошибка. Данное обстоятельство являлось важным при выполнении дальнейшего проектирования интеллектуальной системы платформы онлайн-обучения, способной формировать индивидуальные образовательные траектории для

повышения успеваемости обучающихся и обеспечения оптимальности временного планирования процесса обучения.

Экспериментальные результаты, полученные на разных 11-ти реальных наборах данных, показали высокую эффективность предложенных моделей.

Таблица 1 – Средняя абсолютная ошибка (баллов) прогнозирования оценки на 11-ти наборах данных

	1	2	3	4	5	6	7	8	9	10	11
Две отдельные нейронные сети	9,579	8,870	7,808	7,151	7,717	5,255	7,190	6,750	6,019	7,043	6,785
Одна нейронная сеть с 2-мя выходами	9,600	8,827	7,760	7,087	7,619	5,325	7,165	6,749	6,048	7,187	6,787
Catboost - градиентный бустинг	9,516	8,636	7,685	6,783	7,556	4,957	6,993	6,591	5,868	7,033	6,725

Таблица 2 – Средняя абсолютная ошибка (дней) прогнозирования срока сдачи задания на 11-ти наборах данных

	1	2	3	4	5	6	7	8	9	10	11
Две отдельные нейронные сети	1,981	3,552	2,520	2,647	4,141	2,507	2,322	1,938	1,342	1,099	2,482
Одна нейронная сеть с 2-мя выходами	1,904	3,310	2,497	2,874	4,783	2,592	2,510	1,131	1,599	1,455	2,398
Catboost - градиентный бустинг	1,430	2,698	2,134	2,298	5,404	2,075	2,073	1,057	1,979	1,820	2,880

Как показали результаты, рассмотренные модели адекватно решали поставленную задачу прогнозирования успеваемости обучения. На основе 11-ти проведённых экспериментов были получены следующие результаты средней абсолютной ошибки (таблица 3).

Таблица 3 – Средние абсолютные ошибки по результатам 11-ти экспериментов

	Средняя абсолютная ошибка 'оценки' (баллов)	Средняя абсолютная ошибка 'времени' (дней)
Две отдельные нейронные сети	7,288	2,412

Одна нейронная сеть с 2-мя выходами	7,287	2,459
Catboost градиентный бустинг	7,122	2,350

Анализируя полученные данные, можно судить, что все рассмотренные модели решали задачу корректно.

Сделан вывод, что предложенные методы можно рекомендовать использовать при проектировании индивидуальных образовательных траекторий с целью повышения успеваемости обучающихся и обеспечения оптимальности временного планирования процесса обучения.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 18-37-00400, №18-07-01446, № 19-47-560011, № 20-07-01065, а так же гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-860.2019.9).

Список литературы

1. Запорожко, В.В. Разработка структурной модели массовых открытых онлайн-курсов на базе современных облачных образовательных платформ / В.В. Запорожко, Д.И. Парфенов // Современные наукоемкие технологии, 2017. – № 3. – С. 12-17.
2. Vitiello, M. Walk, S. Helic, D. Chang, V., Guetl, C. Predicting dropouts on the successive offering of a MOOC. In Proceedings of the 2017 International Conference MOOC-MAKER. 2017. pp. 11-20.
3. Tang, J., Qiu, J., Liu, T.X., Gong, J., Zhang, C., Zhang, Q., Xue, Y. Modeling and predicting learning behavior in moocs. In Proceedings of the Ninth ACM International Conference on Web Search and Data Mining. 2016. pp. 93-102.
4. Qiu, J., Tang, J., Liu, T., Gong, J. Modeling and predicting learning behavior in MOOCs. In ACM International Conference on Web Search and Data Mining. 2016. pp. 93-102.
5. Ren, Z. Rangwala, H. Johri, A. Predicting performance on MOOC assessments using multi-regression. In Proceedings of the International Conference Educational Data Mining. 2016. pp. 484-489.
6. Brinton, C.G., Chiang, M. MOOC performance prediction via clickstream data and social learning networks. In Proceedings 2015 IEEE Conf. Comput. Commun., 2015. pp. 2299-2307.

ОБ ОРГАНИЗАЦИИ ПРОПЕДЕВТИЧЕСКОГО ИЗУЧЕНИЯ МАТЕМАТИЧЕСКОГО РАЗДЕЛА «ЛИНЕЙНАЯ АЛГЕБРА» СТУДЕНТАМИ ГУМАНИТАРНЫХ НАПРАВЛЕНИЙ

**Павленко А.Н., канд. физ.-мат. наук, доцент,
Пихтилькова О.А., канд. физ.-мат. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Как правило, изучение раздела «Линейная алгебра» дисциплины «Высшая математика» («Математика») студентами гуманитарных направлений происходит следующим образом:

- 1) введение понятия («Определитель», «Матрица», «Система линейных уравнений» и т.д.);
- 2) приведение (с доказательствами или без них) свойств и методов решений;
- 3) рассмотрение приложений данного понятия, важность практической применимости которых для студентов гуманитарных направлений является сомнительной.

Очевидно, что данный общепринятый способ изучения абстрактного и, следовательно, трудновоспринимаемого материала не способствует высокой мотивации к его изучению.

С целью решения вышеприведенной проблемы в настоящее время в высшей школе всё шире [1-4] применяется двухэтапное изложение учебного материала, при котором перед традиционным изучением раздела дисциплины (дисциплины) проводится его краткое пропедевтическое изложение. В ходе которого студенты должны воспринять основы учебного материала и уяснить широту его приложений, пока не вникая в частности, которые мешают восприятию основных положений рассматриваемого математического раздела.

Учитывая небольшие объемы контактной работы, отводимые дисциплинам математического цикла на гуманитарных направлениях, представляется целесообразным отнести пропедевтическое изучение раздела «Линейная алгебра» во внеаудиторную самостоятельную работу при использовании информационных технологий.

Предлагается для организации самостоятельного пропедевтического изучения данного математического раздела использовать интерактивные методические указания. Для повышения эффективности которых в них могут быть размещены:

- статичные и динамические изображения;
- файлы мультимедиа, содержащие краткие объяснения наиболее важных моментов, динамические чертежи, видео функционирования различных технических приложений данного раздела и т.д.;

- гиперссылки на более подробное изложение положений методических указаний;

- приложений на языках высокого уровня, генерирующих задания в форме тестов [5-7] для самоконтроля усвоения изучаемого материала.

Ниже приведем примерное содержание интерактивных методических указаний для самостоятельного пропедевтического изучения раздела «Линейная алгебра». Предлагается выделить следующих разделов.

1. Приведение исторических сведений о приложениях раздела «Линейная алгебра».

На данном этапе требуется показать в силу каких причин появилась необходимость в данном математическом разделе с указанием конкретных персоналий. Не следует претендовать на полное изложение исторических сведений и приведение всех приложений изучаемого материала, а целесообразно изложить несколько фактов, которые в занимательной форме смогут стимулировать интерес студентов к изучаемой дисциплине.

Акцентировать внимание студентов на важности систем линейных алгебраических уравнений можно с помощью изложения исторического факта, что первый в США цифровой компьютер был в 1942 г. создан Джоном Атанасовым (1903-1995) именно для решения «больших» систем линейных алгебраических уравнений.

В обзоре приложений систем линейных уравнений следует указать, что огромное количество задач математической физики (предсказание погоды, гидро- и аэродинамика, исследование композитных материалов, гравirazведка полезных ископаемых, изучение процессов при атомных взрывах и т.д.) при своем численном решении сводятся к системам линейных алгебраических уравнений.

Стимулировать интерес студентов к понятию «матрица» представляется возможным с помощью упоминания о теории межотраслевого баланса лауреата Нобелевской премии, известного американского экономиста Василия Леонтьева (1905-1999) и отметить эффективность ее применения для исследования экономики США в 1930-е годы, а также для принятия решений об объемах и структуре ленд-лиза и выборе целей для бомбардировок в гитлеровской Германии.

2. Изложение основных понятий и идей раздела «Линейная Алгебра».

Вводить новые понятия целесообразно на примерах, непосредственно связанных с направлением (специальностью) обучения студентов. При этом математическое понятие не только приобретет наглядность и конкретный смысл, но исходя из содержания рассматриваемой задачи, часто могут быть легко обозримы и свойства данного понятия, и методы его нахождения (решения).

В качестве задач, приводящих к понятию системы линейных алгебраических уравнений можно рассмотреть задачи о раскрое, номенклатуре производства, загрузки транспортных средств и т.д. [8].

Введение понятия определителя наглядно и естественно происходит при решении в общем виде системы линейных уравнений с двумя неизвестными. Понятие определителя второго порядка позволяет легко запомнить полученные формулы для неизвестных и еще при этом получить формулы Крамера.

Весьма сложное для восприятия определение произведения матриц и смысл введения обратной матрицы делаются очевидными при рассмотрении матричной формы записи систем линейных алгебраических уравнений.

3. Контроль за эффективностью пропедевтического обучения.

С целью повышения мотивации студентов к пропедевтическому изучению нового материала и получения оперативной информации о результатах его усвоения предлагается вести текущий и/или итоговый тестовый контроль. Последний может содержать как вопросы теоретического характера, так и задачи, раскрывающие в доступной и наглядной форме основные идеи изучаемого раздела или всей дисциплины. При отнесении пропедевтического курса в самостоятельную работу возможно применение существующих в вузах дистанционных компьютерных систем компьютерного тестирования.

В силу предпочтительности наличия у каждого студента индивидуального варианта тестового контроля, представляется целесообразным использование интерактивных компьютерных генераторов однотипных заданий [5-7].

Список литературы

1. Сазонов, В.Н. Пропедевтический курс математического анализа: конспект лекций / В.Н. Сазонов. – М.: Моск. станкоинструм. ин-т., 1989. – 52 с.: ил.
2. Кузнецова, В.А. О целесообразности вводного пропедевтического курса в университете / В.А. Кузнецова // Вестн. Тамбовского гос. ун-та. – 2003. – № 3, том: 8. – С. 406.
3. Темникова И.С. Восстановление школьных и пропедевтика вузовских математических знаний с помощью компьютерных средств обучения: материалы Международной научно-практической конференции “Информационные технологии в образовании и фундаментальных науках (ИТО-Поволжье-2007)”, Казань 18-21 июня 2007 г. / ТГГПУ, Казань.
4. Павленко, А.Н. О целесообразности использования лекционных занятий пропедевтического характера при изучении математических дисциплин гуманитарных направлений / Павленко А.Н., Пихтилькова О.А. // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всерос. науч.-метод. конф. (с междунар. участием), 23-25 янв. 2019 г. – Оренбург : ОГУ, 2019. - С. 1920-1923.
5. Кручинин, В.В. Использование деревьев И/ИЛИ для генерации вопросов и задач // Вестник Томского государственного университета. – 2004. – №284. - С. 183 – 186.

6. Лаптев, В.В. Генерация вариантов заданий для лабораторных работ по программированию / В.В. Лаптев, В.В. Толасова // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2010. – № 1. – С. 127-131.

7. Зорин, Ю.А. Использование алгоритмов комбинаторной генерации при построении генераторов тестовых заданий // Дистанционное и виртуальное обучение. – 2013. – №6. – С. 54 – 59.

8. Сборник задач и упражнений по высшей математике: общий курс: [учебное пособие для экономических специальностей вузов] / А.В. Кузнецов, Д.С. Кузнецова, Е.И. Шилкина и др. – Минск: Высшая школа, 1994. – 284 с.: ил. – ISBN 5-339-00954-8:

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ СЕМАНТИЧЕСКОГО АНАЛИЗА И КЛАССИФИКАЦИИ ОБРАЩЕНИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ SERVICEDESK

**Парфёнов Д.И., кан. тех. наук, Кузнецова Л.Ю.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Классификация текстов – это одна из задач компьютерной лингвистики, которая заключается в отнесении документа к одной из нескольких категорий на основании содержания документа. Автоматическая классификация текстов может производиться на основе продукционных моделей с заранее предписанными стратегиями, либо на основе методов машинного обучения. Одним из примеров задач классификации текстов может служить задача классификации обращений пользователей в системе Service Desk.

Большинство компаний в том или ином виде работают с клиентами и занимаются их поддержкой (консультациями). Кроме того, для успешного функционирования предприятия также необходима техническая поддержка внутренних процессов.

В работе [3] выделены отрицательные аспекты неправильной организации работы отдела поддержки пользовательских обращений, а именно

- отсутствие закрепленных областей компетенции, создающих непонимание важности выполняемых функций;
- риск потери заявки пользователя в общей массе заявок и поручений руководства в следствие не регламентированной формы подачи заявки;
- жесткая зависимость работы компании от «ключевого» специалиста, возникающий, когда некоторый тип работ регулярно выполняется одним сотрудником.

Для обеспечения качественного взаимодействия сторон, существуют системы автоматизации класса Service Desk. Главными задачами Service Desk систем являются возможность приёма и обработки заявок, другими словами, клиент задаёт вопрос (заявку, запрос, тикет) и менеджеры обрабатывают его. Благодаря использованию Service Desk системы возможна совместная работа всех менеджеров компании.

Процессы в Service Desk регламентируют все сложности, которые возникают в работе ИТ-отдела [4]. На рисунке 1 представлена схема управления всеми возникающими проблемами, с которыми может сталкиваться команда поддержки.

В связи с описанными функциями и задачами системы ServiceDesk, задача семантического анализа и классификации обращений пользователей в систему ServiceDesk имеет высокую практическую значимость.



Рисунок 1 – Процессы с ServiceDeskсистеме

Анализ текстов на естественных языках предполагает два этапа:

1) предобработку (индексацию), в ходе которой происходит перевод символов сообщения в нижний или верхний регистр, удаляются числа, знаки препинания и стоп-слова (служебные части речи), а также проводится стемминг (или лемматизация).

2) обучение модели на заранее размеченных данных и последующая классификация текстов.

В связи с тем, что автоматическая обработка текстовой информации с каждым годом становится все более актуальной и востребованной, на сегодняшний день существует большое количество исследований по методам обучения моделей.

В работах [1], [2] проводится сравнительный анализ методов классификации текстов. В обеих работах представлена формальная постановка задачи классификации текстов, описаны методы классификации, а также приведен сравнительный анализ методов обучения классификатора с помощью методов машинного обучения, среди которых выделены метод Байеса, k -ближайших соседей, метод наименьших квадратов, метод опорных векторов, а также методы на основе искусственных нейронных сетей. При этом, основными критериями при оценке качества классификации использовались комбинации точности и полноты. На основе исследования [1] был сделан вывод о том, что наилучшее соотношение этих характеристик

достигается при использовании методов опорных векторов и сверточной нейронной сети. При этом, скорость работы метода Байеса одна из самых высоких, однако точность для различных экспериментов сильно варьируется. Согласно исследованию [2], метод наименьших квадратов демонстрировал наилучшие показатели по показателю полноты, при этом метод опорных векторов оказался лучшим по точности классификации. Сравнительный анализ рассмотренных методов классификации на основе исследований [1] и [2] представлен в таблице 1.

Таблица 1 – Анализ эффективности методов классификации текстов

Метод	Средняя точность, p	Средняя полнота, r
Метод опорных векторов	91,3%	84,2%
k -ближайших соседей	79,5%	77,1%
Сверточная нейронная сеть	91,5%	81,3%
Метод Байеса	74,6%	82,5%

Исходя из актуальности задачи, было принято решение о разработке информационной системы для семантического анализа и классификации обращений пользователей в системе Service Desk на основе метода опорных векторов. Общая схема системы представлена на рисунке 2.

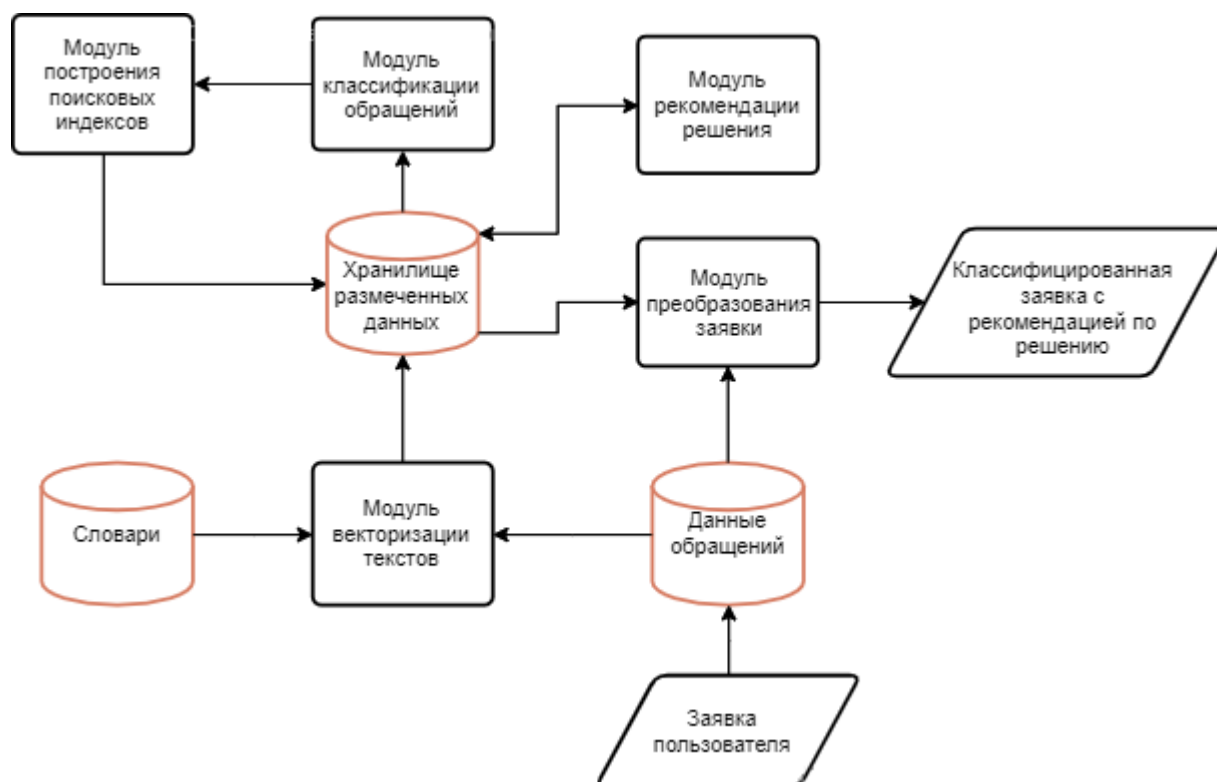


Рисунок 2 – Общая схема системы для семантического анализа и классификации обращений пользователей в системе Service Desk

Пользователь оставляет заявку в системе Service Desk, данные по ней поступают в хранилище, затем происходит векторизация всего обращения с использованием словарей (баз данных) русского языка. Размеченные данные поступают в соответствующее хранилище, откуда их подтягивает модуль классификации обращений. После классификации происходит индексирование текущей заявки с целью уточнения данных заявки в хранилище размеченных данных. Кроме того, после классификации обращения должно быть предложено возможное решение по данной заявке. На выходе система преобразовывает исходную заявку, добавляя к ней присвоенный класс задачи, подразделение-исполнителя и возможное решение по задаче.

Для реализации модуля классификации будут использованы модели на основе метода опорных векторов. Кроме того, для необходимо провести дополнительные исследования для подбора метода создания рекомендаций возможного решения по заявке.

Исследование выполнено при финансовой поддержке РФФИ в рамках научных проектов № 18-37-00400, № 20-07-01065, а так же гранта Президента Российской Федерации для государственной поддержки ведущих научных школ Российской Федерации (НШ-2502.2020.9) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-860.2019.9).

Список литературы

1 Батура Т.В. Методы автоматической классификации текстов /Т.В. Батура // Программные продукты и системы. – 2017. – Т. 30, № 1. – С. 85–99.

2 Епрев А.С. Автоматическая классификация текстовых документов / А.С.Епрев // Математические структуры и моделирование. – 2010. – №21. – С. 65-81

3 Золдак З.С. Выбор и организация системы Service Desk на предприятии / З.С. Золдак // Экономика. Право. Менеджмент: сборник трудов молодых исследователей БГУ. – 2015. №1(3). С. 44-50

4HelpDesk и ServiceDesk. Что это и зачем это нужно вашей компании [Электронный ресурс]. Режим доступа: <https://habr.com/ru/company/deskun/blog/331354/>. – 10.11.2019

ПРОБЛЕМЫ М. ДЕНА В КОМБИНАТОРНОЙ ТЕОРИИ ГРУПП

Пихтилькова О.А., канд. физ.-мат. наук, доцент,
Павленко А.Н., канд. физ.-мат. наук, доцент
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

Основными алгоритмическими проблемами в теории групп, поставленными М. Деном [4] в одной из его работ в 1911 году, являются проблемы равенства и сопряженности в конечно определенных группах и проблема изоморфизма групп.

Исследование этих проблем стимулировало развитие комбинаторных методов в теории групп, что явилось причиной возникновения одного из самых активно развивающихся направлений современной математики — комбинаторной теории групп. В настоящее время имеется целый ряд книг, посвященных данной теме; среди них достаточно назвать монографии Карраса, Магнуса и Солитера [21], а также Линдона и Шуппа [19].

Среди работ, связанных с исследованием проблем М. Дена, наиболее выдающимися являются работы П. С. Новикова [31], доказавшего неразрешимость проблемы равенства слов в конечно определенных группах; им же доказана неразрешимость проблемы изоморфизма групп. Примеры конечно определенных групп с неразрешимой проблемой равенства были даны Буном [2].

С.И.Адяном [9] определено понятие наследственного нетривиального свойства группы и доказано, что не существует алгоритма, позволяющего для произвольной группы с конечным числом образующих и определяющих соотношений распознать выполнимость свойства β , представляющего собой объединение нетривиального наследственного инвариантного свойства, если только существуют группы, обладающие этим свойством β .

Из этого следует, что практически все проблемы, относящиеся к конечно определенным группам, в общем случае неразрешимы.

Отрицательное решение проблемы равенства слов явилось причиной изучения проблем Дена в определенных классах групп.

Для групп с разрешимой проблемой равенства слов возникает более общая проблема - проблема вхождения, впервые рассмотренная Нильсеном в свободных группах и Магнусом в группах с одним определяющим соотношением для так называемых магнусовых подгрупп.

Известно, что проблема вхождения в классе всех конечно определенных групп неразрешима, что непосредственно следует из связи между проблемой вхождения и проблемой равенства слов. Поэтому естественен интерес к изучению рассматриваемой проблемы для каких - то фиксированных классов

групп. Как было отмечено выше, положительное решение проблемы вхождения в свободных группах следует из результата Нильсена.

К. А. Михайловой [28] этот результат был обобщен на свободное произведение групп, доказано, что если в группах A и B разрешима проблема вхождения, то она разрешима в их свободном произведении.

В отличие от свободного произведения, прямое произведение групп, как доказала К. А. Михайлова [29], не наследует свойства сомножителей иметь разрешимой проблему вхождения.

Обобщением проблемы сопряженности слов является проблема обобщенной сопряженности слов, проблема степенной сопряженности и проблема сопряженности подгрупп.

Определение 1. Под обобщенной проблемой сопряженности слов в группе G понимается решение в G системы уравнений $\&_{i=1}^n (z^{-1}w_i z = v_i)$, где $w_i, v_i, i = \overline{1, n}$ — фиксированные элементы группы G .

Существование такого алгоритма для некоторого класса конечно определенных групп позволяет для любого автоморфизма $\varphi \in \text{Aut } G$ определить, является ли он внутренним.

Проблема изоморфизма конечно порожденной коммутативной полугруппы сводится к проблеме обобщенной сопряженности слов в классе $GL_n(\mathbb{Z})$ групп. Поэтому, решение данной проблемы является важной задачей в комбинаторной теории групп.

С описанием множества решений данной системы связана проблема построения централизатора конечно порожденной подгруппы.

Г.С. Маканиным [23] решена известная проблема Артина об описании всех кос в B_{n+1} , коммутирующих с данной косой. Доказано, что централизатор любого элемента в B_{n+1} конечно порожден и указан алгоритм построения его образующих. Используя результат Г. Г. Гурзо [19], обобщившей теорему Г. С. Маканина [23], Т. А. Маканина [24] получила полное решение обобщенной проблемы сопряженности слов в B_{n+1} .

Результаты Г.С. Маканина, Г. Г. Гурзо и Т. А. Маканиной справедливы для групп Артина конечного типа, определенных Брискорном Э. и Сайто К. в статье [18], а именно, в [32] показано, что централизатор конечно порожденной подгруппы конечно порожден и существует алгоритм, выписывающий образующие централизатора; разрешима проблема обобщенной сопряженности слов; дано полное описание решений системы уравнений $\&_{i=1}^n (z^{-1}w_i z = v_i)$.

И. Г. Лысенко [21], доказал разрешимость обобщенной проблемы сопряженности для гиперболических групп, им же установлено, что централизатор элемента в гиперболической группе является конечно порожденным.

В. Н. Безверхний доказал разрешимость проблемы обобщенной сопряженности в группах $C(p) \& T(q)$, где $(p, q) \in \{(6, 3), (4, 4), (3, 6)\}$ и в группах Артина большого типа [10, 14, 15]. Также, для данных классов групп была доказана конечная порожденность централизатора конечной порожденной подгруппы.

Герстеном и Шортом [4] доказана конечная порожденность централизатора элементов для биавтоматных групп.

Помимо указанных выше проблем, мы будем рассматривать проблему А.И. Мальцева [26] о нахождении образующих пересечения конечно порожденных подалгебр данной алгебры, решившего данную проблему для конечно порожденных нильпотентных групп [25]. С данной проблемой тесно связано свойство $\mathcal{H}$ (Хаусона) подалгебр данной алгебры, а именно, алгебра обладает свойством $\mathcal{H}$, если пересечение конечно порожденных подалгебр есть конечно порожденная подалгебра. Известно [5], что свободные группы обладают свойством $\mathcal{H}$. Б. Баумслаг [1] обобщил результат Хаусона на свободное произведение групп.

Для свободных групп проблема А. И. Мальцева о пересечении подгрупп решена В. Н. Безверхним [11]. Конструктивное доказательство теоремы Б. Баумслага, данное в статье [16], позволило ее авторам решить указанную проблему А. И. Мальцева для свободного произведения групп. Там же доказано, что теорема Баумслага на свободное произведение с объединением не переносится. Показано, что свободное произведение групп, обладающих свойством Хаусона, объединенных по конечным группам, обладает свойством Хаусона. Также в данной работе показано, что если сомножители обладают свойством Хаусона и в них разрешима проблема Мальцева и разрешима проблема пересечения смежных классов конечно порожденных подгрупп, то и свободное произведение этих групп, объединенных по конечным подгруппам, наследует указанное выше свойство.

Д. И. Молдаванским в [29] доказывалось, что группы с одним определяющим соотношением с нетривиальным центром свойством Хаусона не обладают.

И. Капович показал [6], что в группе $G = \langle a, t; at^{-1}ata^2t^{-2}a^{-1}t^2 \rangle$ свойство Хаусона также не выполнено.

Работа посвящена решению некоторых алгоритмических проблем в классе групп, являющемся свободным произведением двух свободных групп с коммутирующими подгруппами: $G = \langle A * B; [H, K] = 1 \rangle, H \text{ и } K$ — конечно порожденные подгруппы в A и B соответственно, а именно, описанию централизатора элементов, построению пересечения централизаторов и решению обобщенной проблемы сопряженности. Для групп этого класса Д. Гурвицем [8] доказана разрешимость проблем равенства и сопряженности слов. В работе Р.Е. Шуппа и С.Ф. Миллера [7] исследуется геометрия этих групп и показано, что условия при которых проблема слов разрешима

идентичны для свободного произведения с объединением. Если A и B имеют разрешимую проблему равенства и в подгруппах H и K разрешима обобщенная проблема равенства, то в группе G разрешима проблема равенства.

Теорема 1. Центризатор любого элемента группы G конечно порожден и есть либо циклическая, либо свободная абелева ранга 2, либо подгруппа вида

$$\begin{aligned} C_G(g) &= \langle s, \prod_{i=1}^n * a_i K a_i^{-1} \rangle, a_i^{-1} g a_i \in H, g = s^k, g \notin H, \\ C_G(g) &= \langle s, K * \prod_{i=1}^n * a_i K a_i^{-1} \rangle, a_i^{-1} g a_i \in H, g = s^k, g \in H, \\ C_G(g) &= \langle s, \prod_{i=1}^n * b_i H b_i^{-1} \rangle, b_i^{-1} g b_i \in K, g = s^k, g \notin K, \\ C_G(g) &= \langle s, H * \prod_{i=1}^n * b_i H b_i^{-1} \rangle, b_i^{-1} g b_i \in K, g = s^k, g \in K \end{aligned}$$

Причем $a_i(b_i)$ выбирается как минимальный представитель двойного смежного класса $\langle g \rangle a_i' H (\langle g \rangle b_i' K)$.

Все результаты получены с помощью плоских односвязных диаграмм Ван-Кампена.

Далее решается вопрос описания пересечения конечного числа центризаторов элементов группы G . В рассматриваемом классе групп пересечение конечно порожденных подгрупп в общем случае не является конечно порожденной подгруппой. Это следует из результата Д. И. Молдаванского (1968 г.): группа, содержащая прямое произведение бесконечной циклической подгруппы и свободной ранга 2, не обладает свойством Хаусона [29]. Однако, как доказано автором, для центризаторов подгрупп это свойство справедливо.

Теорема 2. Пересечение конечного числа центризаторов элементов группы G есть конечно порожденная подгруппа одного из типов, описанных в теореме 1.

Теорема 3. Существует алгоритм, выписывающий образующие пересечения конечного числа центризаторов элементов группы G .

Из доказанных теорем получается ряд следствий.

Следствие 1. Центризатор конечно порожденной подгруппы конечно порожден.

Следствие 2. Существует алгоритм, выписывающий образующие центризаторов подгрупп группы G .

Следствие 3. Пересечение центризаторов конечно порожденных подгрупп есть конечно порожденная подгруппа и существует алгоритм, выписывающий образующие этого пересечения.

Далее доказывается разрешимость проблемы обобщенной сопряженности при условии, что подгруппы H и K антинормальны.

Определение 2. Подгруппа P группы G называется антинормальной, если из того, что $g \notin P$ следует, что $g^{-1}Pg \cap P = \{1\}$.

Теорема 4. Существует алгоритм, позволяющий установить, пусто или нет пересечение следующих смежных классов подгрупп: $\bigcap_{i=1}^n g_i C_G(w_i)$, где $C_G(w_i)$ - централизатор элемента $w_i \in G$.

Теорема 5. В группе G разрешима проблема обобщенной сопряженности слов.

Теорема 6. Пусть $G = \langle A * B; [H, K] = 1 \rangle$ конечно определенная группа и $\{w_i\}_{i=1, \overline{n}}, \{v_i\}_{i=1, \overline{n}}$ - слова из G . Если F -какое-то решение системы $\&_{i=1}^n (z^{-1}w_i z = v_i)$, то множество $C_G(H) \cdot F$, где $C_G(H)$ — централизатор подгруппы H , порожденный множеством $\{w_i\}_{i=1, \overline{n}}$ является множеством всех решений системы.

Список литературы

1. Baumslag B. Intersection of finitely generated subgroups in free product. J. London Math. soc., 1966, 41. P. 673-679.
2. Boone W. W. Certain simple, unsolvable problems of group theory.// V, VI. Proc. Kon. ned. akad. wetensch., 1957, 19, №1, 22-27; №2, p. 227-232 (РЖМат, 1959, 78).
3. Dehn M. Über unendliche discontinuierliche Gruppen. Maht. Annal. 71, 116-144, 1.4, II.3, 1911.
4. Gersten S. M., Short H. B. Rational subgroups of biautomatic groups Annals of Math. 1991, 134, P. 125-158.
5. Howson A.G. On the intersection of finitely generated free groups. J. London Math. soc., 1954, 29. P. 428-434.
6. Kapovich I. Howson property and one- relator groups// Commynication in algebra. 1999. V. 27. № 3. P. 1057-1072.
7. Miller, C.F. III, Schupp, P.E. The geometry of Higman-Neumann-Neumann extensions// Comm. Pure. Appl. Math. 26, 787-802(1973).
8. R. Daniel Hurwitz. On the Conjugacy Problem in a Free product with Commuting Subgroup// Math. Ann. 221, 1-8, 1976.
9. Адян С.И. Неразрешимость алгоритмических проблем в теории групп// Труды Мое. Мат. об-ва. 1957. Т.6. С. 231-298.
10. Безверхний В. Н. О нормализаторах $C(p) \& T(q)$ -группах// Алгоритмические проблемы теории групп и полугрупп. Межвуз. сб. научн. тр. - Тула, 1994.
11. Безверхний В. Н. О пересечении конечно порожденных подгрупп свободной группы // Сб. науч. тр. каф. высш. матем.- Тула: Изд-во ТулПИ, 1974. С. 51-56.

12. Безверхний В. Н. Решение проблемы вхождения в группах с одним определяющим соотношением с нетривиальным центром// Сиб. матем. журнал. 1985. № 2. Т. 26 13.
13. Безверхний В. Н. Решение проблемы вхождения для одного класса групп// Вопросы теории групп и полугрупп - Тула: Изд-во ТГПИ им. Л.Н. Толстого, 1972. С. 3-86.
14. Безверхний В. Н. Решение проблемы обобщенной сопряженности слов $C(p) \& T(c)$ -группах// Известия Тульского гос. ун-та. Сер. "Математика". - Тула: Изд-во ТулГУ, 1998.
15. Безверхний В. Н. Решение проблемы обобщенной сопряженности слов в группах Артина большого типа// Фундаментальная и прикладная математика. Т.5. №1. 1999.
16. Безверхний В. Н., Роллов Э. В. О подгруппах свободного произведения групп// Современная алгебра, вып.1.-Л., 1974. С.
17. Безверхний В.Н. О неразрешимости проблемы вхождения для некоторого класса групп// Сб. науч. тр. каф. высш. матем.- Тула: Изд-во ТулПИ, 1974. С. 51-54.
18. Брискорн Э., Сайто . Группы Артина и Кокстера // Математ. заметки: сб. переводов, 1974. 18, № 6. С. 56-79.
19. Гурзо Г.Г. О централизаторах конечных множеств элементов группы кос// Математ. заметки. 1985.Т. 37.№1. С.3-6.
20. Линдон Р., Шупп П. Комбинаторная теория групп.-М.: Мир, 1980.
21. Лысенко И. Г. О некоторых алгоритмических свойствах гиперболических групп// Изв. АН СССР. Сер. мат. 1959. Т.53.№4.
22. Магнус В., Каррас А., Солитер Д. Комбинаторная теория групп.-М.: Наука, 1974.
23. Маканин Г.С. О нормализаторах группы кос// Мат. сб. 1971. 86. № 2. С. 171-179.
24. Маканин Т. А. Об одной системе решений в группе кос// Изв. учеб. заведений: Математика. 1986.№9. С.58-62.
25. Мальцев А. И. Два замечания о нильпотентных группах// Мат.сб. 1955. 37.№3.С. 567-572.
26. Мальцев А. И. О гомоморфизмах на конечные группы // Уч. зап. Ивановского пед. ин-та .1958.С.49-60.
27. Михайлова К. А. Проблема вхождения для прямых произведений групп// Мат. сб. 1966. 70.№2. С. 241 -251.
28. Михайлова К. А. Проблема вхождения для свободного произведения групп//Мат. сб. 1968. 75.№2. С. 199-210.
29. Молдованский Д. И. О пересечении конечно порожденных подгрупп// Сиб. матем. журнал. 1968. № 9. С. 1422-1426.

ОПЫТ МЕТОДИЧЕСКОЙ РАБОТЫ В ИЗЛОЖЕНИИ ТЕМЫ «ПОНЯТИЕ ПРОИЗВОДНОЙ ФУНКЦИИ»

Рассоха Е.Н., канд.пед.наук, доцент, Анциферова Л.М., канд.пед.наук
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

В своих публикациях неоднократно поднимали вопрос о падении от года к году качества математического образования абитуриентов, поступающих в вуз. В настоящее время можно констатировать тот факт, что абитуриенты, поступающие в массовые вузы областных центров страны, например, на технические направления подготовки, имеют в среднем 50-56 тестовых баллов по математике. Это говорит о том, что такой выпускник школы умеет решать первые десять элементарных задач ЕГЭ по математике, отражающие лишь незначительную часть всей программы школьного курса математики. Поэтому исправлять ситуацию приходится преподавателю высшей школы, работая над этой проблемой в различных направлениях – это и работа в области развития и формирования математических способностей студентов, и, в общем и целом, развития и формирования их математической культуры.

Иногда, работая с аудиторией студентов, понимаешь, что необходимо простое упрощение изложения некоторых ключевых тем и понятий. К таким ключевым понятиям дисциплины «Математика» для студентов технических направлений подготовки относится, например, понятие производной функции. Несмотря на то, что данная тема изучается в школьном курсе «Алгебры и начала математического анализа» и в ЕГЭ на нее отведено целых две задачи, бывшие школьники не понимают самого понятия «производной функции».

В связи с этим, вот уже несколько лет подряд, излагаем данную тему, используя методику А.П. Киселева (выдающийся учитель, автор выдающихся учебников по математике, по которым училось не одно поколение советских школьников, имеющих высочайший уровень математических знаний). Можем утвердительно сказать, что данный опыт имеет положительный результат.

Изучение понятия производной функции начинаем также как и А.П. Киселев с введения понятий «Подъем прямой и подъем кривой» следующим образом.

Подъем прямой. Подъемом какой-нибудь прямой CD по отношению к горизонтальной прямой AB называется иногда угол α , образуемый этими прямыми.

Например, говорят: «дорога идет в гору с подъемом в 5° ». Но, чаще, подъем выражается не самим углом α , а его тангенсом. Для нахождения величины тангенса вообразим, что на прямой CD мы взяли произвольную точку M и из нее провели $MN \perp AB$ (см рис 1). Тогда из треугольника $\triangle MEN$ находим: $tg \alpha = \frac{MN}{EN}$.

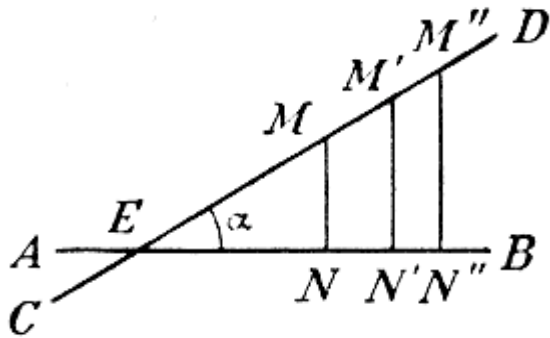


Рисунок 1

Точку M можно брать на прямой CD произвольно, так как если возьмем другие точки $M', M'', \dots$, то, проведя перпендикуляры $M'N', M''N''$, мы получим подобные треугольники, из которых видно, что

$$\frac{MN}{EN} = \frac{M'N'}{E'N'} = \frac{M''N''}{E''N''} = \dots$$

Если, например, $MN = \frac{1}{100} EN$, то и $M'N' = \frac{1}{100} E'N'$, $M''N'' = \frac{1}{100} E''N''$ и

т. д.; тогда можно сказать, что подъем прямой CD равен $\frac{1}{100}$ (или равен 1 метру на протяжении 100 метров по горизонтальному направлению).

На рисунке 2 изображена прямая CD , тоже наклонная к горизонтальной прямой AB , но идущая (слева направо) не в гору, а вниз. Тогда речь может идти не о подъеме прямой CD , а об ее уклоне.

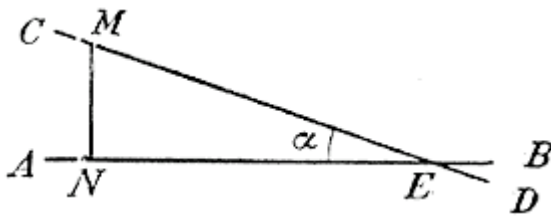


Рисунок 2

Уклон этот тоже измеряется чаще всего тангенсом угла α , образованного CD с AB , так что, можем записать: $\text{уклон} = \frac{MN}{EN}$.

Можно условиться рассматривать уклон как отрицательный подъем, то есть, если $MN = \frac{1}{2} EN$, то можно сказать, что уклон прямой CD равен $\frac{1}{2}$.

Очевидно, что когда прямая CD не наклонна к AB , а параллельна ей или сливается с ней, тогда подъем равен нулю.

Положим теперь, что горизонтальная прямая – это будет ось OX (см. рисунок 3). Тогда подъем прямой CD есть тангенс угла α , образованного этой прямой с положительным направлением оси OX . Этот подъем, на самом деле, можно найти и не продолжая прямую CD до пересечения с осью OX .

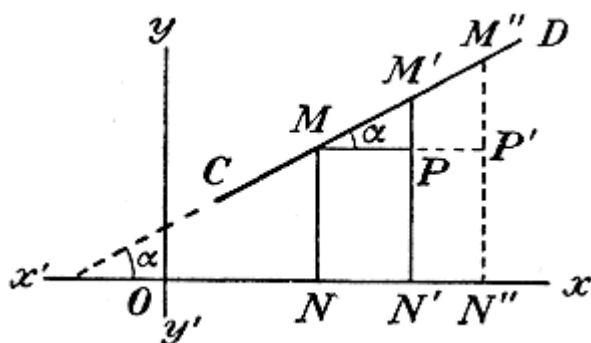


Рисунок 3

Для этого возьмем две какие-нибудь точки на прямой CD , например M и M' , проведем их ординаты MN и $M'N'$ и прямую $MP \parallel OX$. Тогда получим прямоугольный треугольник $\triangle MPM'$, у которого угол $\angle M$ равен α . Следовательно, подъем прямой CD равен отношению $M'P$ к MP . Отрезок MP , равный NN' , показывает, насколько увеличилась абсцисса ON при переходе от точки M к точке M' ; отрезок $M'P$ показывает, насколько при этом переходе увеличилась ордината MN .

Тогда говорят что, отрезок MP , равный NN' , есть *приращение абсциссы* (обозначают - Δx), полученное ею при переходе от точки M к точке M' , а $M'P$ — это *приращение ординаты* (обозначают - Δy), соответствующее приращению абсциссы на NN' . Конечно, если абсциссе ON дадим иное приращение, напр. NN'' , то и ордината MN получит иное приращение $M''P'$, но тангенс угла α по-прежнему есть отношение $M''P'$ к NN'' .

Таким образом:

$$\text{подъем прямой} = \frac{\text{приращение ординаты}}{\text{приращение абсциссы}},$$

в предположении, что эти два приращения соответствуют друг другу.

Если прямая CD образует отрицательный подъем (см. рисунок 4), то при положительном приращении абсциссы ON на отрезок NN' приращение ординаты будет отрицательное, а именно — $QM' = MP$. Тогда отношение отрицательного приращения ординаты к положительному приращению абсциссы будет число отрицательное, что и должно быть, так как уклон есть отрицательный подъем.

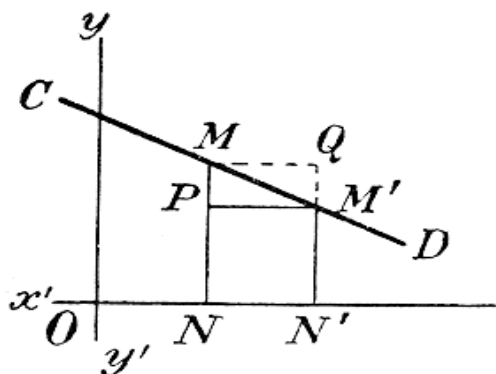


Рисунок 4

Положим, для примера, что прямая CD есть график такой линейной функции:

$$y = -\frac{1}{3}x + 2.$$

Дадим абсциссе x произвольное значение, например, $x = 4$. В этом случае функция будет равна:

$$y = -\frac{1}{3} \cdot 4 + 2 = -\frac{4}{3} + 2 = \frac{2}{3}.$$

Пусть теперь абсцисса x получит какое-нибудь приращение, например, 1. Таким образом, $\Delta x = 1$, а точка $x + \Delta x = 5$ Тогда ордината y будет равна:

$$y = -\frac{1}{3} \cdot 5 + 2 = -\frac{5}{3} + 2 = \frac{1}{3}.$$

и, следовательно, приращение y окажется равным: $\frac{1}{3} - \frac{2}{3} = -\frac{1}{3}$.

$$\text{Поэтому } \text{подъем} = \frac{-\frac{1}{3}}{1} = -\frac{1}{3}.$$

Так оно и должно быть, потому что из уравнения прямой:

$$y = -\frac{1}{3}x + 2$$

видно, что угловой коэффициент равен $-\frac{1}{3}$, а коэффициент этот, будучи

равен тангенсу угла, образованного прямою с положительным направлением оси Ox , выражает подъем прямой (в данном случае уклон).

Далее подводим к понятию касательной кривой в заданной точке.

Общее определение касательной к кривой.

Возьмем на кривой какие-нибудь две точки A и B и проведем через них секущую AP . Вообразим, что точка B , двигаясь по кривой, проходит через положения $B_1, B_2, \dots$ и приближается к точке A . Тогда секущая AP будет занимать последовательно положения $AP_1, AP_2, \dots$ (см. рисунок 5)

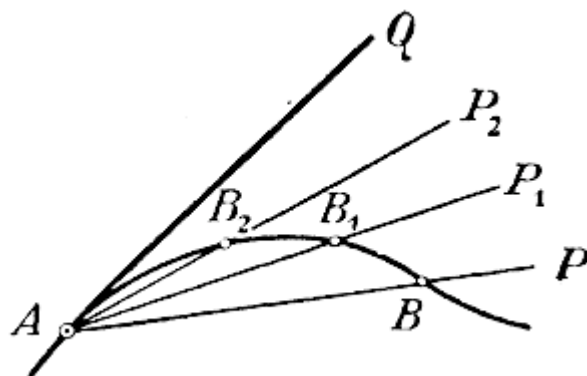


Рисунок 5

Если допустим, что точка B приближается к A неограниченно близко, то секущая приближается все более и более к некоторому предельному положению AQ так, что угол между прямою AQ и секущей делается и остается меньшим любого данного угла, как бы мал он ни был. Это предельное положение секущей называется касательной к кривой в точке A .

Затем уже дается определение касательной к кривой в точке A как прямой, угловой коэффициент которой равен пределу углового коэффициента секущей, при условии, что $\Delta x \rightarrow 0$.

Вводим понятие подъема кривой.

Подъем кривой. Возьмем на кривой, изображенной на рисунке 6, две какие-нибудь точки M и M' , и проведем через них секущую MP . Подъем этой секущей показывает средний подъем кривой на участке от M до M' . Вообразим, что точка M' неограниченно приближается к M . Тогда секущая будет все ближе и ближе подходить к касательной MQ , проведенной к кривой в точке M , и средний подъем кривой, все ближе и ближе будет подходить к равенству с подъемом касательной.

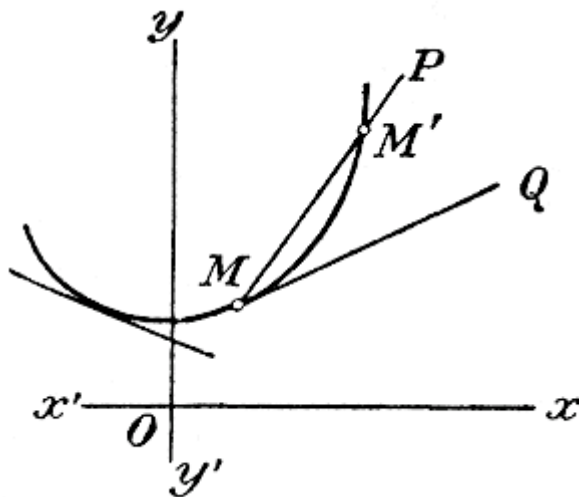


Рисунок 6

Условимся принимать подъем касательной, проведенной к кривой, за подъем самой кривой в точке касания.

Далее можно привести в качестве примера подъем параболы $y = x^2$.

Вычислим подъем в точке M , у которой абсцисса равна 1. Тогда ее ордината будет $MN = ON^2 = 1^2 = 1$. Чтобы найти подъем кривой в точке M , предварительно вычислим средний подъем на участке от точки M до какой-нибудь другой точки M' , у которой абсцисса $ON' = ON + NN'$ и ордината $M'N' = M'P + PN' = -M'P + MN$. Чтобы перейти от M к M' , надо абсциссе ON , дать приращение $\Delta x = NN'$, тогда ордината получит соответствующее приращение $\Delta y = M'P$.

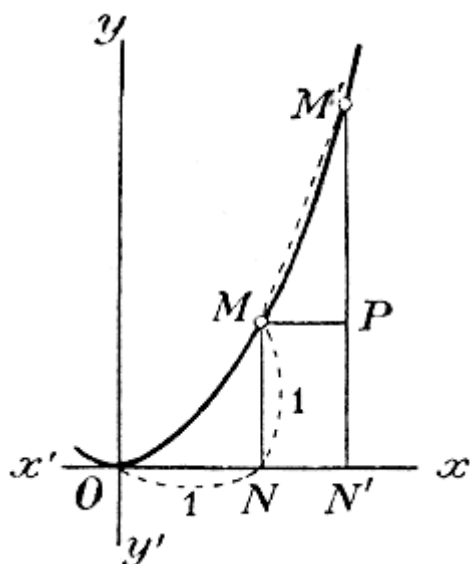


Рисунок 7

$$\text{подъем секущей} = \frac{MP}{NN'} = \frac{MP}{NN'}.$$

Возьмем конкретные значения для приращения абсциссы.

Пусть $NN' = 0,9$. Тогда $ON' = 1 + 0,9 = 1,9$ и $M'N' = 1,9^2 = 3,61$.

Значит, $MP = 3,61 - 1 = 2,61$ и подъем секущей $= \frac{2,61}{0,9} = 2,9$.

Станем теперь уменьшать приращение NN' , приближая, его к нулю: тогда точка M' будет приближаться все ближе и ближе к точке M , и средний подъем, кривой будет приближаться к равенству с подъемом кривой в точке M (с подъемом касательной в точке M). Будем, например, NN' задавать последовательно уменьшающиеся числа:

0,9; 0,8; 0,7; 0,6; 0,5; ...; 0,1.

Выпишем все числа, которые при этом получаются, в такой таблице:

Таблица 1

NN'	0,9	0,8	0,7	0,6	0,5	0,4	0,3	0,2	0,1
ON'	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1
$M'N' = (ON')^2$	3,61	3,24	2,89	2,56	2,25	1,96	1,69	1,44	1,21
$MP = M'N' - MN$	2,61	2,24	1,89	1,56	1,25	0,96	0,69	0,44	0,21
Подъем $\frac{MP}{NN'}$	2,9	2,8	2,7	2,6	2,5	2,4	2,3	2,2	2,1

Из этой таблицы видно, что по мере приближения точки M' к M подъем секущей все уменьшается, приближаясь все более и более к числу 2, так что весьма вероятно, что подъем секущей (средний подъем кривой) стремится к пределу 2, когда приращение $NN' \rightarrow 0$. Если это так, то подъем параболы в точке M , имеющей абсциссу 1 и ординату 1, равен 2.

Затем вводим понятие производной функции, как выражающей подъем кривой.

Определение. Функция, выражающая подъем кривой в какой-нибудь ее точке, в зависимости от абсциссы этой точки, называется производной функцией от той функции, которая выражает эту кривую.

Так, для параболы $y = x^2$, было установлено, что подъем кривой в точке с абсциссой x равен $2x$; эта функция $2x$ называется производной (функцией) от функции x^2 .

Уже после этого строго вводим понятие производной функции, согласно программе вуза. Но, делая такие небольшие отступления от вузовской программы, добиваемся понимания студентами основных понятий дисциплины, что положительно влияет на качество их математических знаний

Список литературы

1. Рассоха Е.Н. Развитие математической культуры студентов технических специальностей: дис....канд. пед. наук: 13.00.08 / Е.Н. Рассоха.— Оренбург, 2005.— 157 с.

2. Рассоха, Е.Н. Психолого-педагогические основы понятия «математическая культура студентов» / Е. Н. Рассоха // Современные образовательные технологии: психология и педагогика: Монография. Кн. 8. — Новосибирск: ЦРНС, 2009. — 251 с. — С. 159-173.

3. Анциферова, Л.М. Преемственность как фактор развития математических способностей старшеклассников в системе «школа-вуз»: дис. канд. пед. наук: 13.00.01 / Л.М. Анциферова. - Оренбург, 2014.— 224 с.

4. Киселев, А.П. Алгебра / А.П. Киселев. — Ч. 1. — М.: Физматлит, 2006. — 152 с.

ПРИМЕНЕНИЕ ИМИТАЦИОННОЙ СРЕДЫ PACKETTRACER ДЛЯ ИССЛЕДОВАНИЯ БАЗОВЫХ СРЕДСТВ ЗАЩИТЫ СЕТЕВЫХ УСТРОЙСТВ

Рычкова А.А., канд. пед. наук, Пантич Д.Р.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

В настоящее время вопрос защиты сетевых устройств является одним из самых актуальных в связи с популярностью обмена информации посредством сетевого взаимодействия. Согласно исследованию PositiveResearch[1], доля компаний, где был получен доступ к локальной вычислительной сети (далее - ЛВС) в рамках тестирования составляет 92%. Данные свидетельствуют о низком уровне защищенности ЛВС. В большинстве организаций не выполняются базовые требования безопасности по защите сетевых устройств.

В статье рассмотрены базовые средства защиты сетевых устройств семейства Cisco в имитационной среде PacketTracer от CiscoSystemsInc [2]. Полученные результаты могут использоваться при проведении лабораторного практикума на профессиональных дисциплинах при подготовки будущих бакалавров по направлению 10.03.01 Информационная безопасность. Применение имитационной среды позволит сформировать необходимые знания и умения студентов в области защиты сетевых устройств, сформировать профессиональные компетенции.

Для исследования базовых средств защиты в лабораторной работе предлагается составить топологию, представленную на рисунке 1.

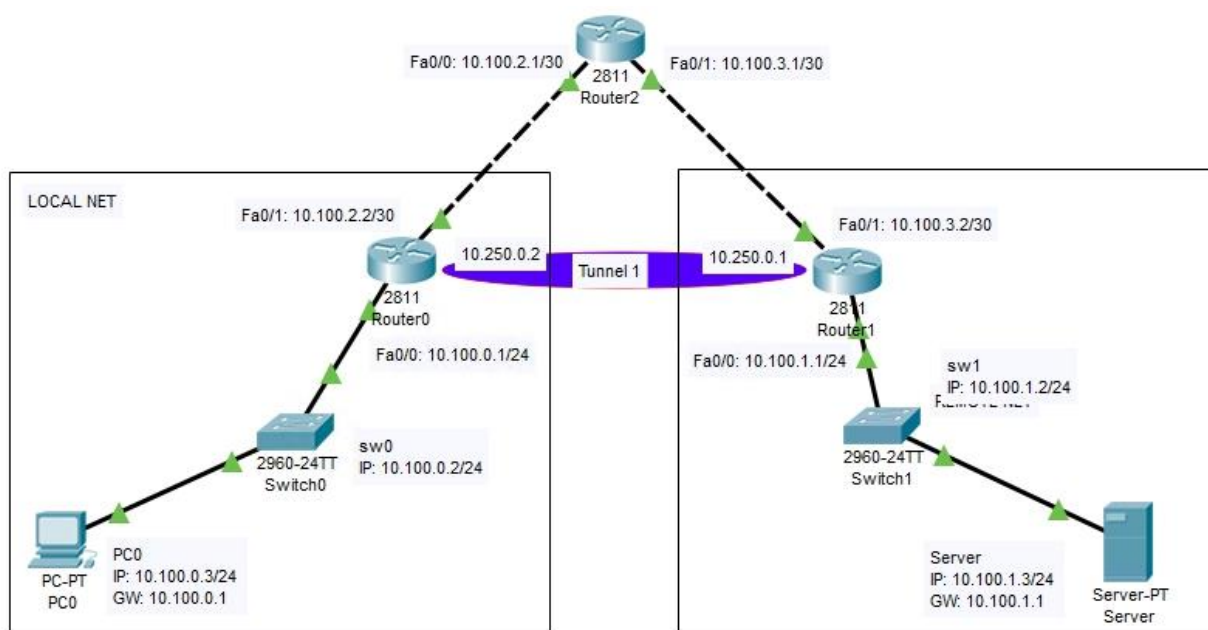


Рисунок - 1 Топология сети

Доступ на каждое сетевое устройство должен быть ограничен парольной защитой. Пароль необходимо устанавливать как при локальном подключении, так и при удалённом. Пример настройки пароля на маршрутизатор представлен на рисунке 2.

```
R0(config)#line con 0
R0(config-line)#password testencrypt
R0(config-line)#login
R0(config-line)#exit
R0(config)#exit
R0#
```

Рисунок 2 - Настройка парольной защиты на маршрутизаторе

Сетевые устройства Cisco хранят пароли в своём конфигурационном файле в открытом виде, что является серьёзной угрозой информационной безопасности (рисунок 3).

```
R0#show run | begin con 0
line con 0
  password testencrypt
!
line aux 0
!
line vty 0 4
  login
!
!
```



Рисунок 3 - Фрагмент конфигурационного файла

Одной из рекомендаций является использование стандартной службы шифрования паролей (рисунок 4).

```
R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#serv
R0(config)#service pass
R0(config)#service password-encryption
```

Рисунок 4 - Шифрование паролей

После этого пароль будет храниться в конфигурационном файле в зашифрованном виде (рисунок 5).

```
show run | begin con 0
line con 0
  password 7 0835495D1D1C0B1400121C10
!
line aux 0
!
```

Рисунок 5 - Фрагмент конфигурационного файла с зашифрованным паролем

Служба шифрования паролей использует стандартный шифр Вижинера, в связи с чем криптостойкость зашифрованного пароля является очень низкой,

существуют ресурсы[3] для дешифровки пароля из конфигурационного файла устройств на базе операционной системы CiscoIOS (рисунок 6).



Рисунок - 6Результат работы сервиса дешифрации паролей

В связи с отсутствием надежного шифрования паролей необходимо обеспечить ограничение доступа ко всем конфигурационным файлам сетевых устройств, включая резервные копии.

В настоящее время удалённый доступ на сетевые устройства является необходимостью в связи с частой потребностью принятия оперативных решений при возникновении различных проблем эксплуатации ЛВС. Сетевые устройства в основном используют следующие протоколы для удалённого доступа:

- SSH (Secure Shell) - сетевой протокол прикладного уровня, позволяющий проводить удаленное управление операционной системой и тунелирование TCP-соединений. Протокол шифрует сетевой трафик.

- Telnet (TErminaL NETwork) - протокол прикладного уровня, используемый для реализации двунаправленного интерактивного текстового интерфейса в сети через виртуальный терминал.

- HTTP (HyperText Transfer Protocol) — протокол передачи гипертекста. Данные передаются в открытом виде.

- HTTPS (S - Secure) - данные передаются в зашифрованном виде.

Кроме этого, есть проприетарные протоколы различных вендоров. В рамках данного исследования будет производиться сравнение Telnet и SSH.

Настройка Telnet на сетевом устройстве представлена на рисунке 7.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret admin
R1(config)#line vty 0 15
R1(config-line)#password remoteaccess
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
```

Рисунок 7 - Конфигурационный файл настройки Telnet

В протоколе Telnet не предусмотрено использование ни шифрования, ни проверки подлинности данных. Так что следует иметь в виду, что сессия Telnet практически не защищена, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне.

Протокол SSH является более защищённым протоколом, чем Telnet, пример его настройки представлен на рисунке 8

```
R0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R0(config)#ip domain-name local.net
R0(config)#username cisco password sshconnect
R0(config)#crypto key generate rsa
The name for the keys will be: R0.local.net
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R0(config)#ip ssh version 2
*map 1 0:0:54.224: %SSH-5-ENABLED: SSH 1.99 has been enabled
R0(config)#enable secret admin
R0(config)#line vty 0 15
R0(config-line)#transport input ssh
R0(config-line)#login local
R0(config-line)#exit
R0(config)#exit
R0#
```

Рисунок 8 - Пример настройки конфигурационного файла SSH

Для аутентификации в SSH используется протокол на основе алгоритмов электронной подписи RSA или DSA. Обмен информацией между устройствами происходит в зашифрованном виде. Для создания общего сеансового ключа используется алгоритм Диффи – Хеллмана. Для шифрования передаваемых данных используются симметричное шифрование: AES, Blowfish или 3DES. Целостность проверяется с помощью HMAC-SHA1 или HMAC-MD5.

В случае если необходимо обмениваться конфиденциальной информацией за пределами ЛВС, необходима создание зашифрованного канала связи между организациями. Дело в том, что использование протоколов туннелирования, таких как GRE, создает лишь логическую взаимосвязь между организациями, но сами данные будут по-прежнему проходить через устройства сетевого провайдера с угрозой перехвата со стороны третьих лиц. Одним из наиболее распространенных способов шифрования сетевого трафика в GRE-туннелях является использование защищенного протокола сетевого уровня модели OSI - IPSec.

IPSec позволяет шифровать трафик, а также проверять целостность и подлинность сетевых пакетов. IPSec может использовать следующие алгоритмы шифрования:

- AES (Advanced Encryption Standard);
- DES (Data Encryption Standard);
- 3DES (Triple DES).

Работа IPSec делится на несколько этапов. Первым является IKE-протокол, использующийся для обмена ключами между устройствами. Первый сессионный ключ IKE хранится в конфигурации, либо на стороне сертификационного сервера. После выполнения процесса аутентификации начинается процесс шифрования трафика. IPSec со временем меняет сессионный ключ из соображений безопасности.

Применение имитационной среды PacketTracer от CiscoSystemsInc в учебном процессе позволит студентам закрепить теоретические знания в области информационной безопасности ЛВС, сформировать умения настраивать конфигурационные файлы сетевого оборудования, наглядно представить работу современных защищенных сетевых протоколов.

Список литературы

1. Positive Research 2019 [Электронный ресурс]/ Сборник исследований по практической безопасности// АО «Позитив Текнолоджиз». - Москва. - 296 с. - URL <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf> (дата обращения: 25.12.2019).
2. CiscoPacketTracer : [оф. сайт]. - Электрон. дан. Cisco. - Режим доступа: https://www.cisco.com/c/ru_ua/training-events/netacad/training-courses/cisco-packet-tracer.html(дата обращения: 25.12.2019)
3. DecryptCiscoType 7 password. - Электрон. дан. iBeast Business Solutions - Режимдоступа<http://ibeast.com/tools/CiscoPassword/index.asp>

О МЕТОДАХ ПРОВЕРКИ ЧИСЛА НА ПРОСТОТУ

Сикорская Г.А., д-р пед. наук, доцент, Галушкин Д.А., Данильчук М.В.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»

До недавнего времени считалось, что у простых чисел нет применения за пределами теоретической математики, однако, во второй половине прошлого века, они нашли свое применение в криптографических схемах с открытым ключом, таких как RSA. Подобные схемы основаны на колоссальной разнице в сложности выполнения двух задач: проверки числа на простоту и факторизации числа, представляющего собой произведение двух больших простых.

Самым наивным и очевидным методом проверки числа N на простоту является метод перебора делителей, основанный на переборе всех натуральных чисел k от 2 до $N - 1$. При этом, если N делится без остатка на k , то N – составное. Если же не нашлось ни одного такого k , то N – простое.

Существует довольно простая оптимизация этого метода, которая заключается в ограничении k не до $N - 1$, а до $\sqrt{N}$. Если $N = ab$, то меньшее из чисел a и b не больше $\sqrt{N}$. И из делимости N на a однозначно следует его делимость и на b . При этом, очевидно, проверка делимости на большее из чисел a и b уже не нужна. Первым математиком, указавшим на это, был Леонардо Фибоначчи[9].

Запишем алгоритм метода перебора делителей на псевдокоде:

```
Вход: натуральное число  $n$ , которое надо проверить на простоту
Выход: простое, означает, что число  $n$  является простым числом
        составное, означает, что число  $n$  является составным числом

если  $n \bmod 2 = 0$ , то вернуть составное
для  $k := 3, 5, 7, 9, \dots$  пока  $k^2 \leq n$ :
    если  $n \bmod k = 0$ , то вернуть составное
вернуть простое
```

Перебор делителей до корня в практических задачах почти не применяется из-за высокой вычислительной сложности. Однако, если проверяемые числа достаточно малы, то алгоритм удобен своей простой реализацией.

Рассмотрим один из тестов простоты натурального числа n , основанный на малой теореме Ферма - тест Ферма, открытый Пьером Ферма в 1640 году. Тест Ферма основан на лемме: Для любого простого числа p и целого числа k ,

не кратного p , произведения k и чисел $1, 2, 3, \dots, p - 1$ при делении по модулю на p в остатке дают числа $1, 2, 3, \dots, p - 1$ с точностью до перестановки (т.е. в другом порядке) [1].

Данную теорему можно применить к тестированию чисел на простоту: если $a^{p-1} - 1$ не делится на p , то p – составное число. Однако, если a и p взаимно простые числа и $a^{p-1} - 1$ делится на p , то p может быть как простым, так и составным. Т.е. выполнение сравнения $a^{p-1} \equiv 1 \pmod{p}$ является необходимым, но не достаточным признаком простоты числа. Если число p – составное, то оно называется псевдопростым Ферма по основанию a , например, 341 – псевдопростое по основанию 2 [4].

При проверке выбирают несколько чисел a , таким образом, повышая вероятность того, что p – простое число.

Тест Ферма самый ненадежный из вероятностных тестов, но он используется для нахождения составных чисел, так как однозначно определяет их.

Запишем алгоритм теста Ферма на псевдокоде:

Вход: натуральное число n , которое надо проверить на простоту, натуральное число p , которое задает параметр безопасности
Выход: простое с вероятностью v , означает, что число n является простым с вероятностью равной v
составное, означает, что число n является составным

для $i = 1, 2, \dots$, пока $i \leq p$:

пусть a – случайное число, $2 \leq a \leq n - 2$

если $a^{n-1} \pmod{n} \neq 1$, то вернуть составное

вернуть простое с вероятностью $1 - \left(\frac{1}{2}\right)^p$

Рассмотрим еще способ генерации простых чисел, способ, основанный на теореме Вильсона: натуральное число $p > 1$ будет простым тогда и только тогда, когда $(p - 1)! + 1$ делится на p , или же: $(p - 1)! \equiv -1 \pmod{p}$ [2].

Запишем алгоритм Вильсона на псевдокоде:

Вход: натуральное число n , которое надо проверить на простоту
Выход: простое, означает, что число n является простым числом
составное, означает, что число n является составным числом

если $((n - 1)! + 1) \pmod{n} = 0$, то вернуть простое
иначе вернуть составное

Теорема Вильсона редко применяется для генерации простых чисел, так как даже эффективные алгоритмы подсчета факториала очень медленные, то есть и сам тест, основанный на данной теореме слишком медленный для практических задач.

Далее, тест Люка-Лемера. Тест Люка-Лемера – это детерминированный и безусловный тест простоты для чисел Мерсенна, без доказательства предложенный Эдвардом Люком в 1878 году. Доказал же его Лемер в 1930 году в своей диссертации. Позднее, в 1952 году при участии Лемера были проведены вычисления на компьютере, в результате которых тест Люка-Лемера открыл простые числа M_{521} и M_{607} [3].

Лемер вывел следующий критерий простоты чисел Мерсенна:

Пусть p – простое число. Число Мерсенна $M_p = 2^p - 1$ простое тогда и только тогда, когда оно делит нацело $(p - 1)$ -й член последовательности S , задаваемой рекуррентно: $S_k = 4$, если $k = 1$, иначе $S_k = S_{k-1}^2 - 2$.

Тест Люка – Лемера позволил найти самое большое простое число на сегодняшний день, являясь основой проекта распределенных вычислений GIMPS.

Запишем алгоритм теста Люка – Лемера на псевдокоде:

Ввод: простое число p , которое является показателем степени в числе Мерсенна $M_p = 2^p - 1$

Вывод: простое, означает, что число $M_p = 2^p - 1$ является простым числом
составное, означает, что число $M_p = 2^p - 1$ является составным числом

Пусть $s = 4$ – первый член последовательности S , $k = 1$ – номер члена последовательности S , $m = 2^p - 1$ – p -ое число Мерсенна.

пока $k \neq p - 1$:

$s = (s^2 - 2) \pmod{m}$

$k = k + 1$

если $s = 0$, то вернуть простое

иначе вернуть составное

Далее, тест Миллера-Рабина – вероятностный тест простоты, являющийся модификацией алгоритма Миллера. Тест Миллера-Рабина опирается на проверку ряда равенств, которые выполняются для простых чисел, если хотя бы одно из них не выполняется, то тогда число – составное, иначе оно вероятно простое.

В основе теста лежит следующее утверждение: пусть n – простое число и $n - 1 = 2^s d$, где d – нечетно. Тогда для любого a из Z_n выполняется хотя бы одно из условий:

1. $a^d \equiv 1 \pmod{n}$;

2. существует целое число $r < s$ такое что $a^{2^r d} \equiv 1 \pmod{n}$ [5].

Высокая скорость и точность работы этого теста позволяет эффективно использовать его для работы криптосхем с открытым ключом, таких как RSA, где требуется быстро проверять большие случайные числа, на простоту.

Запишем алгоритм теста Миллера-Рабина на псевдокоде:

Вход: натуральное число n , которое надо проверить на простоту, натуральное число p , которое задает параметр безопасности
Выход: простое с вероятностью v , означает, что число n является простым с вероятностью равной v
составное, означает, что число n является составным

представить $n - 1$ в виде $n - 1 = 2^s t$, t – нечетное

(1) для $i = 1, 2, \dots$, пока $i \leq p$:

пусть a – случайное число, $2 \leq a \leq n - 2$

пусть $x = a^t \pmod{n}$

если $x = 1$ или $x = n - 1$, то перейти на следующую итерацию цикла (1)

(2) для $j = 1, 2, \dots$, пока $j \leq s - 1$

пусть $x = x^2 \pmod{n}$

если $x = 1$, то вернуть составное

если $x = n - 1$, то перейти на следующую итерацию цикла (1)

вернуть составное

Далее, тест Соловея-Штрассена – $\frac{1}{4}$ -вероятностный тест простоты, открытый Робертом Соловеем и Фолькером Штрассеном. В отличие от всех предыдущих описанных тестов, этот тест всегда корректно определяет, что простое число является простым, однако для составных чисел может дать неверный ответ.

В основе теста лежит малая теорема Ферма и свойства символа Якоби: если n – нечетное составное число, то количество целых чисел a , взаимно простых с n и меньших n , удовлетворяющих сравнению $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, где $\left(\frac{a}{n}\right)$ – символ Якоби, не превосходит $\frac{n}{2}$ [7].

Алгоритм параметризуется количеством «раундов». В каждом таком раунде мы будем выбирать случайное число a , меньше n и проверять справедливость вышеописанного сравнения.

Запишем алгоритм теста Соловея-Штрассена на псевдокоде:

Вход: натуральное число n , которое надо проверить на простоту, натуральное число p , которое задает количество проверок.

Выход: простое с вероятностью v , означает, что число n является простым с вероятностью равной v
составное, означает, что число n является составным.

для $i = 1, 2, \dots$, пока $i \leq p$:

пусть a – случайное число, $2 \leq a \leq n-1$

если $\text{НОД}(a, n) > 1$, то вернуть составное

если $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$, то вернуть составное

вернуть простое с вероятностью $1 - \left(\frac{1}{2}\right)^p$

Большим плюсом теста является то, что он точно распознает числа Кармайкла, однако его точности недостаточно для использования в практических целях. Тест Соловея-Штрассена успешно применяется в решении проблем факторизации [9].

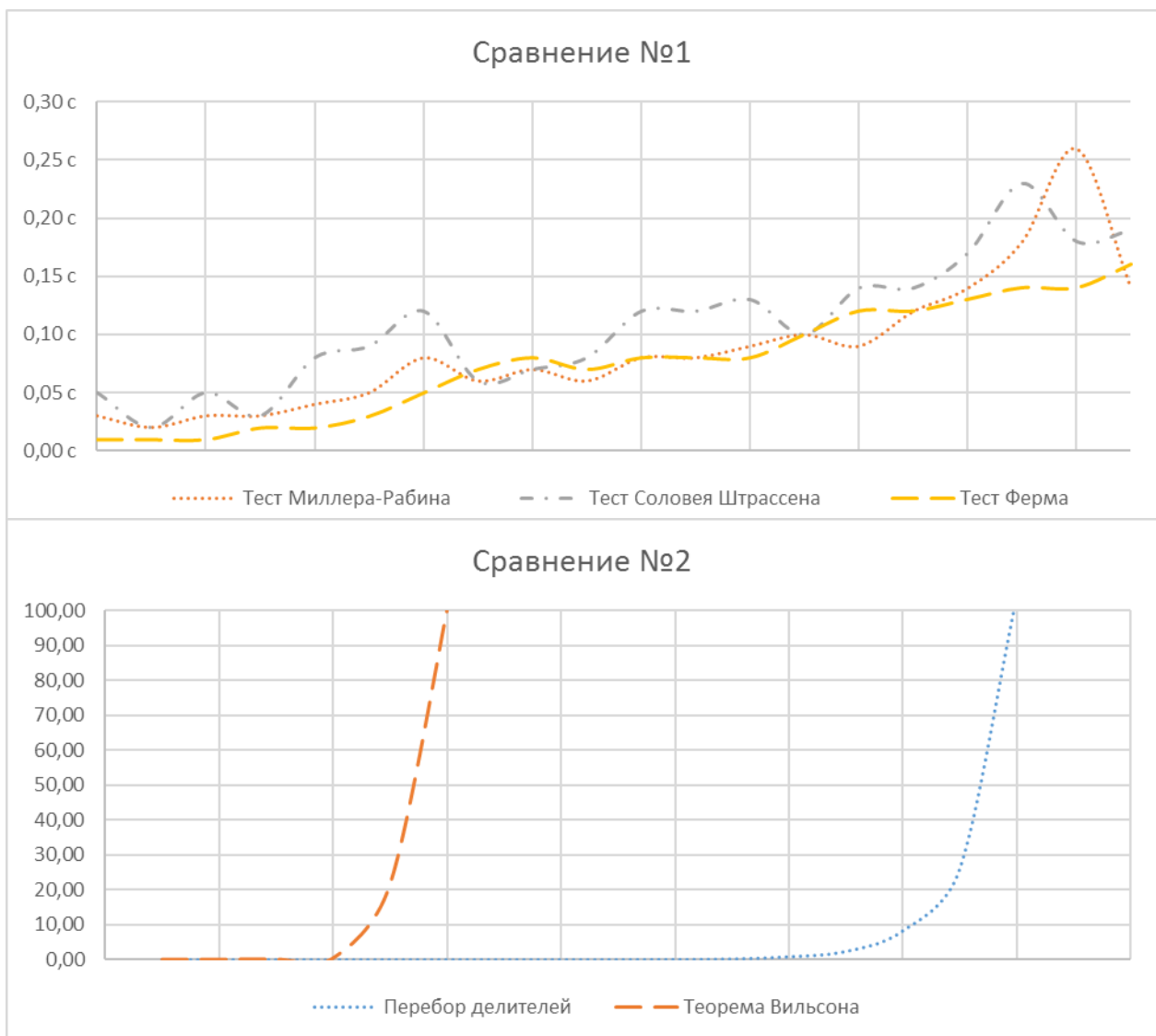
Сравним описанные алгоритмы по разным параметрам:

Название теста	Тип теста	Вероятность	Вычислительная сложность	Примечания
Перебор делителей	истинный	-	$O(n^{\frac{1}{2}})$	Часто используется для нахождения небольших чисел
Теорема Вильсона			$O(p!)$	Подсчет факториала большого числа требует больших вычислительных мощностей и много времени
Тест Люка-Лемера			$O(p^3)$	Самые большие простые числа были найдены при помощи теста Люка-Лемера
Теста Ферма	вероятностный	2^{-k}	$O(\log^3 n)$	Не учитывает бесконечное количество чисел Кармайкла
Тест Соловея-Штрассена		2^{-k}	$O(\log^3 n)$	Учитывает числа Кармайкла, в отличие от теста Ферма, но недостаточно точен.
Тест Миллера-Рабина		4^{-k}	$O(\log^3 n)$	Используется на практике, эффективен и дает высокую вероятность простоты

Мы проверили написанные нами алгоритмы рассмотренных тестов и сравнили их на различных простых числах.

Вероятностные тесты проверялись на числах длиной от 37 до 128 десятичных знаков, для каждого из них был установлен порог в 50 «свидетелей простоты», таким образом, вероятность простоты была очень близка к единице. Алгоритмы на таких числах показали себя примерно на одном уровне.

Перебор делителей сравним на небольших числах с методом, использующим теорему Вильсона, хоть она и уступает в вычислительной сложности. На графике видно, как время работы алгоритма, использующего теорему Вильсона резко возрастает при проверке чисел больших 10^6 , когда же метод перебора делителей быстро работает при числах, меньших чем 10^{16} .



В заключение своей статьи приведем примеры реализации описанных выше алгоритмов на языке Python.

1. Программа «Метод перебора делителей»

2. Программа «Критерий Вильсона»

```
import math

def methodOfSearchOfDivisors(n):
    if n % 2 == 0:
        return False
    for k in range(3, int(math.sqrt(n) + 2), 2):
        if n % k == 0:
            return False
    return True

number = int(input("Введите число: "))
if methodOfSearchOfDivisors(number):
    print("Оно простое")
else:
    print("Оно составное")
```

3. Программа «Тест Люка-Лемера»

```
import math

n = int(input("Введите число: "))

def WilsonTheorem(num):
    if (math.factorial(num - 1) + 1) % num == 0:
        return True
    else:
```

```
p = int(input("Введите простое число P: "))
s = 4
k = 1
m = pow(2, p) - 1
while k != p - 1:
    s = (s * s - 2) % m
    k += 1
if s == 0:
    print("Число 2^P - 1 =", m, "простое")
else:
    print("Число 2^P - 1 =", m, "составное")
```

4.Программа «Тест Ферма»

```
p =int(input("Введите простое число P: "))
s =4
k =1
m =pow(2, p)-1
while k != p -1:
    s =(s*s -2)% m
    k +=1
if s ==0:
print("Число 2^P - 1 =",m, "простое")
else:
print("Число 2^P - 1 =", m, "составное")
```

5.Программа «Тест Миллера-Рабина»

```
import random
n=int(input("Введите число: "))
p =int(input("Введите параметр безопасности: "))

def representation(num):
    num -=1
    i =0
    while num %2==0:
        num //=2
        i +=1
    return num, i

s, t = representation(n)

def testMillerRabin(sec, odd, exp, num):
    for i inrange(sec):
        a = random.randrange(2, num -1)
        x =pow(a, odd, num)
        if x ==1or x == num -1:
            continue
        for j inrange(exp -1):
            x =pow(x,2, num)
        if x == num -1:
            break
        else:
            returnFalse
    returnTrue

if testMillerRabin(p, s, t, n):
print("Это число простое с вероятностью",1-pow(0.5, p))
else:
print("Это число составное")
```

6. Программа «Тест Соловея-Штрассена»

```
import math
import random

n=int(input("Введите число: "))
p =int(input("Введите параметр безопасности: "))

def getting rid(a, b, r):
    t =0
    while a %2==0:
        t +=1
        a //=2
    if t %2!=0:
    if b %8==3or b %8==5:
        r =-r
    if a %4== b %4==3:
        r =-r
        c = a
        a = b % c
        b = c
    return a, b, r

def jacobs(a, b):
    if math.gcd(a, b) !=1:
    return 0
        r =1
        a, b, r = getting rid(a, b, r)
    while a !=0:
        a, b, r = getting rid(a, b, r)
    return r

def testSolovayStrassen(num, sec):
    for i in range(1, sec):
        random.seed()
        a = random.randint(2, num-1)
    if math.gcd(a, num)>1:
    return False
    if pow(a, (num-1)//2, num) != jacobs(a, num)% num:
    return False
    return True
```

Список литературы

1. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии, МЦНМО, 2003
2. Виноградов И. М. Основы теории чисел. — 5 изд. — М.-Л.: Гостехиздат, 1952.
3. Кибернетический сборник: журнал / пер. с англ. С. В. Чудова. — М.: Мир, 1986. — Вып. 23. — С. 51—99.
4. Нестеренко А. Введение в современную криптографию. Теоретико-числовые алгоритмы. — 2011. — С. 79 - 90. — 190 с.
5. Кормен Т., Лейзер Ч. Глава 33.8. Проверка чисел на простоту // Алгоритмы. Построение и анализ
6. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2001. — С. 42 - 59. — 104 с.
7. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие // Казань: Казанский университет. — 2011
8. Томас Кормен, Чарльз Лейзерстон, Рональд Ривест, Клиффорд Штайн. Section 31.8: Primality testing // Introduction to Algorithms. — Second Edition. — MIT Press; McGraw-Hill, 2001. — P. 889–890.
9. Menezes, A. J. (Alfred J.), 1965-. Handbook of applied cryptography. — Boca Raton: CRC Press, 1997. — xxviii, 780 pages c.

О ПРИМЕНЕНИИ АЛГЕБРАИЧЕСКИХ МЕТОДОВ ПРИ РЕШЕНИИ ЭКОНОМИЧЕСКИХ ЗАДАЧ

**Сикорская Г.А., д-р пед. наук, доцент, Яковлева О.Е.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Современная экономика базируется на многих математических дисциплинах. Так, применение арифметических и геометрических прогрессий дает возможность рассчитать процессы, связанные с последовательностями экономических показателей и объектов. Комбинаторика позволяет определять результаты, возникающие при различных сочетаниях экономических объектов, их перестановках и размещениях. Геометрия применяется при вычислениях, связанных с пространственными отношениями и формами экономических объектов. Математическая логика дает возможность оценки экономической ситуации с точки зрения истинности или ложности используемой информации. С помощью инструментов теории вероятностей возможны обоснование экономических расчетов, связанных с явлениями случайного характера. Математическая статистика обеспечивает сбор, обработку и анализ экономических статистических материалов[2].

Очевидно, для решения экономической задачи необходимо вначале уяснить ее смысл и, соответственно, установить цель решения. После чего, выяснив основные пороги достижения установленной цели, то есть детально оценить экономическую ситуацию. А далее, - определить наиболее значимый численный показатель и построить математическую модель, устанавливающую количественные зависимости избранного показателя от условий задачи.

Приведем пример небольшой экономической задачи.

Надо купить товар весом в 50 кг. при условии, что взвешивание производилось некоторое время тому назад, и при этом было определено процентное содержание в товаре жидкости, которое составляло 96%. На момент покупки, за счет усушки, доля жидкости уменьшилась до 92%. Необходимо рассчитать, сколько весит предлагаемый товар.

Решение. Вначале рассчитаем процент и вес сухого остатка в товаре. При первом замере жидкости сухой остаток составлял 4% и весил 2 кг. При втором замере, соответственно, 8% и снова 2 кг (вес сухого остатка не меняется). Составляем пропорцию:

8% - 2 кг,

100%- x кг.

Откуда, находим $x=25$ кг.

Предметом нашего исследования является изучение применения основ линейной и векторной алгебры при решении экономических задач.

Начнем с разработки и использования данных. Наиболее удобно хранение и обработка данных в матричной форме.

Пусть, например, распределения ресурсов по отдельным отраслям экономики выглядит следующим образом:

Ресурсы	Отрасли экономики	
	Промышленность	Сельское хозяйство
Электроэнергия	5,9	4,8
Трудовые ресурсы	4,2	6,3
Водные ресурсы	7,3	5,6

Матрицей данную таблицу и показатели можно записать в более компактной форме:

$$\begin{pmatrix} 5,9 & 4,8 \\ 4,2 & 6,3 \end{pmatrix}$$

Или, например, какое – либо предприятие выпускает продукцию трех видов K_1 (брюки), K_2 (свитера), K_3 (платья). На изготовление продукции уходит два вида сырья S_1 (хлопок), S_2 (шерсть).

Для определения расхода сырья составляем матрицу:

$$A = \begin{pmatrix} 34 & 45 \\ 13 & 21 \end{pmatrix}$$

В этой матрице каждый элемент a_{ij} – это единицы сырья каждого типа, которые расходуются на производство единицы каждого вида. Также дан план выпуска всей продукции – матрица

$$B = (80 \ 51 \ 17).$$

Кроме того, указана стоимость единицы каждого типа сырья в виде матрицы

$$C = \begin{pmatrix} 25 \\ 16 \end{pmatrix}$$

Найдем при заданных данных, общую стоимость сырья.

Способ первый:

Находим отдельно затраты первого и второго вида сырья.

$$S_1 = 34 \cdot 80 + 13 \cdot 51 + 26 \cdot 17 = 3825 \text{ единиц.}$$

$$S_2 = 45 \cdot 80 + 21 \cdot 51 + 34 \cdot 17 = 5249 \text{ единиц.}$$

Способ второй:

Все известные нам значения записаны с помощью матриц A и B , тогда их произведение $B \cdot A$ – это затраты сырья

$$S=B \cdot A=(80 \cdot 51 \cdot 17) \cdot \begin{pmatrix} 34 & 45 \\ 13 & 21 \\ 26 & 34 \end{pmatrix}=(3825 \quad 5249)$$

Следующим действием находим общую стоимость сырья:

$$Q=3825 \cdot 25+5249 \cdot 16=179609$$

В матричном виде:

$$Q=S \cdot C=(B A) C=(3825 \quad 5249) \cdot \begin{pmatrix} 25 \\ 16 \end{pmatrix}=(179609)$$

Таким образом, общая стоимость сырья 179609.

Рассмотрим еще одну задачу.

Каждое предприятие выпускает 3 вида продукции с потреблением трех разных видов сырья, у каждого есть продолжительность работы в году, а также цена. Требуется выяснить производительность каждого предприятия, по каждому виду изделия за год; потребность каждого предприятия по каждому виду сырья за год; а также годовую сумму каждого предприятия для закупки сырья, необходимого при определенном количестве рабочих дней и выпуска изделий.

Составим таблицу со всеми исходными данными.

Вид изделия	Производительность предприятия			Затраты сырья		
	<i>I</i>	<i>II</i>	<i>III</i>	<i>1</i>	<i>2</i>	<i>3</i>
<i>1</i>	4	3	9	4	5	2
<i>2</i>	5	2	8	3	4	3
<i>3</i>	6	4	7	8	6	7
	Кол-во дней отработанных за год			Цена каждого сырья		
	150	170	120	32	24	16

Теперь составим матрицу, характеризующую экономическую совокупность производства.

$$A=\begin{pmatrix} 4 & 3 & 9 \\ 5 & 2 & 8 \\ 6 & 4 & 7 \end{pmatrix}$$

Каждый столбец матрицы соответствует производительности каждого предприятия по каждому виду продукции. Отсюда следует, что годовая производительность каждого предприятия по каждому виду продукции получается умножением каждого элемента матрицы А на количество рабочих дней в году, для каждого предприятия ($i=1,2,3,4,5$), где i – это количество рабочих дней в году. Таким образом, годовая производительность каждого предприятия по каждому изделию описывается матрицей.

$$A_{\text{Год}} = \begin{pmatrix} 4 \cdot 150 & 3 \cdot 170 & 9 \cdot 120 \\ 5 \cdot 150 & 2 \cdot 170 & 8 \cdot 120 \end{pmatrix} = \begin{pmatrix} 600 & 510 & 1080 \\ 750 & 340 & 960 \end{pmatrix}$$

Матрица затрат сырья на единицу изделия имеет вид:

$$B = \begin{pmatrix} 4 & 3 & 8 \\ 5 & 4 & 6 \end{pmatrix}$$

Определяем расход по всем видам сырья:

$$A \cdot B = \begin{pmatrix} 4 & 3 & 9 \\ 5 & 2 & 8 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 & 8 \\ 5 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 49 & 51 & 113 \\ 46 & 47 & 108 \end{pmatrix}$$

Для того чтобы определить потребность каждого предприятия по каждому виду сырья за год умножим матрицу АВ на количество дней, отработанных за год.

$$C = \begin{pmatrix} 49 \cdot 150 & 51 \cdot 170 & 113 \cdot 120 \\ 46 \cdot 150 & 47 \cdot 170 & 108 \cdot 120 \end{pmatrix} = \begin{pmatrix} 7350 & 8670 & 13560 \\ 6900 & 7990 & 12960 \end{pmatrix}$$

Чтобы определить стоимость годового запаса сырья для каждого предприятия необходимо матрицу С умножить на матрицу D–матрицу стоимости сырья. $D=(322416)$

$$\begin{pmatrix} 7350 \cdot 32 & 8670 \cdot 24 & 13560 \cdot 16 \\ 6900 \cdot 32 & 7990 \cdot 24 & 12960 \cdot 16 \end{pmatrix} = \begin{pmatrix} 235200 & 208080 & 216960 \\ 220800 & 1919760 & 207360 \end{pmatrix}$$

Следовательно, мы нашли суммы кредитования предприятий для закупки сырья.

$$\text{Ответ: } \begin{pmatrix} 235200 & 208080 & 216960 \\ 220800 & 1919760 & 207360 \end{pmatrix}$$

Далее, рассмотрим использование систем линейных уравнений в экономике.

Задача. Обувная фабрика специализируется по выпуску изделий трех видов: сапог, кроссовок и ботинок; при этом используется сырье трех типов: S_1, S_2, S_3 . Нормы расхода каждого из них на одну пару обуви и объем расхода сырья на 1 день заданы таблицей

:

	Нормы расхода сырья на одну пару, усл. ед.			Расход сырья на 1 день, усл. ед.
	Сапоги	Кроссовки	Ботинки	
S_1	2	3	5	600
S_2	1	1	2	250
S_3	2	3	4	550

Найти ежедневный объем выпуска каждого вида обуви.

Решение. Пусть ежедневно фабрика выпускает x_1 пар сапог, x_2 пар кроссовок, x_3 пар ботинок. Тогда в соответствии с расходом сырья каждого вида имеем систему:

$$\begin{cases} 2x_1 + 3x_2 + 5x_3 = 600 \\ x_1 + x_2 + 2x_3 = 250 \\ 2x_1 + 3x_2 + 4x_3 = 550 \end{cases}$$

Решим систему по теореме Крамера.

$$\Delta = \begin{vmatrix} 2 & 3 & 5 \\ 1 & 1 & 2 \\ 2 & 3 & 4 \end{vmatrix} = 2 \cdot 1 \cdot 4 + 3 \cdot 2 \cdot 2 + 3 \cdot 1 \cdot 5 - 5 \cdot 1 \cdot 2 - 3 \cdot 2 \cdot 2 - 3 \cdot 1 \cdot 4 = 1$$

Т.е. система имеет единственное решение:

$$\Delta_1 = \begin{vmatrix} 600 & 3 & 5 \\ 250 & 1 & 2 \\ 550 & 3 & 4 \end{vmatrix} = 600 \cdot 1 \cdot 4 + 3 \cdot 2 \cdot 550 + 3 \cdot 250 \cdot 5 - 5 \cdot 1 \cdot 550 - 3 \cdot 2 \cdot 600 - 3 \cdot 250 \cdot 4 = 100$$

$$x_1 = \frac{\Delta_1}{\Delta} = \frac{100}{1} = 100$$

$$\begin{vmatrix} 2 & 600 & 5 \\ & & \end{vmatrix}$$

$$\Delta_2 = \begin{vmatrix} 1 & 250 & 2 \\ 2 & 550 & 4 \end{vmatrix} = 2 \cdot 250 \cdot 4 + 600 \cdot 2 \cdot 2 + 550 \cdot 1 \cdot 5 - 5 \cdot 250 \cdot 2 - 550 \cdot 2 \cdot 2 - 600 \cdot 1 \cdot 4 = 50$$

$$x_2 = \frac{\Delta_2}{\Delta} = \frac{50}{1} = 50$$

$$\Delta_3 = \begin{vmatrix} 2 & 3 & 600 \\ 1 & 1 & 250 \\ 2 & 3 & 550 \end{vmatrix} = 2 \cdot 1 \cdot 550 + 3 \cdot 250 \cdot 2 + 3 \cdot 1 \cdot 600 - 600 \cdot 1 \cdot 2 - 3 \cdot 250 \cdot 2 - 3 \cdot 1 \cdot 550 = 50$$

$$x_3 = \frac{\Delta_3}{\Delta} = \frac{50}{1} = 50$$

Т.е. фабрика выпускает 100 пар сапог, 50 пар кроссовок и 50 пар ботинок.

Ответ: (100, 50, 50).

Помимо матриц и матричных уравнений в экономике часто используются и векторы.

Например, необходимо вычислить производственные показатели предприятия, которые отображены в следующей таблице.

Вид изделий	Кол-во изделий	Расход сырья	Норма времени изготовления	Цена (руб.)
1	25	7	6	13
2	20	3	10	16
3	15	8	7	20
4	10	5	15	18

Необходимо определить следующие ежесуточные показатели: расход сырья А, затраты рабочего времени В и стоимость С выпускаемой продукции предприятия. По приведенным данным составим векторы, которые характеризуют весь производственный цикл:

$r = (25, 20, 15, 10)$ – вектор ассортимента;

$a = (7, 3, 8, 5)$ – вектор расхода сырья;

$b = (6, 10, 7, 15)$ – вектор затрат рабочего времени;

$c = (13, 16, 20, 18)$ – ценовой вектор.

Тогда величины, которые нам нужно найти, будут равны скалярным произведениям вектора ассортимента на три других вектора:

$A = r \cdot a = 25 \cdot 7 + 20 \cdot 3 + 15 \cdot 8 + 10 \cdot 5 = 405$ кг;

$$B = pb = 25 \cdot 6 + 20 \cdot 10 + 15 \cdot 7 + 10 \cdot 15 = 605 \text{ ч};$$

$$C = pc = 25 \cdot 13 + 20 \cdot 16 + 15 \cdot 20 + 10 \cdot 18 = 1125 \text{ руб.}$$

Ответ: 405 кг, 605 ч, 1125 руб.

Рассмотрим еще задачу, демонстрирующую применение основ векторной алгебры в экономике.

В таблице представлены ежесуточные экономические показатели завода:

Вид изделия	Расход сырья (кг)	Время изготовления (ч)	Количество изделий	Цена изделий (рублей)
1.Протяжки шпоночные	10	5	30	70
2. Резец токарный, пластина из твердого сплава T15K6	7	16	18	320
3. Развертка	4	31	5	400
4. Головка торцевая	6	14	10	150

Найдем цены, расходы и затраты сырья.

Для решения поставленной задачи введем четыре вектора для рассмотрения производственного процесса.

$p = (10, 7, 4, 6)$ – вектор расход сырья.

$t = (5, 16, 31, 14)$ – вектор времени.

$b = (30, 18, 5, 10)$ – вектор изделия товара.

$c = (70, 320, 400, 150)$ – вектор цены.

Заметим, что соответствующие скалярные произведения векторов, будут представлять собой искомые величины.

$$b \cdot p = 30 \cdot 10 + 18 \cdot 7 + 5 \cdot 4 + 10 \cdot 6 = 300 + 126 + 20 + 60 = 506 \text{ килограмм}$$

$$b \cdot t = 30 \cdot 5 + 18 \cdot 16 + 5 \cdot 31 + 10 \cdot 14 = 150 + 288 + 155 + 140 = 733 \text{ часа}$$

$$b \cdot c = 30 \cdot 70 + 18 \cdot 320 + 5 \cdot 400 + 10 \cdot 150 = 2100 + 5760 + 2000 + 1500 = 11360 \text{ рублей}$$

Ответ: 506 килограмм, 733 часа и 11360 рублей.

Далее рассмотрим некоторые применения основ линейной алгебры к моделированию экономических процессов. Очевидно, что к моделированию прибегают всегда, когда необходимо разобраться в каком-нибудь сложном явлении, уловить его скрытые закономерности. Так экономическое моделирование применяется для изучения производственных возможностей. Производственные возможности показывают способность предприятия производить различные наборы (сочетания) товаров при постоянстве ресурсов и при условии их полного использования[6].

Рассмотрим формулу эффективности (Э):

$$\mathcal{E} = P/Z$$

где P – результат деятельности, Z – затраты на получение данного результата.

При построении моделей многих экономических процессов используются основы линейной алгебры. Так, в качестве примера математической модели экономического процесса, приводящей к понятию собственного вектора и собственного значения матрицы, рассмотрим линейную модель обмена (модель международной торговли).

$$a_{1j} + a_{2j} + \dots + a_{nj} = 1 \quad (j = 1, 2, \dots, n).$$

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

$$p_i = a_{i1} x_1 + a_{i2} x_2 + \dots + a_{in} x_n.$$
$$p_i \geq x_i \text{ (i = 1,2,...,n)}.$$
[illegible]
$$x_1(a_{11} + a_{21} + \dots + a_{n1}) + x_2(a_{12} + a_{22} + \dots + a_{n2}) + \dots + x_n(a_{1n} + a_{2n} + \dots + a_{nn}) \\ > x_1 + x_2 + \dots + x_n.$$
$$x_1 + x_2 + \dots + x_n > x_1 + x_2 + \dots + x_n.$$

Таким образом, неравенство $p_i > x_i$ ($i = 1, 2, \dots, n$) невозможно, и условие $p_i \geq x_i$ принимает вид $p_i = x_i$ ($i = 1, 2, \dots, n$) (с экономической точки зрения это понятно, так как все страны не могут одновременно получать прибыль.)[6].

Вводя вектор $x = (x_1, x_2, \dots, x_n)$ национальных доходов стран, получим матричное уравнение:

$$AX = X,$$

где X - матрица-столбец из координат вектора x , т.е. задача свелась к отысканию собственного вектора матрицы A , отвечающего собственному значению, равному единице.[5]

Межотраслевой баланс (МОБ, метод «затраты-выпуск») — экономико-математическая балансовая модель, характеризующая межотраслевые производственные взаимосвязи в экономике страны; связи между выпуском продукции в одной отрасли; затратами, расходом продукции всех участвующих отраслей, необходимым для обеспечения этого выпуска.

Рассмотрим модель Леонтьева многоотраслевой экономики. Эта модель отражает многие существенные особенности современного производства и в то же время сравнительно легко поддается расчету. Во многих странах мира модель Леонтьева используется для экономического анализа, планирования и прогнозирования.

Основной задачей данной модели Леонтьева является нахождение вектора валового выпуска (X) по известному вектору конечного потребления (Y) и матрице коэффициентов прямых затрат (A), что эквивалентно решению балансового уравнения (в матричной записи):

$$X = A \cdot X + Y \quad (1)$$

Откуда,

$$X = (E - A)^{-1} Y.$$

Матрицу $(E - A)^{-1}$ называют матрицей коэффициентов косвенного потребления.

Условием разрешимости балансового уравнения является существование и неотрицательность данной матрицы, т.е. неотрицательность каждого ее элемента.

Справедливо соотношение

$$(E - A)^{-1} = E + A + A^2 + \dots$$

Откуда

$$X = Y + AY + A^2Y + \dots \quad (2)$$

Соотношение (2) показывает, что весь валовой выпуск складывается из затрат: 0-го порядка (Y), 1-го порядка (AY), 2-го порядка (A^2Y) и т.д.

Очевидно, что при решении относительно простого балансового уравнения (1) необходимо применять знания линейной алгебры: нахождение произведения матриц; вычисление обратной матрицы; нахождение собственных векторов и собственных значений матрицы.

Рассмотрим задачу: в таблице приведены коэффициенты прямых затрат и конечная продукция отраслей на плановый период, у.д.е.

Отрасль		Потребление		Конечный продукт
		Промышленность	Сельское хозяйство	
Производство	Промышленность	0,4	0,25	160
	Сельское хозяйство	0,4	0,5	200

Найти плановые объёмы валовой продукции отраслей, межотраслевые поставки, чистую продукцию отраслей.

Решение: Выпишем матрицу коэффициентов прямых затрат A , вектор конечной продукции Y :

$$A = \begin{pmatrix} 0,4 & 0,25 \\ 0,4 & 0,5 \end{pmatrix}$$

$$Y = \begin{pmatrix} 160 \\ 200 \end{pmatrix}$$

Заметим, что матрица A продуктивна, так как её элементы положительны и сумма элементов в каждом столбце меньше единицы.

1. Найдём матрицу

$$E - A = \begin{pmatrix} 1-0,4 & -0,25 \\ -0,4 & 1-0,5 \end{pmatrix} = \begin{pmatrix} 0,6 & -0,25 \\ -0,4 & 0,5 \end{pmatrix}$$

Тогда матрица полных затрат:

$$S = (E - A)^{-1} = \begin{pmatrix} 2,5 & 1,25 \\ 2 & 3 \end{pmatrix}$$

2. По формуле $X = (E - A)^{-1} \cdot Y = SY$ найдём вектор валового продукта X :

$$X = \begin{pmatrix} 2,5 & 1,25 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 160 \\ 200 \end{pmatrix} = \begin{pmatrix} 650 \\ 920 \end{pmatrix}$$

4. Межотраслевые поставки x_{ij} найдём по формуле $x_{ij} = a_{ij} \cdot x_j$
 $x_{11} = a_{11} \cdot x_1 = 0,4 \cdot 650 = 260$;

$$x_{12} = a_{12} \cdot x_2 = 0,25 \cdot 920 = 230$$

$$x_{21} = a_{21} \cdot x_1 = 0,4 \cdot 650 = 260$$

$$x_{22} = a_{22} \cdot x_2 = 0,5 \cdot 920 = 460$$

5. Чистая продукция промышленности равна: $650 - 260 - 260 = 130$

Чистая продукция сельского хозяйства: $920 - 230 - 460 = 230$

На примере рассмотренных задач мы продемонстрировали значимость вклада вносимого линейной и векторной алгеброй в экономику. Нельзя переоценить пользу использования методов алгебры в экономических задачах. Конечно, не все экономические процессы и изменения можно описать, используя только алгебраический инструмент, но большинство расчетов существенно упрощается в результате использования линейной и векторной алгебры.

Список литературы

1. Блинова Ю.Ю., Родина Е.В. Решение экономических задач матричным методом // Современные наукоемкие технологии. 2014. № 5-2. С. 140-142
2. Гулай Т.А., Долгополова А.Ф., Мелешко С.В. Математические методы исследования экономических процессов // Международный журнал экспериментального образования. 2016. № 12-1. С. 116-117
3. Линейная алгебра / Крон Р.В., Попова С.В., Смирнова Н.Б., Долгих Е.В. // учебное пособие для студентов вузов сельскохозяйственных, инженерно-технических и экономических направлений / Москва, 2015.
4. Манько А.И., Гулай Т.А., Жукова В.А., Мелешко С.В., Невидомская И.А. Обзор методов социально-экономического прогнозирования и их применение в реальной экономике // Наука и образование: современные тренды. 2015. № 2 (8). С. 438-448.
5. Немцова А.В., Попова С.В. Применение средств матричной алгебры для решения задач экономического содержания // Современные наукоемкие технологии. 2014. № 5-2. С. 171 - 172.
6. Чупрынов, Б.П. Математика в экономике: математические методы и модели: Учебник для бакалавров / М.С. Красс, Б.П. Чупрынов; Под ред. М.С. Красс. - М.: Юрайт, 2013. - 541 с.
7. Carter R. A. L., Zellner A. The ARAR Error Model for Univariate Time Series and Distributed Lag // Studies in Nonlinear Dynamics & Econometrics. 2004. 8(1), article 2.

АНАЛИЗ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ ВЫСОКОГО УРОВНЯ

**Синицын Ю.И., канд.техн.наук, доцент, Байков В.А.
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Введение. В настоящее время все чаще используются системы видеонаблюдения для систематического вывода, анализа и интерпретации данных, необходимых для прогнозирования, планирования, оценки и обеспечения общественной безопасности. В статье предложена структура системы видеонаблюдения, которая позволяет осуществлять доступ к данным от видеокамер и основана на интегрированных системах наблюдения.

Точность результатов значительно улучшится, если будет использована иерархическая интегрированная архитектура видеонаблюдения (FVSA). На высоком уровне FVSA состоит из аппаратной структуры, поддерживаемой программным интерфейсом.

FVSA представляет систему видеонаблюдения в виде иерархической системы, где границы подсистем основаны на административной собственности и географическом положении.

В целом, система видеонаблюдения на основе FVSA будет удовлетворять следующим требованиям:

- FVSA может сделать данные доступными, где могут автоматически запрашиваться любые «открытые» системы видеонаблюдения;
- иметь унифицированный интерфейс интеллектуального анализа данных независимых систем видеонаблюдения через надежный программный интерфейс приложения (API);
- система видеонаблюдения может работать в существующей системе компьютерных сетей [1].

Сервис-ориентированная сетевая архитектура:

- повысит точность результатов видеонаблюдения;
- имеет автономную и непрерывную идентификацию;
- отслеживает и исследует объекты с любой видеокамеры;
- генерирует информацию для принятия обоснованных решений;
- имеет высокий уровень авторизации и аутентификации;
- выполняет высокое сжатие видеоданных (для хранения).

Методы решения. В статье мы предлагаем новую структуру, которая поддерживает автоматическую генерацию данных видеонаблюдения и контролируемый доступ к данным из любой разрешенной системы видеонаблюдения с целью повышения точности предупреждений безопасности, системы планирования общественной безопасности и поддержки принятия решений, основанные на государственных системах видеонаблюдения.

На рисунке 1 показана концептуальная модель системы видеонаблюдения высокого уровня FVSA с системными службами в модульном представлении, где представлены следующие модули [2]:

- сетевые видеорегистраторы (i-NVR - предназначены для удаленного мониторинга, управления и записи видео и аудио информации от IP-видеосерверов и IP-видеокамер);
- служба очереди;
- сервер данных (MDS);
- хранилище видеоданных;
- сервер аналитики;
- веб-службы;
- пользовательская компьютерная система.

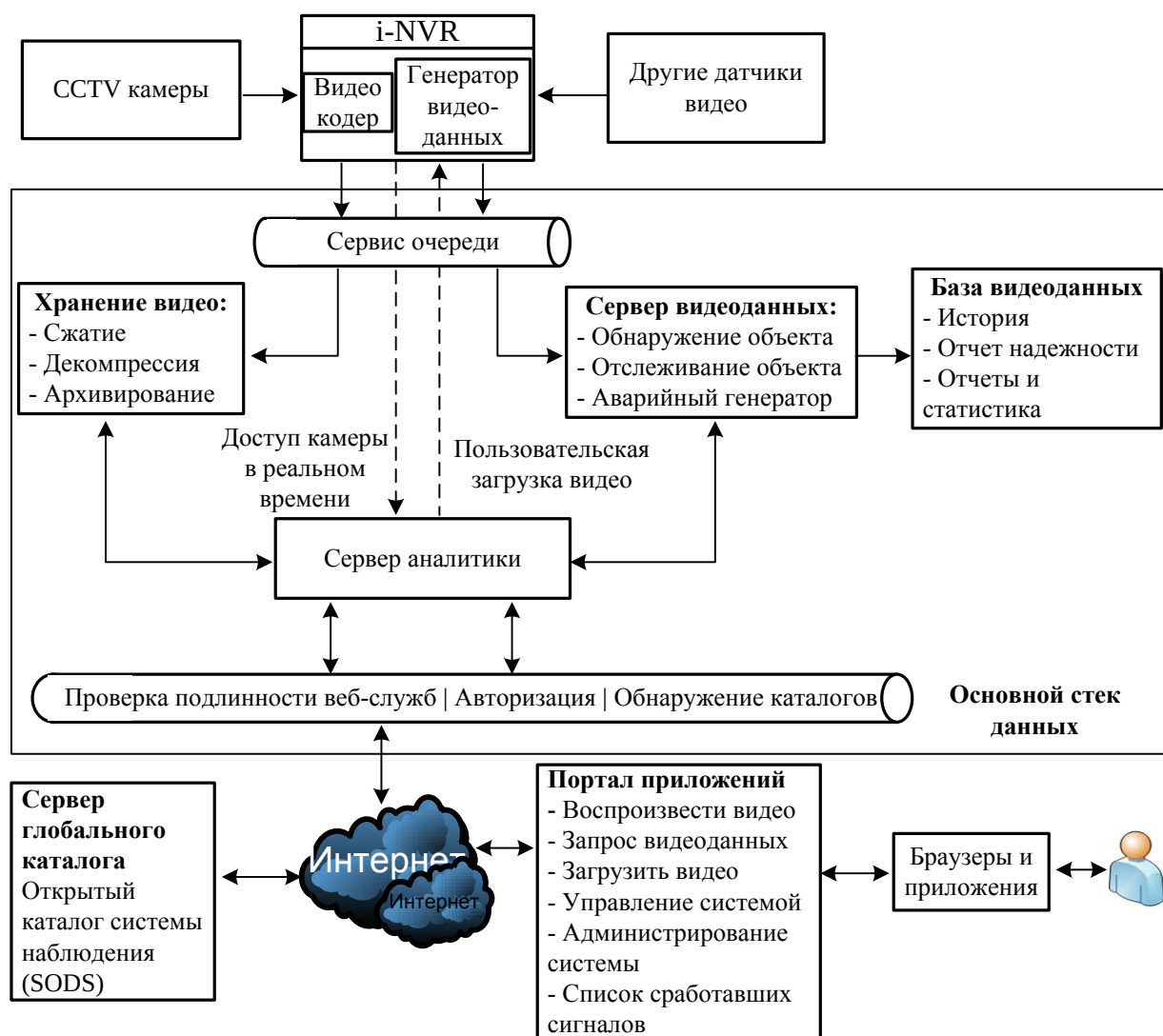


Рисунок 1 - Концептуальная модель системы видеонаблюдения высокого уровня FVSA с системными службами в модульном представлении

Сервер аналитики. Сервер аналитики отвечает за аналитику и исследование видеоданных, он отвечает за выполнение запросов, генерирование трендов, предупреждений, прогнозирование будущих событий на основе изучения более ранних событий. Эта система в идеале реализация надежной платформы больших данных, такой как стек Apache Hadoop. Платформа Big Data может быть развернута на обычных компьютерах, так что стоимость оборудования может быть низкой для небольших систем с простотой масштабирования. Она содержит совместимые механизмы баз данных / решение для хранения и управления видеоданными.

Хранилище (хранилище видеоданных, база видеоданных). Интеллектуальное хранилище позволяет временно сжимать, распаковывать и архивировать видеоданные. Видеоданные, перед сохранением их в течение определенного времени, могут распаковаться (упаковываться) и передаться на блок обработки. По истечении заданного времени (установленным программно) программный интерфейс выдает команду на удаление архивного видео, тем самым освобождается место на накопителе (магнитном носителе) для новых видеоданных. Видеоданные содержат информацию, извлеченную из видеокладов, включая идентификацию камеры, захваченные объекты и т.д. Сервер видеоданных (VDS) должен быть включен в любую реализацию этой архитектуры независимо от размера компьютерной сети - он индексирует и хранит видеоданные и отвечает за следующие операции:

- определение типа всех видеокамер в компьютерной сети (он получает данные от них);
- видеоданные являются основным интегрированным ресурсом в этой архитектуре - все запросы / исследования по наблюдению проводятся на видеоданных через API;
- он действует как сетевой идентификатор.

Интеллектуальные сетевые видеорегистраторы (i-NVR). В дополнение к подключению нескольких камер, i-NVR кодирует видеофайлы и генерирует видеоданные перед отправкой их на хранение [2].

Система массового обслуживания (СМО). Система, которая производит обслуживание поступающих в неё требований. Обслуживание требований в СМО осуществляется активным коммутационным оборудованием компьютерной сети.

Веб-сервисы RESTful (REST определяет ряд архитектурных принципов проектирования Web-сервисов, ориентированных на системные ресурсы, включая способы обработки и передачи состояний ресурсов по HTTP разнообразными клиентскими приложениями, написанными на различных языках программирования). Управляют всеми входящими и исходящими трафиками. Они включают в себя систему безопасности в смысле аутентификации, авторизации, управления сессиями и аудита системы. Они также автоматически обнаруживает и регистрирует или обновляет службу каталогов.

Сервер каталогов (средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации). Эта служба обнаруживает, проверяет и организует уникальную идентификацию для всех развернутых объектов систем видеонаблюдения.

Служба отвечает за каталогизацию доступных сведений о видеосистеме и контактных данных.

Пользовательская система. Он состоит из пользовательского портала и устройств, как настольный компьютер, планшет, мобильные телефоны и средства дистанционного зондирования устройств, такие как спутниковые камеры, видеокамеры дорожного движения и мобильные устройства, используемые сотрудниками службы общественной безопасности.

Портал предоставляет интерфейс для сбора видеоданных с разных устройств и для запроса и реагирования на действия пользователя, такие как загрузка данных, воспроизведение видео и запрос данных.

На практике, некоторые из модулей могут быть объединены - например, установлены веб-службы, сервер данных (исключая хранилище) и службы очередей на сервере аналитики, который в идеале является реализацией платформы больших данных, такой как платформа Apache Hadoop.

Стоит отметить, что описанная выше структура может быть построена в зависимости от количества установленных камер и бюджета организации. Если мы рассмотрим случай, который требует только 1 камеру, то видеокамера может быть оборудована для выполнения функций i-NVR в дополнение к съемке объектов.

В небольших видеосистемах, состоящих только из нескольких видеокамер, интеллектуальная камера может выполнять комбинированные операции. Однако в больших системах вся обработка видео может быть достигнута на i-NVR, в то время как неинтеллектуальные видеокамеры с высоким разрешением могут быть используется для сбора данных. Системный администратор может настроить несколько камер в одной сети наблюдения, даже если они развернуты в разных географических точках. Это может быть достигнуто путем иерархической настройки i-NVR.

Сетевая архитектура может расти только до ограниченного размера - там, где ограничение диктуется емкостью памяти маршрутизатора, мощностью обработки процессора и скорости передачи. Для того, чтобы построить большие компьютерные сети, где маршрутизация может эффективно масштабироваться, существует потребность в иерархическом проектировании. Иерархическая сеть разбита на области(или на подсети), где каждое устройство маршрутизации имеет полное знание только о своей локальной области. Для каждой компьютерной подсети существует межсетевой маршрутизатор, который знает характеристики и параметры соседних подсетей [1].

Компьютерные подсети основаны на этажных подсетях, ведомственных компьютерных сетях, общих сетях компаний и городских компьютерных сетях. Эти разделы обычно определяются политикой и правом собственности,

они повышают масштабируемость, производительность, безопасность и эффективность больших компьютерных сетей.

Заключение. Решения, предложенные в статье, включают унификацию независимых систем видеонаблюдения. Реализация FVSA позволяет независимой системы интегрироваться для создания более крупных компьютерных систем видеонаблюдения (или унифицированных систем). В результате мы предлагаем иерархическую конфигурацию высокого уровня для устройств и служб систем видеонаблюдения, которая позволит взаимодействовать как с локальными, так и глобальными системами видеонаблюдения. Структура системы видеонаблюдения позволит осуществлять доступ к данным от видеокамер и основана на интегрированных системах видеонаблюдения.

Список литературы

1. Синицын Ю.И. Разработка аппаратного обеспечения для подсистемы видеонаблюдения. Сборник статей Международной научно-практической конференции «Материалы и методы инновационных исследований и разработок». Часть 1. Самара НИЦ АЭТЕРНА - 10 марта 2018.. - С. 28 – 30.

2. Системы интеллектуального видеонаблюдения [Электронный ресурс]. – Режим доступа: https://rvigroup.ru/download/RVi_2019.pdf (дата обращения: 14.12.2019)

ИССЛЕДОВАНИЕ АРХИТЕКТУРЫ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Синицын Ю. И., канд.техн.наук, доцент, Гриценко А. Д.

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Введение. Использование средств видеонаблюдения в качестве одного из рубежей комплексной защиты объектов информатизации, позволяет проводить мониторинг помещений в режиме реального времени с возможностью записи и последующего анализа видео. Это делает эту работу востребованной и актуальной. Использование организацией систем видеонаблюдения позволяет защитить объекты информатизации от незаконных действий со стороны злоумышленника, либо избежать этого на этапах их зарождения. Так же система видеонаблюдения помогает в предотвращении внештатных ситуаций на объекте и дисциплинарных нарушений сотрудников за счет непрерывного наблюдения за их работой.

За счет грамотного усовершенствование подсистемы видеонаблюдения есть возможность сократить расходы на человеческие ресурсы и уменьшить время реагирования на прецеденты информационной безопасности. В следствии того, что один или несколько операторов подсистемы видеонаблюдения могут производить наблюдение за всем объектом информатизации и своевременно принимать решения по устранению внештатной ситуации [1].

Обеспечение безопасности объекта информации состоит в решении трех взаимосвязанных задач:

- конфиденциальность;
- целостность;
- доступность.

Основные задачи, стоящие перед системой видеонаблюдения можно обозначить как:

- обнаружение объекта наблюдения;
- распознавание;
- идентификация.

На рисунке 1 представлена наиболее полная концептуальная модель информационной безопасности, которая является общей для всех информационных систем.

Источниками информации на объекте защиты являются документы и электронные носители. Основные угрозы – это угрозы целостности и конфиденциальности, а цели угроз – это хищение, уничтожение и модификация защищаемой информации. Способы утечки – утечка и несанкционированный доступ (НСД) к информации [1].

Методы решения. На рисунке 2 изображена интеллектуальная система видеонаблюдения, состоящая из трех разных уровней. Подсистема получает аудиовизуальные данные с видеокамер, микрофонов и считывателей. Изначально низкоуровневый контекстный модуль на нижнем уровне собирает видеоданные от источников оборудования в зоне мониторинга. Данные, полученные от различных источников, передаются в модуль высокого уровня. Модуль высокого уровня распознает действия человека[2].

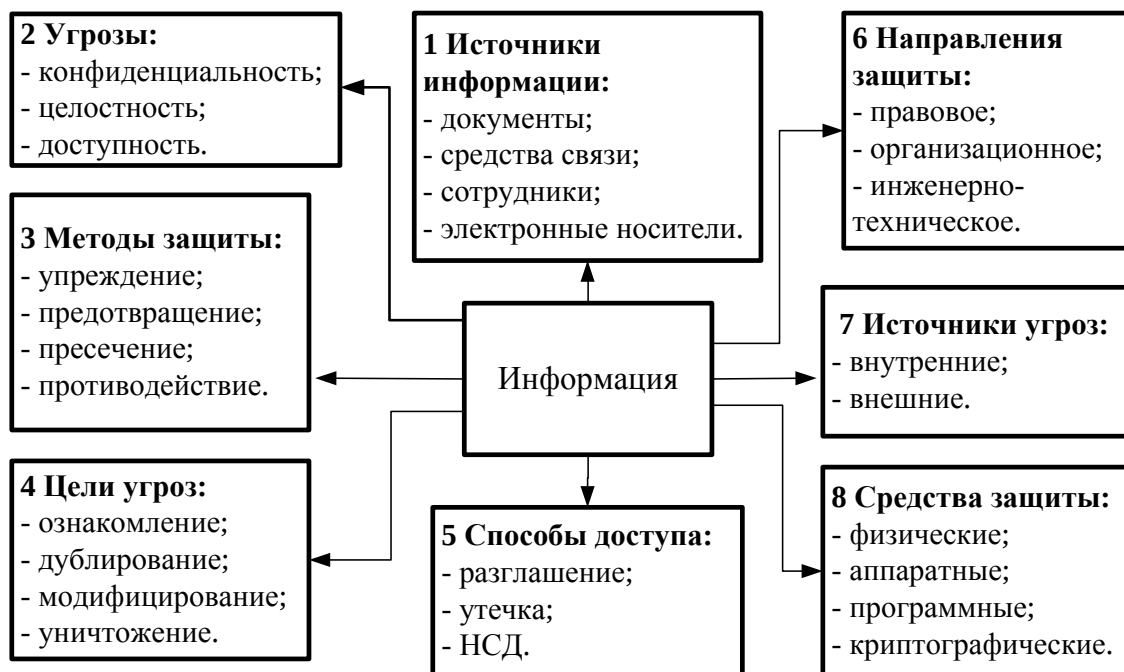


Рисунок 1 - Концептуальная модель информационной безопасности

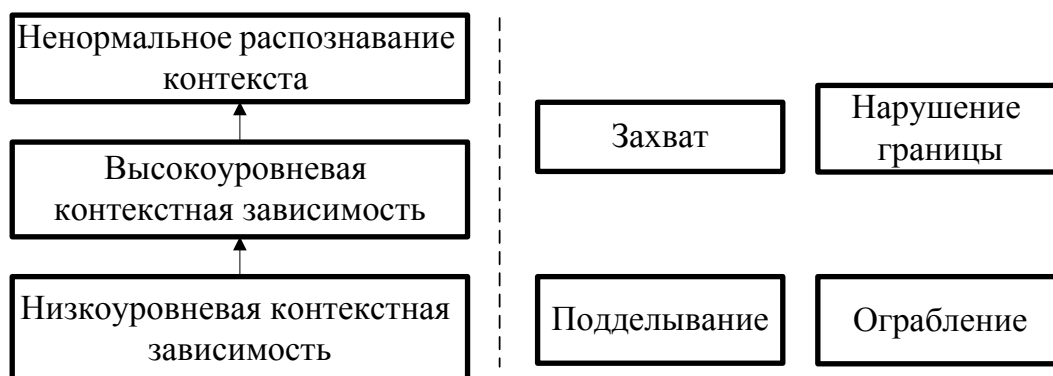


Рисунок 2 - Трехуровневая контекстно-зависимая система видеонаблюдения

На рисунке 3 показана архитектура интеллектуальной видеосистемы наблюдения. Компоненты описывается следующим образом[2]:

1. Инфраструктура считывания. Инфраструктура считывания используется для сбора различных данных от аппаратных устройств разнородного слежения в повсеместной сетевой среде. Данные от слежения инфраструктура передает в контекстный агрегатор и изменяется как предопределенный формат для понимания контекста.

2. База данных контекста. База данных контекста относится к модулю, в котором измененные данные из Context Broker (который используется для будущего понимания контекста) сохраняются. соответствующие данные представлены в виде индекса безопасности и так далее.

3. Context Broker: Context Broker. Сохраняет данные в контекстную базу данных (БД), которая передается из контекстного агрегатора. Данные обрабатываются для использования соответствующего пространства.

4. Менеджер сообщества. Когда событие происходит в определенном месте в соответствии с нашими предопределенными критериями, менеджер дает инструкции своему сервисному контроллеру создать соответствующие службы, которые определены редактором сообщества.

5. Редактор сообщества. Редактор сообщества создает сообщество, которое создает предопределенное событие, которое происходит в нашей зоне мониторинга. Сообщество динамически создается и хранится в хранилище шаблонов сообщества.

6. Service Discoverer и Invocator. Когда происходит событие, менеджер контекста находит соответствующий сервис через сервис Discoverer и, если он существует, Service Invocator выполняет соответствующую услугу, хранящуюся в шаблоне сообщества.

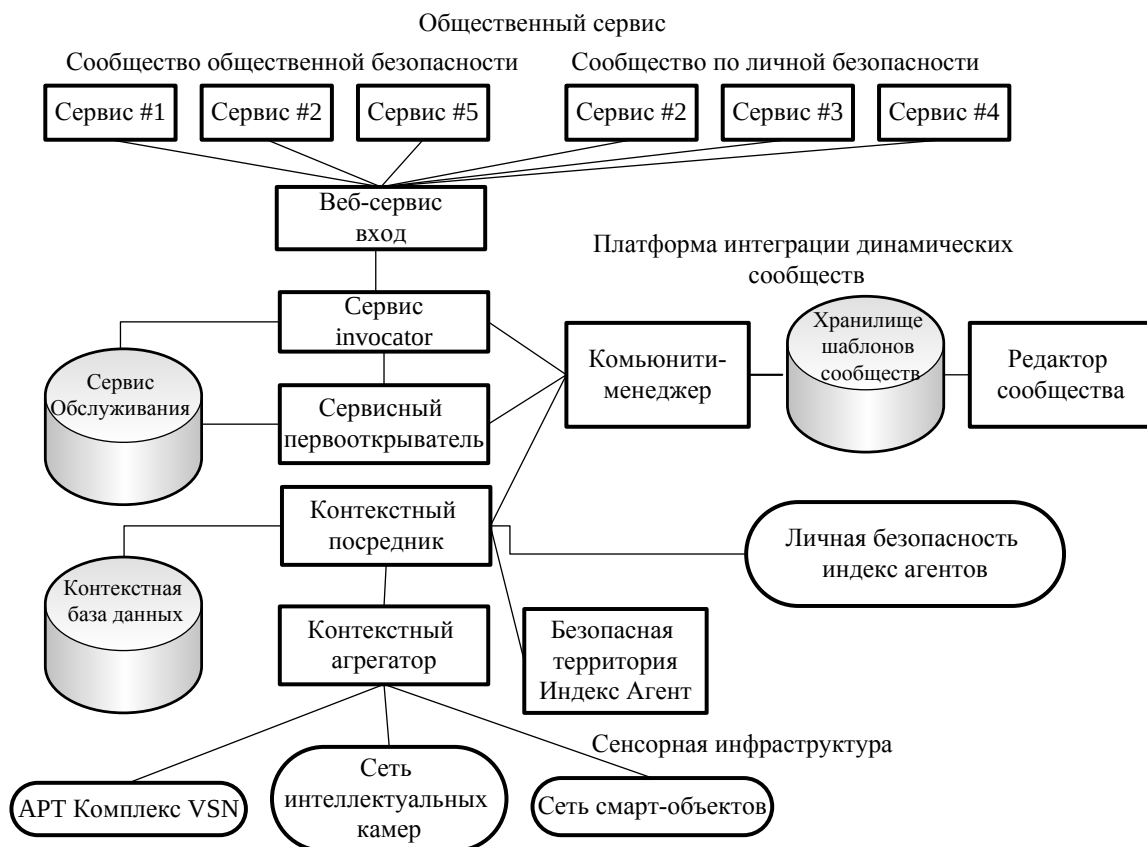


Рисунок 3 - Архитектура системы видеонаблюдения

Когда происходит вмешательство в зоне мониторинга, данные слежения передаются в Context Broker и Context Broker дает команду агенту индекса обновить последнее пространство индекса безопасности в базе данных индексов. Приложение видеокамеры вычисляет свой индекс безопасности пространства в индексной БД. Если вычисленное значение индекса безопасности пространства превышает пороговое значение, оно подает команду видеокамере для мониторинга области с помощью функции PTZ-камеры. Наконец, пользовательский агент отправляет сигнал тревоги - сообщение пользователю путем расчета индекса безопасности[2].

Схема многокамерного слежения применяется для непрерывного захвата видео движение объекта. Поле зрения (FOV) камер видеонаблюдения PTZ автоматически устанавливают сравнение сходства изображений. Фиксированные камеры покрывают область интереса (ROI) и анализируют изображение в реальном времени для представления объектов и их отслеживание в случае аномальной ситуации. Система автоматически отправляет аварийное сообщение системы видеонаблюдения, когда происходит вмешательство или НСД. После получения сообщения система показывает объект и указывает его местоположение в безопасности индекса. Если объект движется в поле зрения фиксированной камера, камера PTZ отслеживает объект с помощью управления PTZ. В противном случае, если объект исчезает из поля зрения фиксированной камеры, наша система

пытается получить объект с помощью автономного метода совместной работы с использованием смежной топологии камеры в неперекрывающаяся зоне.

Основная цель интеллектуальной системы видеонаблюдения заключается в обеспечении события в реальном времени на основе установленных правил. Агенты мониторинга и наблюдения затем получают оповещения в режиме реального времени, позволяющие им реагировать на угрозы и другие важные события активно в их среде. Однако системы наблюдения имеют разные установленные правила событий и правила обмена сообщениями с поставщиками.

Заключение. В этой статье мы предложили интеллектуальную систему наблюдения, которая обеспечивает различные услуги, такие как идентификация объекта, анализ размера объекта, локализация объекта, обнаружение взлома, распознавание активности и отслеживание движущихся объектов. Наблюдение системы имеют разные установленные правила событий и правила обмена сообщениями с поставщиками. Таким образом, мы определили правила для обмена анализируемой информацией между распределенными системами наблюдения или гетерогенными системами наблюдения.

Список литературы

1. Синицын Ю.И. Разработка подсистемы видеонаблюдения для промышленного объекта. Сборник статей Международной научно-практической конференции «Развитие науки и техники: механизм выбора и реализации приоритетов» Часть 3. Уфа: НИЦ АЭТЕРНА, 2017. - С. 138 – 140.

2. Дамьяновски В. А. «ССТV. Библия видеонаблюдения. Цифровые и сетевые технологии»: ООО «Ай-ЭС-ЭС Пресс», 2006. -478 с.

ДИСТРИБУТИВЫ LINUX КАК АЛЬТЕРНАТИВА ОС WINDOWS В ПОДГОТОВКЕ IT-СПЕЦИАЛИСТОВ

**Токарева М.А., канд.техн.наук, доцент, Кулантаева И.А., канд.пед.наук
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Свободное программное обеспечение – это комплексный спектр программных решений, в рамках которых права пользователя юридически защищены авторскими правами на основе свободных лицензий [1]. Впервые термин «свободное программное обеспечение» («free software») ввел программист Ричард Столлман. В этом определении отразились принципы открытой разработки программного обеспечения в научном сообществе, которые сложились в университетах США в 1970-х годах. Переход на свободное программное обеспечение был необходим для сохранности авторства программ и одновременного предоставления возможности для их критики и чтения всем научным сообществом.

Важно отметить, что полноценный переход на свободное программное обеспечение (ПО) возможен не только при использовании соответствующих лицензий, но, и прежде всего, при скоординированном взаимодействии между разработчиками и пользователями. Соответственно, чем больше у свободной программы активных пользователей, корректирующих ее и вносящих существенные дополнения и замечания, тем качественнее идет процесс развития программы. Сегодня такой подход к разработке программы оказывается часто более эффективным, чем традиционные методы, используемые при создании проприетарной программы. Проприетарным является любое программное обеспечение, лицензия на которое содержит условие о выплате правообладателю вознаграждения за предоставляемое по лицензии право использования программы. Проприетарной лицензией является любой возмездный лицензионный договор.

В конце декабря 2010 года Председатель Правительства Российской Федерации В.В. Путин подписал распоряжение о переходе государственных бюджетных организаций, а также органов федеральной исполнительной власти на свободное ПО. В приложении к распоряжению описаны подробности такого перехода и сроки его выполнения. Основой такого пакета свободного ПО является операционная система Linux [2].

Первоначальными движущими факторами, которые обусловили внедрение свободного ПО в госсекторе, являлись экономические преимущества решений на базе свободного ПО, независимость государственных организаций от иностранных поставщиков проприетарного ПО, более широкие возможности контроля и самостоятельного развития программных решений [3].

В настоящее время ПО с открытым исходным кодом широко используется в органах государственного управления и бюджетных организациях во всем мире - как в экономически развитых, так и в развивающихся странах (рисунок 1).

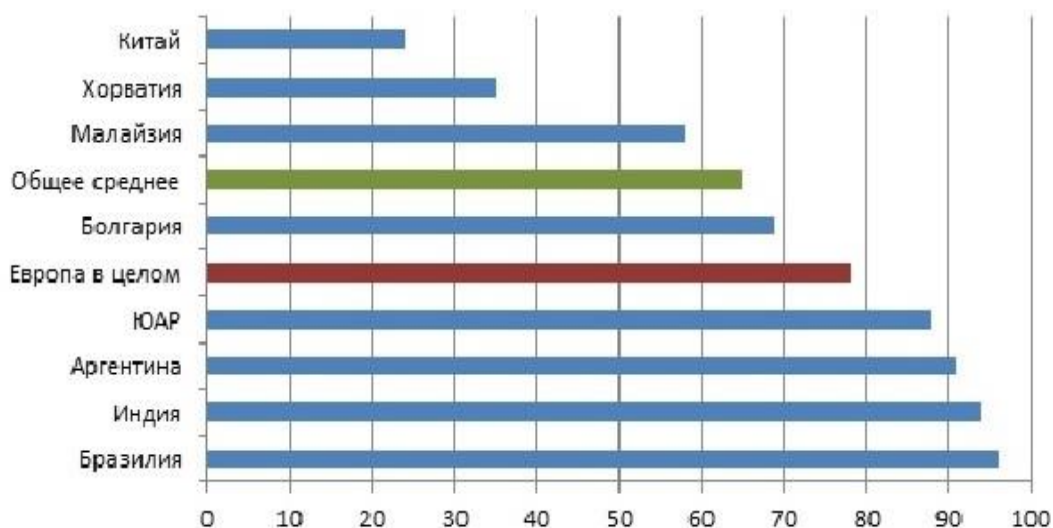


Рисунок 1 - Мировой опыт внедрения СПО

По данным ООН доля использования СПО в крупных компаниях США - 87%, в Латинской Америке более 56%, 72% европейских компаний используют СПО в бизнесе. Из 178 стран-членов ООН 84 страны используют на серверах свободные операционные системы, что составляет 47% от общего числа.

Для общеобразовательных учреждений России в ходе эксперимента по внедрению свободного ПО был разработан дистрибутив ALT Linux 4.0, включающий специально подобранный набор программ образовательного характера. Дистрибутив в составе пакета «Первая помощь 2.0» был разослан по всем школам России и может использоваться бесплатно. В дальнейшем дистрибутив ALT Linux был доработан компанией-производителем, выпущена версия 5.0, доступная для массового использования. Набор программ был несколько изменён, улучшен интерфейс программы [4].

Кроме упомянутых версий школы могут использовать другие дистрибутивы Linux, подавляющее большинство которых распространяются под свободной лицензией GPL.

Linux – это свободно распространяемые операционные системы, которые основаны на ядре Unix. Общее название не подразумевает какой-либо единой «официальной» комплектации Linux; они распространяются в основном бесплатно в виде различных готовых дистрибутивов, имеющих свой набор прикладных программ и уже настроенных под конкретные нужды пользователя. Возникновение Linux связывают с 1991 г., когда молодой финский программист Линус Торвальдс (от его имени и происходит название Linux), начал работу над первой версией системы. Предшественники Linux -

операционные системы семейства UNIX имеют очень давнюю историю (даже операционные системы от Microsoft имеют в своей основе коды и принципы работы, заимствованные от UNIX). Linux обладает всеми свойствами современной Unix-системы, включая настоящую многозадачность, развитую подсистему управления памятью и сетевую подсистему [5,6].

Linux – довольно своеобразная, по сравнению с Windows, операционная система. Чтобы люди, привыкшие к Windows не испытывали трудностей при переходе на Linux разработчики операционной системы и программ для неё, стараются сделать её похожей на Windows. После своего возникновения (и по сей день) Linux начал переживать настоящий расцвет популярности. Связано это в первую очередь с тем, что ядро операционной системы Linux, как и подавляющее большинство написанных под неё программ обладают двумя важными отличительными признаками - это, во-первых, бесплатность, в отличие от Windows, во-вторых - открытость исходного кода, что означает, что каждый мог использовать и модифицировать этот код по своему усмотрению. В настоящее время вокруг Linux сложилось гигантское сообщество программистов, которые постоянно занимаются совершенствованием Linux, разработкой новых версий и разновидностей этой операционной системы, написанием самых разнообразных программ, работающих под Linux [6,7].

В отличие от ядра, дистрибутивы могут содержать коммерческие компоненты, и потому их свободное распространение может быть ограничено. В таком случае авторы дистрибутива делают доступными все свободные компоненты. Обычно под словосочетанием «ОС Linux» понимают дистрибутивы GNU/Linux общего назначения. В настоящее время существуют сотни самых разных дистрибутивов, многие из которых отличаются друг от друга цветом оформления, обоями и комплектом предустановленных программ. Но есть немало самобытных разработок, которые имеют полное право называться самостоятельными операционными системами. Рассмотрим ниже самые распространенные дистрибутивы Linux по версии проекта distrowatch.com, который учитывает выбор людей со всего мира и размещает дистрибутивы Linux по местам их популярности [8].

Конечно, переход системы образования на совершенно новую операционную систему - мера скорее вынужденная, чем необходимая: частное программное обеспечение требует немалых финансовых затрат. Годами создаваемые программные и методические наработки для Windows оказываются невостребованными. Безусловно, это грозит откатом системы информатизации на несколько лет назад.

Самый серьезный негативный аспект перехода на свободное ПО – это отсутствие методической и программной поддержки процесса обучения, поэтому параллельно с реализацией плана перехода необходимо уделять внимание этой проблеме, которая приобретает особую актуальность при подготовке специалистов в области IT-технологий.

Авторами разработана контрольно-обучающая программа по обучению работы с ОС Linux, которая проходит апробацию в изучении дисциплины «Операционные системы, среды, оболочки» для бакалавров общего профиля по направлению подготовки «Информационные системы и технологии».

Исходя из анализа принципов к разработке компьютерных средств обучения, следует, что контрольно – обучающие программы должны обеспечивать расчлененность учебной работы на шаги и завершение каждого шага самопроверкой и возможным корректирующим воздействием. Также имеет значение использование автоматизированной системы управления деятельностью обучающегося, индивидуализация обучения, опосредованное взаимодействие субъектов образовательного процесса, которому отводится большая часть времени работы, и реализация режима апелляции обучающегося, что позволяет восстановить непосредственное его взаимодействие с преподавателем.

При работе с программой после прохождения процедуры регистрации пользователю открывается главная форма, представленная на рисунке 2. На главной форме располагается приветствие и панель с уровнями подготовки. Пользователю предлагается выбрать любой из уровней подготовки, а также ознакомиться с информацией о программном продукте.

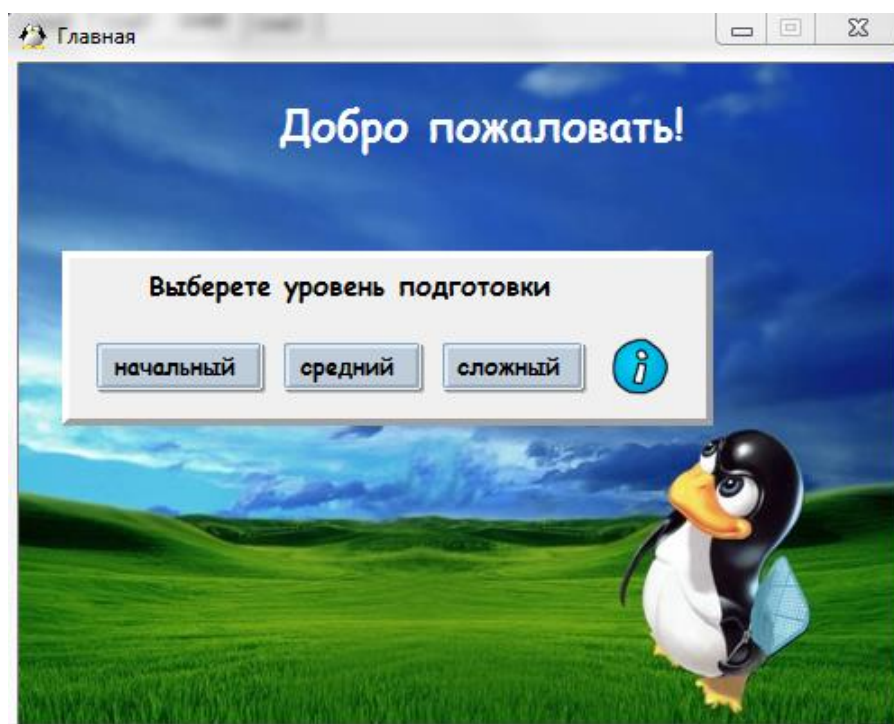


Рисунок 2 – Главная страница

При выборе начального уровня подготовки открывается форма, на которой располагается список тем и панель с кнопками (рисунок 3). При нажатии на кнопку «Пройти тест» пользователю будет предложено пройти тест по начальному уровню. При нажатии на кнопку «На главную»

пользователю предоставится возможность сменить уровень подготовки на главной странице. Теоретический материал в начальном уровне подготовке подобран для пользователя, который совсем не знаком с ОС Linux и никогда не работал с ней. В данный уровень включены основные понятия о Linux, ее дистрибутивах и основных графических интерфейсах. Пример оформления темы «Что такое Linux» представлен на рисунке 4.

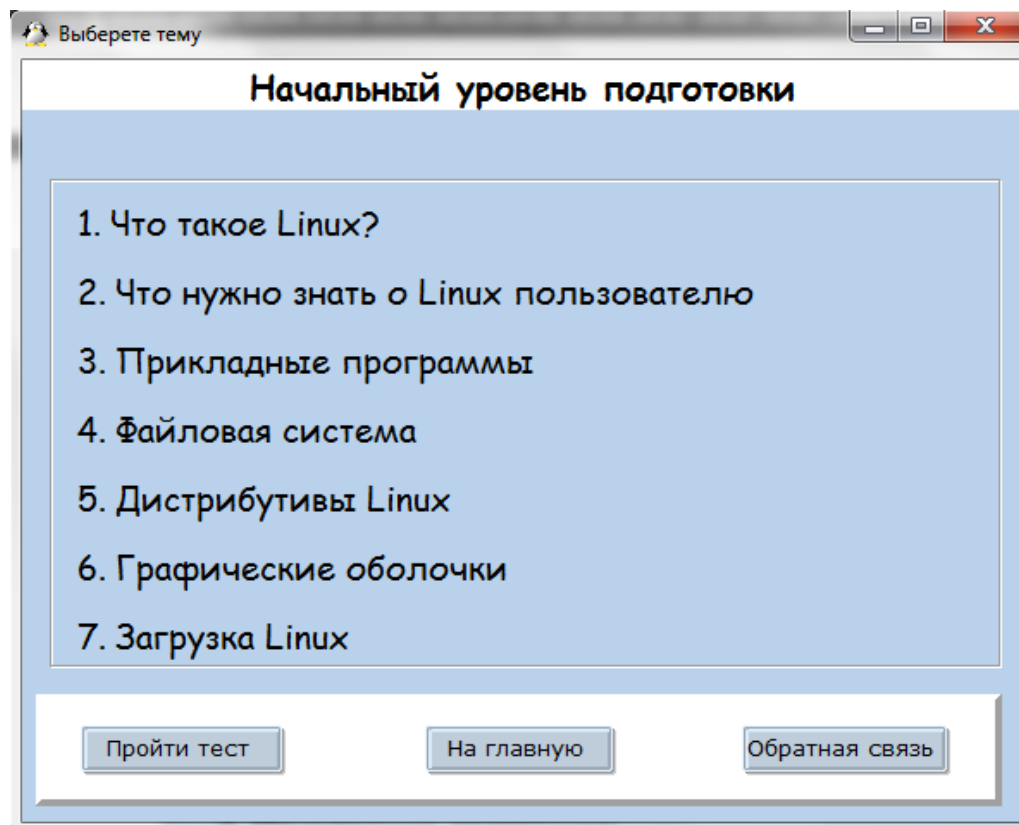


Рисунок 3 – Начальный уровень подготовки

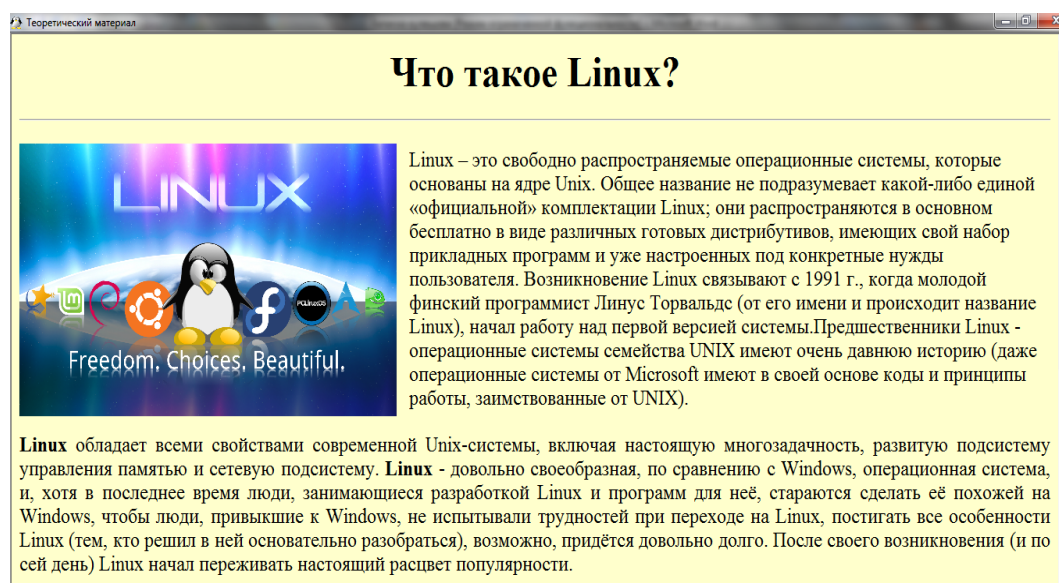


Рисунок 4 – Пример оформления темы

При выборе среднего уровня подготовки открывается такая же форма как и в начальном уровне (рисунок 5). Теоретический материал в среднем уровне подготовки предназначен для пользователей, которые ознакомлены с теоретическими материалами из начального уровня и уже готовы для базовой работы в ОС Linux. Каждая тема содержит как и теоретический материал так и практический по работе в прикладных программах Linux. Каждая тема содержит иллюстрации для наиболее комфортного обучения. На рисунке 6 представлен пример оформления темы «Презентация OpenOffice.org Impress».

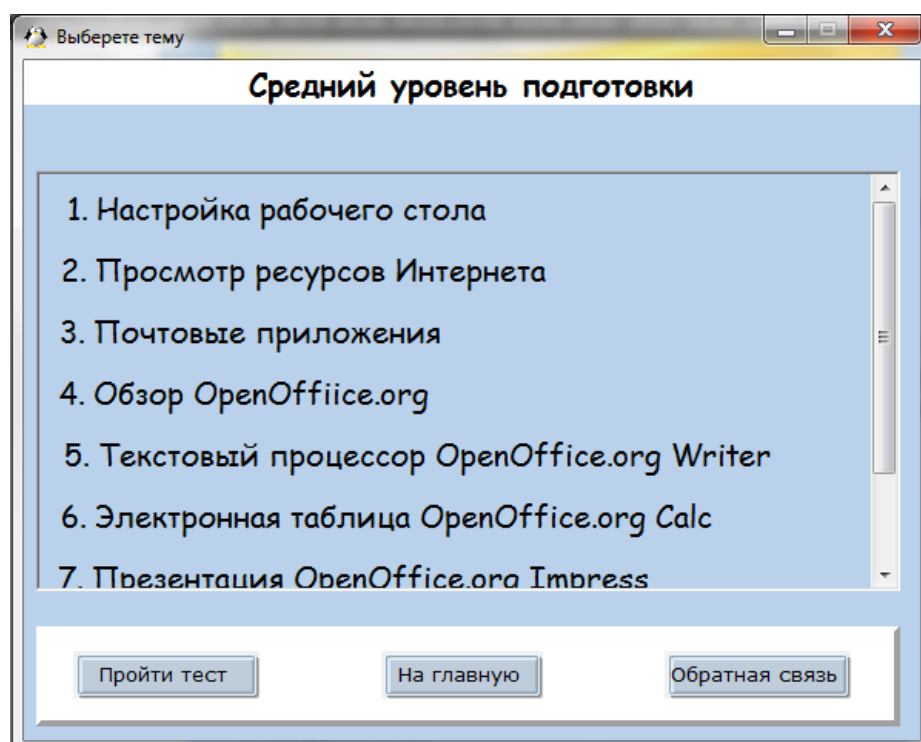


Рисунок 5 – Средний уровень подготовки

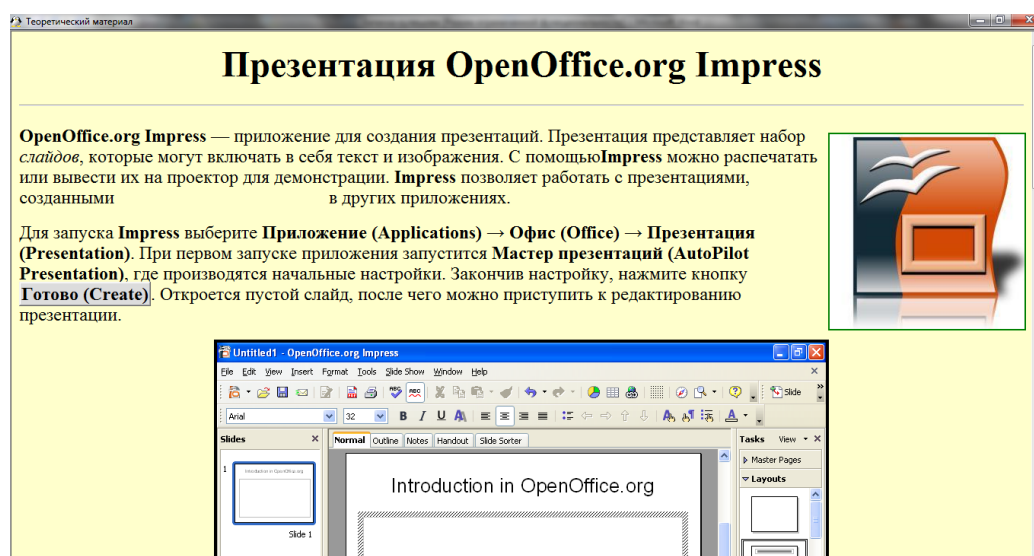


Рисунок 6 – Пример оформления темы

Форма сложного уровня подготовки кроме стандартных элементов содержит кнопку «Пройти итоговый тест» (рисунок 7). Материал сложного уровня подготовки предназначен для более продвинутых пользователей, которые хотят научиться работать с файлами и каталогами напрямую через терминал а также научиться устанавливать прикладные программы и виртуальную машину. Пример оформления темы «Файловая система» представлен на рисунке 8.

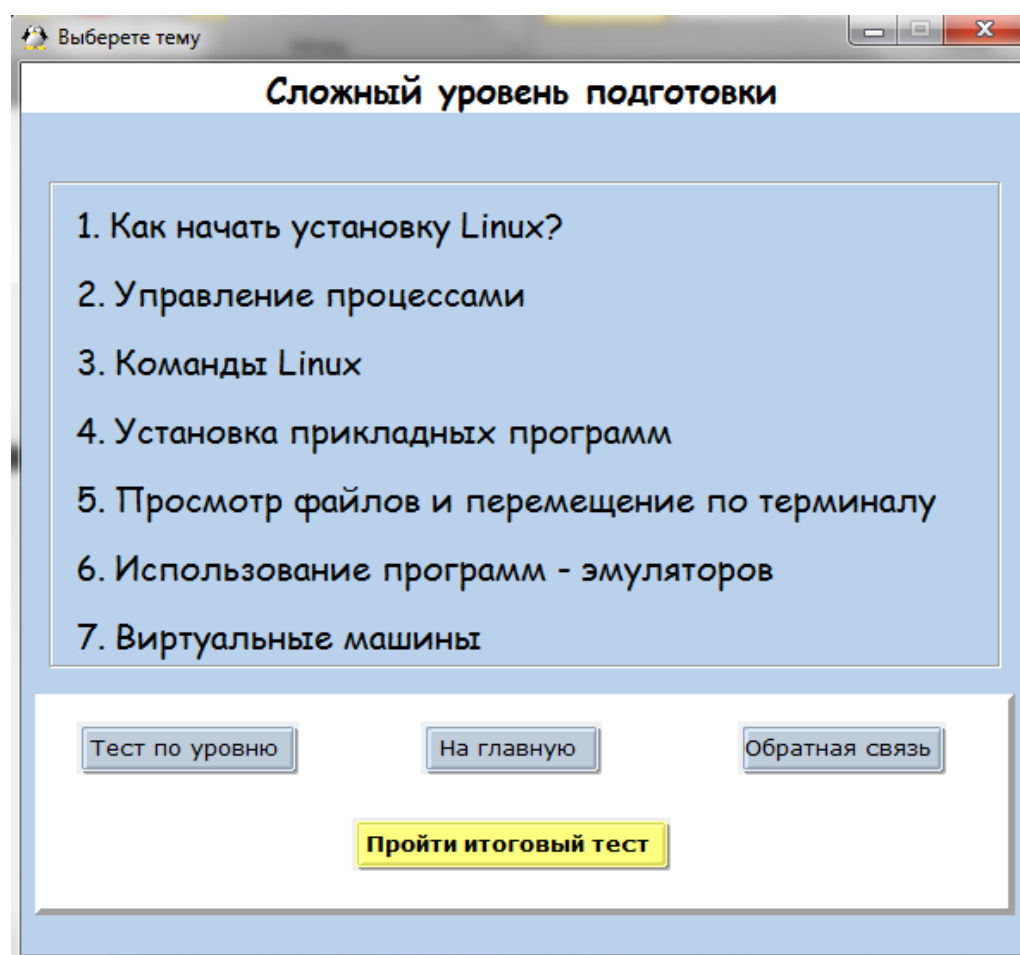


Рисунок 7 – Сложный уровень подготовки

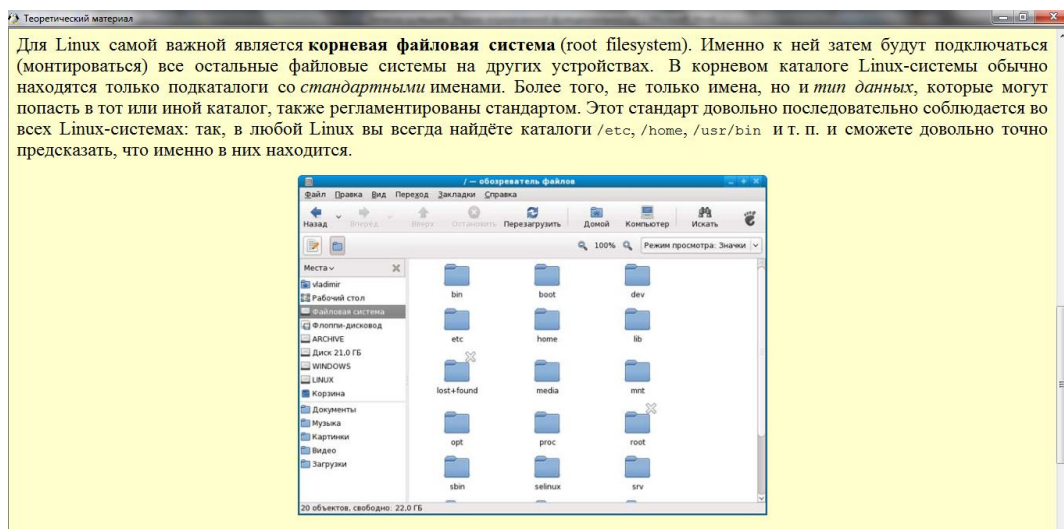


Рисунок 8 – Пример оформления темы

В конце каждой темы имеются вопросы для самопроверки, которые предназначены для усвоения и структуризации полученных знаний (рисунок 9).

Вопросы для самопроверки:

1. При помощи чего хранят данные на диске операционные системы?
2. Что представляет собой классическая файловая система?
3. Как называется в Linux корневой каталог?
4. Что такое монтирование?
5. Что обычно находится в корневом каталоге Linux-системы?

Назад Далее

Рисунок 9 – Вопросы для самопроверки

По изучению теоретического материала обучающемуся необходимо пройти тест по уровню и проверить свои знания. На рисунке 10 представлен тест по начальному уровню:

Тест

Тест по начальному уровню

Кто в 1991 году начал работу над первой версией ОС Linux?

☐ Стив Джобс ☐ Линус Торвальдс
☐ Билл Гейтс ☐ Торвальд Линукс

Linux имеет ... исходный код

☐ Закрытый ☐ Неизменяемый
☐ Открытый ☐ Нет верного ответа

Какую лицензию имеет Linux?

☐ Общедоступную ☐ Полукommerческую
☐ Коммерческую ☐ GNU

Является ли система Linux многопользовательской?

☐ Является

Результат На главную Сменить уровень Теория

Рисунок 10 – Тест по начальному уровню

Какая среда способствует запуску Windows - приложений в Linux?

☐ Microsoft Office
☐ Ubuntu
☐ Linux Mint
☐ Wine

Выберете аналог офисных программ Windows для Linux

☐ Microsoft Office
☐ Ubuntu Lab
☐ Office Wine
☐ Libre Office

Правильных ответов 1 из 7 вопросов
Очень плохой результат! Изучите темы снова, и пройдите тест!

Результат На главную Сменить уровень Теория

Рисунок 11 – Результат теста

Итоговый тест на знание ОС Linux

Вопрос № 1

Что такое сетка в Inkscape?

- ☐ набор пересекающихся штриховых линий
- ☐ набор пересекающихся сплошных линий
- ☐ набор пересекающихся пунктирных линий

Вопрос № 2

Как называется стандартный файл-менеджер среды XFCE?

- ☐ Dolphin
- ☐ Nautilus
- ☐ Thunar
- ☐ Far

Вопрос № 3

Диапазон ячеек в OpenOffice Calc - это:

- ☐ все ячейки одного столбца;
- ☐ множество допустимых значений.
- ☐ все ячейки одной строки
- ☐ две или более ячеек листа, рассматриваемых как единое целое

Рисунок 12 – Итоговый тест

При неудачном результате тестирования (рисунок 11) переход на следующий уровень блокируется и обучающемуся предлагается снова изучить теоретический материал. При настойчивом желании пользователя перейти на другой уровень, программа предлагает ответить на дополнительные вопросы.

На рисунке 12 представлен фрагмент итогового теста, который проходится после изучения всего теоретического материала на всех уровнях подготовки. Он включает в себя 25 вопросов, представленных в разной форме.

Структура данной программы включает в себя блок обучения, блок контроля, и блок информации и литературы. Весь теоретический материал, представленный в блоке обучения, соответствует принципам и требованиям положенными в основу компьютерных средств обучения. Программа обладает гибким алгоритмом управления, непрерывным и разноуровневым контролем обучения (пошаговым, рубежным, итоговым). Все данные о пользователе, в том числе и результаты тестирований, сохраняются, тем самым позволяя отслеживать собственные достижения.

Контрольно – обучающая программа создана при помощи инструментов Delphi и FrontPage, представляет собой продукт, который помогает пользователю легко ориентироваться, найти нужную информацию, глубоко изучить материал, ознакомиться подробно с интересующими или

необходимыми темами. Представленный материал позволяет наглядно продемонстрировать теоретическую и практическую информацию во всем ее многообразии и системности, что способствует формированию профессиональных компетенций по дисциплине.

Список литературы

1 Андропова, Е.В. Информационные технологии на базе свободного программного обеспечения: учеб. пособие / Е.В Андропова, М.А Губин, Т.Н. Губина. – Елец: ЕГУ, 2008.

2 О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения (2011–2015 годы) [Электронный ресурс]: распоряжение Правительства Российской Федерации от 17 декабря 2010 г. №2299-р// КонсультантПлюс: справочная правовая система / разраб. НПО «Вычисл. математика и информатика». – Москва: Консультант Плюс. – Режим доступа: <http://www.consultant.ru>.

3 Черный, В.Л. Апробация Пакета Свободного Программного Обеспечения (ПСПО) в учебных заведениях РФ. Итоги и перспективы / В.Л. Черный // Третья конференция «Свободное программное обеспечение», Переславль, 2–3 февраля 2008 г. – М., ALT Linux: 2008.

4 Отставнов, М. Прикладные свободные программы и системы в школе/ М. Отставнов. - М.: Институт Логики, ALT Linux Team, 2003.

5 Кирх, О. LINUX для профессионалов. Руководство администратора сети / О. Кирх. - М.: СПб: Питер, 2009. - 368 с.

6 Колисниченко, Д.Н. Linux. Полное руководство / Д.Н. Колисниченко, Питер В.. - М.: СПб: Наука и Техника, 2007. - 784 с.

7 Валади, Дж. 100% самоучитель Linux / Дж. Валади. - М.: Технолоджи-3000, 2015. - 336 с.

8 Рассел, Дж. Список дистрибутивов Linux / Джесси Рассел. - М.: Книга по Требованию, 2012. - 100 с.

РАЗРАБОТКА ЭЛЕКТРОННОГО УЧЕБНОГО ПОСОБИЯ «ТЕХНИЧЕСКИЕ СРЕДСТВА РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ»

**Токарева М.А., канд. техн. наук, доцент, Тлегенова Т.Е., канд. пед. наук
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Оренбургский государственный университет»**

Компьютерные технологии проникли практически во все области человеческой деятельности. Одним из наиболее перспективных направлений применения компьютерных технологий является их внедрение в учебный процесс, что в настоящее время становится стандартом образования.

Проблема широкого применения компьютерных технологий в сфере образования в последнее десятилетие вызывает повышенный интерес в отечественной педагогической науке. Большой вклад в решение проблем внедрения компьютерных технологий в образование внесли российские и зарубежные ученые Агапова О.И., Громов Г.Р., Шолохович В.Ф., Гриценко В.И., Красильникова В.А., Кривошеев О.А., Клейман Г., Пейперт С., Сендов Б., Хантер Б. и др.

Современный уровень развития технического и программного обеспечения предоставляет широкие возможности в использовании компьютеров в сфере образования. В связи с этим, современный учебный процесс сложно представить без использования компьютерных учебников, задачников, тренажеров, лабораторных практикумов, справочников, энциклопедий, тестирующих и контролирующих систем и других компьютерных средств обучения.

Электронные учебники и электронные пособия позволяют индивидуализировать и дифференцировать процесс обучения, осуществлять контроль с диагностикой ошибок и обратной связью, осуществлять самоконтроль и самокоррекцию учебной деятельности, формировать умение принимать оптимальное решение в различных ситуациях, развивать определенный тип мышления (наглядно-образный, теоретический), усиливать мотивацию обучения, формировать культуру познавательной деятельности. Они помогают обеспечить каждому пользователю выбор, создание и реализацию индивидуальной траектории получения образования и приобретения навыков и умений [1].

В данной работе представлено разработанное электронное учебное пособие по одной из традиционных тем курса информатики в вузе – раздел «Технические средства реализации информационных процессов».

В настоящее время данная тема сохраняет свое значение как весьма актуальная для понимания процессов сбора, хранения, обработки и передачи информации, а также в связи с широким использованием компьютера для выполнения различных видов работы с информацией. Изучая данный раздел,

студенты должны осознать, что компьютер является мощным инструментом специалиста, что знания технических средств для обработки информации позволит им быть конкурентоспособными на современном рынке труда, компетентными и свободно владеющими современными информационными технологиями.

Однако, проанализировав ряд рабочих программ [2-4] в традиционном курсе информатики в вузе уделяется, на наш взгляд, недостаточное внимание вопросам изучения особенностей технического обеспечения информационных систем, архитектуры персонального компьютера, основных и периферийных устройствах ЭВМ, отводя на данный раздел самое большое 4 часа аудиторного времени.

В связи с этим в условиях сокращения аудиторного времени на освоение образовательной программы подготовки бакалавриата традиционные подходы к организации учебного процесса не обеспечивают в полной мере формирование профессиональной компетентности выпускников вуза, как результат - неполное знание материала, его недостаточное понимание студентами.

Решить эту проблему способна методика, основанная на использовании современных форм обучения в частности компьютерная поддержка в виде электронного учебного пособия. Раздел «Технические средства реализации информационных процессов» рассматривается на примере дисциплины «Информатика».

Цель учебного пособия – дать обучающимся представление об особенностях технического обеспечения информационных систем, архитектуре персонального компьютера, основных и периферийных устройствах ЭВМ, сформировать у них умения и навыки работы с компьютером как средством управления информацией при решении задач профессиональной деятельности.

Для эффективной работы с электронным учебным пособием необходима правильная организация структуры излагаемого материала. Правильный выбор структуры может облегчить взаимодействие пользователя с информацией.

Материал пособия подобран таким образом, чтобы сформировать у обучающихся “фундамент” знаний и умений по принципам функционирования и организации данных в ЭВМ, что позволит им в дальнейшем использовать их при работе с персональным компьютером, в выборе технических средств для обработки данных в соответствии с поставленной задачей. Электронное учебное пособие «Технические средства реализации информационных процессов» охватывает темы полного лекционного курса по изучению организации информационных процессов в компьютере.

Структура электронного пособия приведена на рисунке 1, имеет блочно-модульную модель представления учебного материала и выглядит следующим образом:

1. Теория
2. Практика
3. Контроль знаний
4. Справка

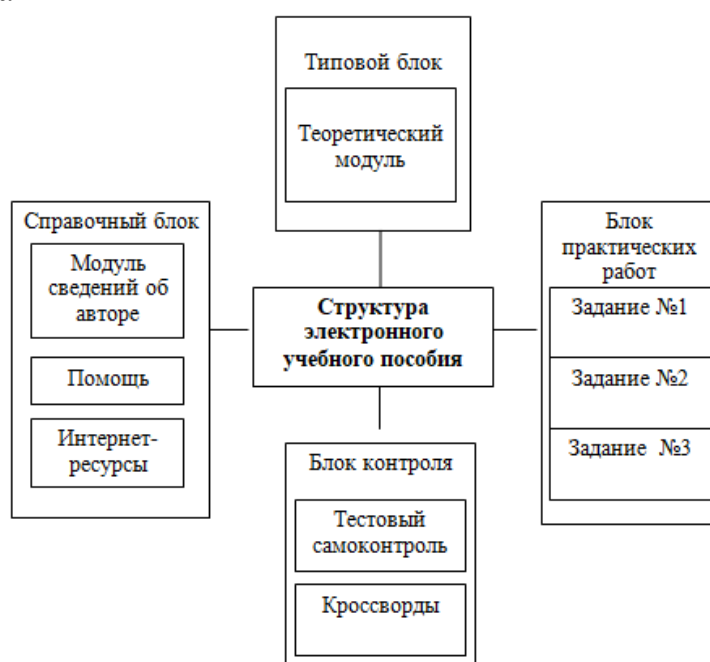


Рисунок 1 – Схематическое отображение структуры электронного пособия

В теоретическом блоке рассматриваются основные разделы теоретической информатики: устройства персонального компьютера, организация информационных процессов в ЭВМ, архитектурные принципы устройства ЭВМ, внутренние устройства ЭВМ, внешние устройства ЭВМ.

В блок 1 входят четыре главы:

В главе 1 «Организация информационных процессов в ЭВМ» описываются процессы сбора, обработки, накопления, хранения, поиска и распространения информации, взаимосвязь данных информационных процессов.

В главе 2 «Архитектурные принципы устройства ЭВМ» рассматривается классическая структура и принципы работы ЭВМ, основные блоки ЭВМ, принципы организации вычислительной системы, состав, порядок и взаимодействие основных частей ЭВМ, их функциональные возможности.

Глава 3 «Внутренние устройства ЭВМ» описывает основные аппаратные компоненты компьютера (системная плата, процессор, оперативная память, слоты для установки контроллеров внешних устройств), а также устройства непосредственно взаимодействующие с процессором и предназначенные для хранения выполняемых программ и данных, непосредственно участвующих в вычислениях.

Глава 4 «Внешние устройства ЭВМ» посвящена устройствам, посредством которых можно ввести информацию в компьютер и вывести ее в

необходимом для оператора формате, также описываются внешние запоминающие устройства – магнитного, оптического, магнитооптического и электронного принципа действия.

Практический блок посвящен практическому изучению устройства персонального компьютера. Представляет собой виртуальные лабораторные работы, которые позволят лучше узнать изучаемый объект, в процессе работы с ним. Для закрепления понятийного аппарата студенты могут выполнять серии тренировочных заданий, решают учебные задачи. Каждый компонент этого раздела может использоваться самостоятельно.

Блок контроля включает вопросы для проверки знаний обучающихся в виде тестирования и решения кроссворда (рисунок 2), позволяющие оценить знания студентов на следующих уровнях (степенях):

1. понятийная ступень (термины, понятия, определения, правила, законы);
2. репродуктивная ступень (типовые ситуации, применение определенных правил в типовых ситуациях, принятие решений по шаблону и образцу);
3. творческая ступень (применение усвоенных знаний в комплексе, межпредметные связи; самостоятельный выбор подхода к решению из спектра изученных, выстраивание по этапам нестандартного решения).



Рисунок 2 – Пример интерактивного кроссворда

В справочном блоке содержатся общие рекомендации работы с электронным учебным пособием, информация об авторе, о минимальных технических требованиях к компьютеру, ссылки на интернет-ресурсы.

Также в электронном учебном пособии «Технические средства реализации информационных процессов» используются модели с анимированными сюжетами, с целью повышения интереса обучающихся, наглядного отображения работы устройства. В моделях с анимированными сюжетами, как правило, предлагается несколько кадров, в ряде случаев сюжеты можно просматривать в увеличенном или уменьшенном вариантах.

Многие явления в условиях компьютерной аудитории не могут быть продемонстрированы. В результате обучающиеся испытывают трудности в их изучении. Электронный учебник с обучающими фрагментами и практическими заданиями, созданными при помощи Flash, помогает не только создать модель таких явлений и показать, как работает то или иное устройство но также позволяет изменять условия протекания процесса в устройстве (рисунок 3).



Рисунок 3 – Пример практического задания с анимированным сюжетом

К несомненным преимуществам электронного учебного пособия можно отнести:

- предоставляет возможность выбора индивидуального темпа обучения и самостоятельного маршрута обучения;
- теоретический материал разбит по главам, весь объем материала в учебном пособии представлен компактно;
- учебное пособие содержит анимационные видеоролики, иллюстративные средства наглядности, фрагменты анимированных примеров, гиперссылки, позволяющие быстро находить требуемую информацию;
- для закрепления пройденного материала, выработки умений и навыков разработан комплекс творческих практических и тренировочных заданий с анимированными интерактивными сюжетами;
- по окончании изучения каждой главы представлены вопросы для проверки знаний обучающихся в виде тестирования и решения кроссворда;
- в учебном пособии имеется удобная система навигации;
- учебное пособие работает в режиме off-line.

Таким образом, разработанное электронное учебное пособие «Технические средства реализации информационных процессов» может использоваться в качестве иллюстративного материала, как самостоятельный продукт, так и в качестве электронного средства обучения для проведения

лекционных, лабораторных и практических занятий у студентов различных направлений подготовки по изучению раздела «Технические средства реализации информационных процессов» в курсе информатики. Пособие может быть использовано как дополнительное учебное пособие в традиционном учебном процессе, так и в качестве специального курса или для самостоятельной работы.

Список литературы

1. Красильникова, В. А. Теория и технология компьютерного обучения и тестирования: монография / В. А. Красильникова. – Москва: Дом педагогики, 2009. – 339 с.
2. Рабочая программа дисциплины «Б1.Д.Б.11 Информатика» [Электронный ресурс]: Официальный сайт / Оренбургский государственный университет. URL: <http://www.osu.ru/doc/4577/prof/4412/lvl/3/year/2019/> (дата обращения: 30.12.2019)
3. Рабочая программа дисциплины «Б1.Д.Б.12 Информатика» [Электронный ресурс]: Официальный сайт / Оренбургский государственный университет. URL: <http://www.osu.ru/doc/4577/prof/4528/lvl/3/year/2019/> (дата обращения: 30.12.2019)
4. Рабочая программа дисциплины «Б1.Д.Б.14 Информатика» [Электронный ресурс]: Официальный сайт / Оренбургский государственный университет. URL: <http://www.osu.ru/doc/4577/prof/4783/lvl/3/year/2019/> (дата обращения: 30.12.2019)

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕТОДОВ СТЕГОАНАЛИЗА ГРАФИЧЕСКИХ ФАЙЛОВ

Шухман А.Е.¹, канд.пед.наук, доцент, Шухман Е.В.², канд.физ.-мат.наук

¹Оренбургский государственный университет,

²Оренбургский государственный педагогический университет.

Стремительное развитие компьютерных технологий приводит к тому, что огромное количество информации, составляющей интеллектуальную собственность или государственную тайну, хранится и обрабатывается в цифровой форме и передается с помощью локальных или глобальных компьютерных сетей. В этой связи возникают проблемы защиты государственной и коммерческой тайны от несанкционированного доступа, предотвращения военного и государственного шпионажа, киберпреступлений.

Наиболее эффективно секретность компьютерных сообщений обеспечивают методы криптографии и стеганографии. Криптографическая защита предполагает изменение информации за счет ее шифрования. Доступ к исходным данным имеют лишь лица, имеющие ключи для дешифровки. Тем, кто несет ответственность за безопасность компаний и учреждений, не требуется скрывать свои коммуникации. Чтобы обеспечивать их безопасность, достаточно криптографии, так как значительные успехи в области разработки криптографических методов позволяют сегодня обеспечивать высокий уровень секретности передаваемой информации. Но, злоумышленник, передающий секретные сообщения в таком виде, рискует привлечь к себе внимание специальных служб.

Повысить степень секретности он может путем дополнительного использования стеганографических методов [1]. Суть компьютерных стенографических методов состоит в том, что секретное сообщение встраивается в некий объект-контейнер, не привлекающий внимание (им может быть текстовый, графический, аудио- или медийный файл), и открыто передается адресату. В этом случае, стандартными средствами защиты информации практически невозможно обнаружить факт утечки данных, или переписку преступных элементов.

Таким образом, среди пересылаемых потоков данных в сети Интернет могут присутствовать нежелательные и даже опасные: например, коммуникации между террористами и преступниками, экстремистские материалы, вредоносные программы. На повестку дня выходит проблема обнаружения в огромном цифровом потоке тех файлов, которые на первый взгляд не вызывают никаких подозрений, а на самом деле скрывают враждебную информацию в засекреченной форме.

В связи с этим большую актуальность приобретает стегоанализ [2]. Основная задача стеганоанализа – установление факта присутствия в контейнере скрытой информации. Несмотря на широкое распространение стеганографических программ, не существует качественных инструментов

стегонализа, которые позволяют автоматизировать процесс обнаружения скрытой информации в изображениях, видео, аудио, текстах и пр. Эффективность автоматических методов стегоанализа до сих пор плохо изучена, при реализации стегоаналитических приложений возникает проблема выбора метода анализа.

Для поиска эффективных методов обнаружения стегосообщений, необходимо изучить методы создания стегообъектов, а они напрямую зависят от типа файла-контейнера (в нашей работе мы ограничимся графическими файлами), целей сокрытия информации и структуры контейнера.

В соответствии с тем, какая область в структуре контейнера подлежит модификации, различают форматные и неформатные стегометоды. Использование первых ограничено невысокой стеганографической стойкостью при довольно низкой пропускной способности и более целесообразно для организации цифровых водяных знаков. Второе направление оказалось более перспективным и базируется на модификации параметров пространства сокрытия файла, характеризующих непосредственно данные самого изображения.

Самым распространенным методом стеганографического сокрытия на сегодня является метод замены наименее значимых бит (LSB — Least Significant Bit метод) [1]. Цифровые изображения представляют из себя массив пикселей. Младшие значащие биты (LSB) каждого пикселя изображения несут в себе меньше всего информации, так как человеческий глаз обычно не способен заметить изменения в этих битах. Чтобы скрыть сообщение в изображении, используют от одного до четырех младших битов. Среди этих бит и распределяют коды символов стегосообщения. Метод применим к растровым изображениям (файлам формата BMP, PNG), представленным в формате без компрессии. При простоте реализации этот метод позволяет достигать огромной пропускной способности, поэтому большинство free- и shareware стеганографических продуктов реализуют именно метод LSB. Это обстоятельство, в свою очередь, определяет актуальность разработки методов его анализа для практического применения.

Эффективность и простота прямого метода замены младших бит привлекает ученых к созданию модификаций данного метода [3]. Для встраивания секретного сообщения их разработчики используют не все подряд пиксели изображения, а выделяют определенные последовательности точек, отвечающие некоторым математическим закономерностям, при этом сохраняя распределение битов из исходного файла. Исследования показывают, что незначительные изменения в исходном алгоритме LSB значительно затрудняют процесс обнаружения скрытого сообщения.

Например, большую популярность приобретает метод, который называют ± 1 встраиванием, или выравниванием младших бит (LSB-matching) [1]. Этот алгоритм случайно меняет значения элементов контейнера (пикселей) с помощью операции ± 1 так, что их младшие биты приводятся в соответствие с битами сообщения. Несмотря на то, что такой алгоритм

достаточно схож с обычной заменой младших битов, его оказывается труднее обнаружить. Но метод ± 1 имеет недостаток, который заключается в независимости вносимого шума. Не менее известен на современном этапе метод HUGO, который можно назвать модификацией метода ± 1 встраивания. Главный принцип его построения заключается в минимизации определенных искажений при встраивании с помощью специальной функции так, чтобы вносимые изменения происходили с вероятностью, обратно пропорциональной возможности обнаружить эти изменения. Алгоритм использует алгебраические методы выделения используемых областей, тесно связанные с методами построения корректирующих кодов.

Разработано большое число различных методов стегоанализа для обнаружения скрытых сообщений в графических файлах [2]. Отметим, что в отличие от криптоанализа, когда метод шифрования предполагается заранее известным, а неизвестен только секретный ключ, стегоанализ обычно не предполагает знания исходного изображения, использованного стеганографического алгоритма, алгоритма шифрования, ключа и длины сообщения. Наиболее интересны универсальные методы стегоанализа, которые работают с любыми стеганографическими алгоритмами. К таким универсальным методам относят визуальные и статистические методы.

Визуальные методы основаны на способности человека сравнивать изображения и выделять отличия в сопоставляемых образах. О наличии скрытой информации могут сигнализировать незначительные искажения в изображении, однако такие искажения могут появиться и в результате сжатия с потерями, используемого в популярном формате JPEG.

Для обнаружения сообщения, внедренного с помощью замены наименее значимых бит, может использоваться визуальный анализ битовых срезов. Основная идея метода заключается в сравнении изображения в целом с изображениями его битовых срезов. Для каждого из трех составляющих цветов – красного, зеленого и синего, первый срез – это изображение, построенное самыми младшими битами, второй срез – изображение, построенное вторыми битами и т.д. Если скрываемая информация записывается в подряд идущие пиксели, то на изображении битовых срезов, соответствующих младшим битам, область, включающая скрытое сообщение, будет выглядеть как равномерно зашумленная. В то же время, остальная часть изображения будет повторять особенности целого изображения, то есть граница между заполненной и пустой частями контейнера будет отчетливо видна.

Статистические методы стегоанализа пытаются обнаружить отличие исследуемого изображения от «естественного», которое не включает скрытых сообщений. Так метод оценки частот появления k -битовых серий оценивает частоту появления различных вариантов k -битовых последовательностей в младших битах цветов пикселей в исследуемом изображении. Например, для $k=2$ анализируется количество пар соседних битов (00, 01, 10, 11), для $k=3$ – троек (000, 001, 010, 011, 100, 101, 110, 111). Для обычных изображений

существует значимая разница между частотами разных последовательностей, при скрывании информации значения частот становятся близкими. Этот метод позволяет выявить скрытое сообщение только при заполнении контейнера не менее чем на 60%.

Для обнаружения скрытых данных при меньшем заполнении контейнер можно использовать анализ распределения пар значений на основе критерия χ^2 (Хи-квадрат), который предложили А. Пфитцман и А. Вестфелд в 2000 году [4]. Идея метода состоит в том, что в исходных изображениях младшие биты цветов пикселей не являются случайными. Это означает, что количества пикселей со значениями, отличающимися на единицу, обычно сильно отличаются. Наоборот, если количество пикселей, имеющих цвет N , примерно совпадает с количеством пикселей, имеющих цвет $N+1$, для каждого N , то скорее всего изображение содержит встроенное сообщение. Метод Хи-квадрат позволяет количественно оценить вероятность внедрения сообщения на основе вычисления близости значений частот четных и нечетных элементов изображения.

Отметим, что результаты метода Хи-квадрат зависят от способа скрывания данных. При последовательной записи данных в наименьшие значащие биты элементов контейнера метод обеспечивает хорошие результаты, а при псевдослучайном выборе элементов для хранения, равномерно распределенных по всей длине изображения, метод не срабатывает. Существуют модификации Хи-квадрат, например, применение его для блоков изображения определенного размера. Если выбирается блок сравнительно небольшого размера, то вероятность ложного обнаружения возрастает, и наоборот, при увеличении длин блоков вероятность ложных обнаружений падает, а вместе с ней падает и вероятность правильного обнаружения. На сегодняшний день пока не разработан критерий, позволяющего оптимальным образом выбирать размеры блоков.

Эффективно обнаружить сообщение, внедренное с помощью псевдослучайных последовательностей, помогает регулярный сингулярный (Regular-Singular, RS) анализ, который разработали Дж. Фридрих, М. Гольян и Р. Ду в 2001 г [5].

Метод основан на разделении изображения на связанные группы G из n пикселей. Для каждой группы определяется функция гладкости $f(G)$ – сумма разностей соседних пикселей в группе. Чем шумнее группа, тем больше будет значение функции гладкости.

Далее вводится функция флиппинга F , такая что $F(F(x)) = x$. При данном анализе используют три функции флиппинга: F_1 - инверсия младшего бита, F_0 – тождественная функция $F_0(x) = x$, F_{-1} - прибавление единицы.

Для каждого пикселя из группы G применяется одна из трех функций флиппинга, вектор из номеров этих функций образует маску M . Лучшие результаты будут, если маска будет симметричной из номеров 0,1. Например для четырех пикселей: 1,0,0,1. Все группы G делятся на три вида: регулярные (обычные), для которых $F(G)$ имеет гладкость выше, чем G , сингулярные

(единичные), для которых $F(G)$ имеет гладкость ниже, чем G , а также неиспользуемые, для которых гладкость не меняется. Для маски M можно посчитать число регулярных и сингулярных групп. То же самое можно сделать для инвертированной маски. Установлено, что для обычных изображений инвертирование маски почти не меняет число регулярных и сингулярных групп. Если же в изображение скрыта информация, то инвертирование маски изменит число групп, при этом метод RS анализа позволяет оценить объем внедренного сообщения.

Также высокой эффективностью обладает метод анализа простых пар (Sample Pair Analysis, SPA), предложенный в 2003 году Ву. Думитреску и Вангом [6]. Этот метод является обобщением RS-анализа, но работает значительно быстрее.

Для экспериментального изучения стегоанализа была выбрана программа StegMachine [7], написанная на языке Python, которая позволяет анализировать файлы в форматах BMP, PNG и JPG в следующих режимах:

1. visual - визуальный анализ битовых срезов, с указанием количества младших битов, выбранного для исследования;
2. chi – метод Хи-квадрат;
3. rs – метод RS анализа;
4. spa – метод SPA анализа простых пар.

Одной из первых задач стегоанализа изображений формата BMP является выбор серии незаполненных контейнеров для последующего автоматического тестирования различных стеганографических программных продуктов. Выборка должна быть представительной, т.е. содержать множество файлов с различными параметрами. Обычно оцениваются такие параметры как размеры изображения, наличие "естественных шумов" (более "шумные" естественные природные изображения, полученные с цифрового фотоаппарата или сканера по сравнению с менее "шумными" искусственными картинками, созданными в графических редакторах), количество цветов и т.д.

Для исследования было отобрано 80 изображений: вместе с фотографиями наполненными яркими красками, отбирались изображения с преобладанием пастельных тонов; обрабатывались фото отличающиеся по сюжету (пейзаж, цветы, портретные фото, праздничные концерты, бытовые сцены), яркости, четкость изображений по диапазону цветов, присутствующих в палитре. Исходные изображения имели максимальное разрешение 5760×3840 . Для дальнейшей работы эти изображения были сохранены в среднем разрешении 1024×683 и низком разрешении 500×333 . Таким образом, было получено 240 контейнеров. В качестве секретного сообщения был использован текстовый файл на русском языке размером 64396 байт. Для файлов с низким разрешением размер скрываемого файла оказался слишком высоким, поэтому для них применялся усеченный вариант текста размером 43055 байтов.

Для подготовки стегоконтейнеров использовались программы QuickStego, Xiao Steganography и OpenPuff. Для каждого файла-контейнера

было выполнено внедрение текста каждой из выбранных программ, после чего проводилась проверка корректности извлечения скрытой информации с помощью тех же программ.

Исходя из объема текстового сообщения и разрешения отобранных изображений, был рассчитан процент заполнения контейнеров для высокого, среднего и низкого разрешения графических файлов.

Для высокого разрешения количество пикселей изображения составляет $5760 \times 3840 = 22118400$. Каждый пиксел содержит три байта цвета, из которых по одному младшему биту может быть использовано для внедрения текста. Всего полезная емкость контейнера составляет $22118400 \times 3 = 66355200$ бит. Объем внедряемого текста составляет $64396 \times 8 = 515168$ бит, таким образом процент заполнения контейнера будет равен $\frac{515168}{66355200} = 0,0078 = 0,78\%$.

Аналогичные подсчеты для среднего и низкого разрешения дают следующие результаты: 24,6% и 68,9%.

Для оценки скорости стегоаналитических методов программа StegMachine запускалась в режимах chi, rs и spa для каждого файла. Среднее время обработки приведено в таблице 1.

Таблица 1. Среднее время работы стегоаналитических алгоритмов

Разрешение	Стегоаналитический метод		
	χ^2	RS - анализ	SPA- анализ
Высокое (5760x3840)	31,32	319,6	83,93
Среднее (1024x683)	2,96	9,63	2,44
Низкое (500x333)	2,01	2,3	0,6

Зависимость времени работы алгоритмов от объема изображения представлена на рис.1.

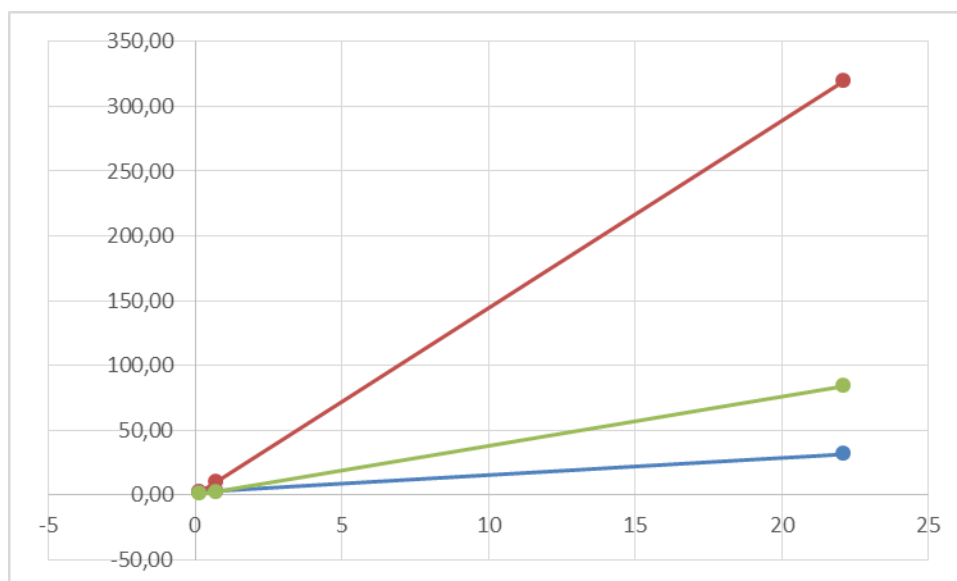


Рис 1. Зависимость времени работы алгоритмов от объема изображения

Из рис. 7 видно, что время работы алгоритмов приблизительно линейно зависит от объема исходных данных.

Наиболее быстрым алгоритмом для изображений большого объема является метод Хи-квадрат, для изображений низкого разрешения самый быстрый метод – SPA-анализ.

Самый медленный алгоритм – RS-анализ, время его работы для изображений высокого разрешения превышает 6 минут, поэтому на практике его использование может быть нецелесообразно.

Для оценки эффективности методов стегоанализа сопоставлялось вычисленное значение коэффициента заполнения контейнера с реальным значением y , рассчитанным в предыдущем пункте. Для этого вычислялась относительная погрешность измерения по формуле $p = \frac{|x-y|}{y}$. Средняя относительная погрешность приведена в таблице 2.

Таблица 2. Средняя относительная погрешность вычисления коэффициента заполнения контейнера для стегоаналитических алгоритмов

Разрешение	Стегоаналитический метод		
	χ^2	RS - анализ	SPA- анализ
Высокое (5760x3840)	92%	62%	35%
Среднее (1024x683)	85%	41%	22%
Низкое (500x333)	52%	23%	11%

Анализ результатов показывает, что метод Хи-квадрат дает очень высокую относительную погрешность, во многом его результаты определяются не процентом заполнения контейнера, а особенностями исходного изображения. Наиболее высокую точность показал метод SPA-анализа.

Очень важным тестом являлось применение стегоаналитических алгоритмов к незаполненным контейнерам. Метод Хи-квадрат показал практически 100% ложных срабатываний: метод во всех изображениях обнаружил подозрительные области, занимавшие от 20 до 100% пискелей. RS-анализ на незаполненных контейнерах показывал процент заполнения от 0,1% до 1,5%, SPA-анализ – от 0 до 0,4%.

Таким образом, экспериментальное исследование показало, что наиболее точным методом является SPA-анализ, относительная погрешность которого не превышает 35%. Также этот метод демонстрирует высокую скорость обработки изображений, поэтому его можно использовать для автоматического анализа.

Список литературы

1. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2002.
2. Швидченко И.В. Методы стеганоанализа для графических файлов // Искусственный интеллект, 2010, № 4–С. 697-705.
3. Елтышева Е. Ю., Фионов А. Н. Построение стегосистемы на базе растровых изображений с учетом статистики младших бит // Вестник СибГУТИ. 2009. №1. С. 67-84.
4. Westfeld A. Pfitzmann A. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and S-Tools-and Some Lessons Learned // 3rd International Workshop on Information Hiding (2000). — URL: <http://www.ece.cmu.edu/~adrian/487-s06/westfeld-pfitzmann-ihw99.pdf>
5. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images // ACM Workshop on Multimedia and Security, 2001, pp. 27-30 – URL: http://www.ws.binghamton.edu/fridrich/Research/acmwrkshp_version.pdf
6. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в JPEG-файлах // Вестник ВГУ, серия: Системный анализ и информационные технологии, 2007, № 1 – С.21-30.
7. StegMachine is a flexible tool for stegoanalysis. URL: <https://github.com/Panda-Lewandowski/StegMachine/blob/master/stegmachine.py>