мы должны передать секретный ключ на другой конец провода. Если мы просто передадим ключ, курьер сможет расшифровать наше послание. Алгоритм Диффи-Хеллмана как раз и призван решить эту задачу.

Алиса и Боб хотят использовать общий ключ для шифрования переписки. Рассмотрим детально этот процесс, используя краски вместо чисел (рисунок 1):

1. Алиса и Боб выбрали общую краску.
2. Алиса и Боб выбрали по одной секретной краске.
3. Алиса и Боб смешали общую и секретную краску.
4. Алиса и Боб обменялись получившимися смешанными красками.
5. Алиса смешала полученную смешанную краску от Боба со своей секретной краской.
6. Боб смешал полученную смешанную краску от Алисы со своей секретной краской.
7. Теперь у Алисы и Боба есть общая секретная краска.

Суть смешения красок в том, что один и тот же цвет можно получить смешением различных цветов и чтобы подобрать перебором настоящие исходные цвета нужно совершить огромное количество вычислений.

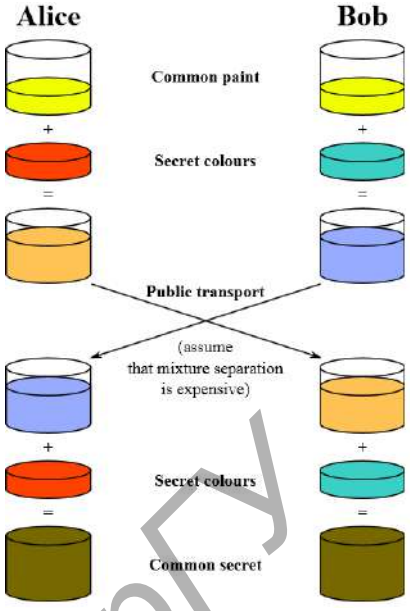

Рисунок 1 — Визуализация алгоритма Диффи-Хеллмана [4]

В реальной задаче вместо цветов используют функцию остатка от деления, так как, так же, как с цветами, функция результат z в выражении $x \ mod \ y = z$, можно получить используя совершенно различные целые числа x и y. Задача нахождения z, является задачей линейного логорифмирования, которую, на данный момент, человечество не научилось решать эффективно, поэтому данный алгоритм является таким надежным.

Заключение. В данной статье мы рассмотрели метод защиты от перехвата сетевого трафика. Данную задачу позволяет решить алгоритм Диффи-Хеллмана. В настоящее время он является достаточно надежным, т. к. еще не появились программные комплексы, имеющие высокую вычислительную мощность.

Список цитируемых источников

1. *Таненбаум, Э.* Распределенные системы. Принципы и парадигмы / Э. Таненбаум, М. ван Стеен. — СПб. : Питер, 2003. — 877 с
2. *Хант, К.*TCP/IP. Сетевое администрирование : пер. с англ. / К. Хант. — 3-е изд. — СПб : СимволПлюс, 2004. — 816 с.
3. *Олифер, В. Г.* Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер — 4-е изд. — СПб. : Питер, 2014. — 944 с.
1. *Шнайер, Б.* Прикладная криптография. Протоколы, алгоритмы и исходный код на С / Б. Шнайер. — М. : Вильямс, 2016. — 842 с.

УДК 004.65

К. Ю. Матусевич, О. Д. Кравчук

Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

СОЗДАНИЕ АРИФМЕТИЧЕСКОГО ТРЕНАЖЕРА

Введение. В современном мире каждый человек применяет базовые правила арифметики, даже не задумываясь об этом. Поэтому развитие этих способностей необходимо начинать как можно раньше, с самого детства человека, так как в условиях нашего мира невозможно будет догнать то, что было упущено раньше. Тренажеры могут быть использованы для дополнительной работы с первоклассниками учителями и родителями в классе и дома как для индивидуальной, так и коллективной подготовки [1]. Они способствуют автоматизации вычислительных навыков у ребенка, отработке умений складывать, вычитать, сравнивать и решать простые задачи.

Целью исследования является создание арифметического тренажера, с возможностью выбора количества примеров, разрядности и действия, в котором пропущены разные числа — не обязательно результат.

Объектом исследования являются возможности, компоненты, методы и способы создания приложений, использующих Windows Forms.

Объектом исследования является оконное развивающее приложение для тренировки устного счета.

Основная часть. Оконное приложение — это класс приложений, использующих для взаимодействия с пользователем элементы графического пользовательского интерфейса, т. е. объекты типа: окна, кнопки, поля ввода, элементы контроля и многие другие.

В качестве среды разработки использован Embarcadero C++ Builder, который предоставляет широкие возможности для создания оконных приложений.

Исходными данными в приложении являются имя игрока, которое используется для сохранения результатов и набор настроек параметров игры. Настройки нужны для корректной генерации вопросов по выбранному арифметическому действию, определения количества вопросов, разрядности чисел и выбора режима игры. В обычном режиме игры нет ограничения по времени для решения примера, а в режиме «на время» на весь блок вопросов предусмотрено ограниченное количество времени, которое рассчитывается согласно выбранным настройкам.

Перед началом игры необходимо настроить режим (рисунок 1), для чего необходимо заполнить следующие параметры:

– «Действие», для которого возможны 4 варианта выбора: вычитание, деление, умножение, сложение;

– «Разрядность», определяющая разрядность чисел в примерах;

– «Количество вопросов»: доступно три варианта количества вопросов: от 10 до 15, от 16 до 20, от 21 до 25;

– «Режим игры». В режиме игры «Обычный» у игрока нет ограничения по времени. Режим «На время» создает для пользователя определенное количество времени, предусмотренное для решения всех примеров. Количество времени зависит от других выбранных настроек. Так, на примеры с использованием деления и умножения выделяется больше времени.

По желанию игрока можно нажать на кнопку «Случайно». После нажатия на эту кнопку в каждом пункте настроек случайным образом выберется один пункт. Для сохранения настроек необходимо нажать кнопку «Сохранить». Эта кнопка также ведет обратно на главный экран приложения.

До начала игры необходимо ввести в поле «Имя» свое имя, которое необходимо для дальнейшего сохранения результата в файл. После нажатия кнопки «Начать игру» появляется окно, в котором будет происходить сам игровой процесс. После этого появляется кнопка «Начать», которая выводит первый пример и запускает таймер. После вывода примера игроку нужно ввести в соответствующую ячейку предполагаемый ответ. Остальные ячейки при этом недоступны для ввода. Для сохранения ответа необходимо нажать кнопку «Проверить», затем кнопку «Продолжить» — для вывода следующего примера. Разрабатываемое приложение имеет генерирует новый набор примеров каждый раз, когда игрок начинает новую игру. Один из примеров представлен на рисунке 2.

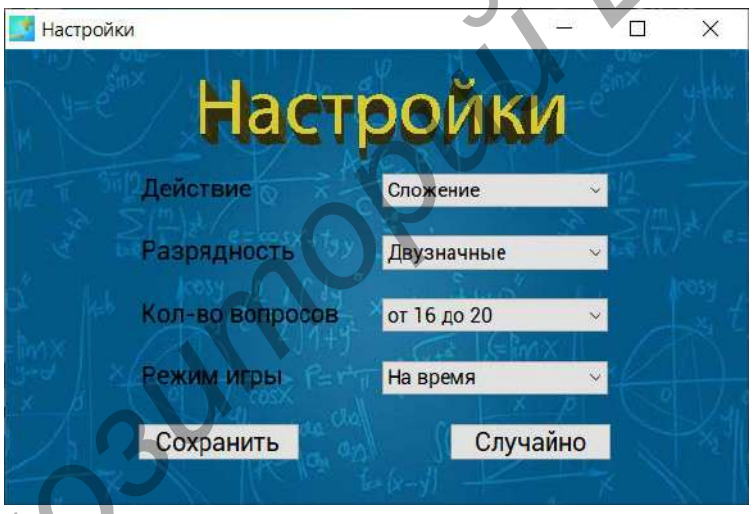

Рисунок 1 — Окно «Настройки»

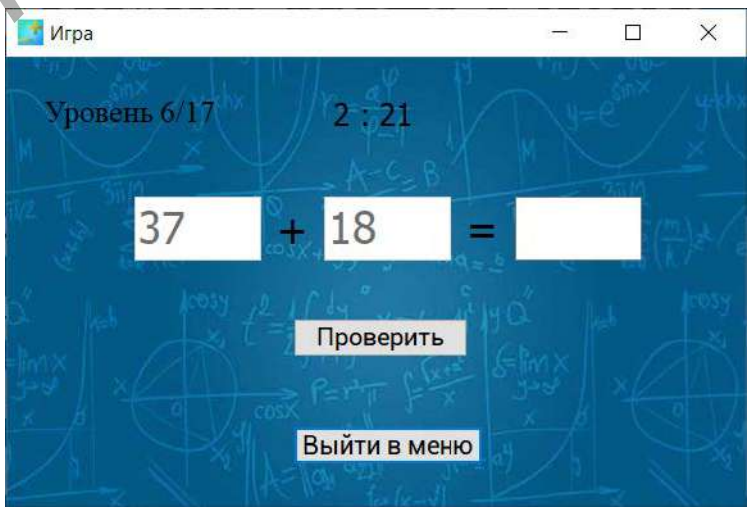

Рисунок 2 — Вид примеров в процессе игры

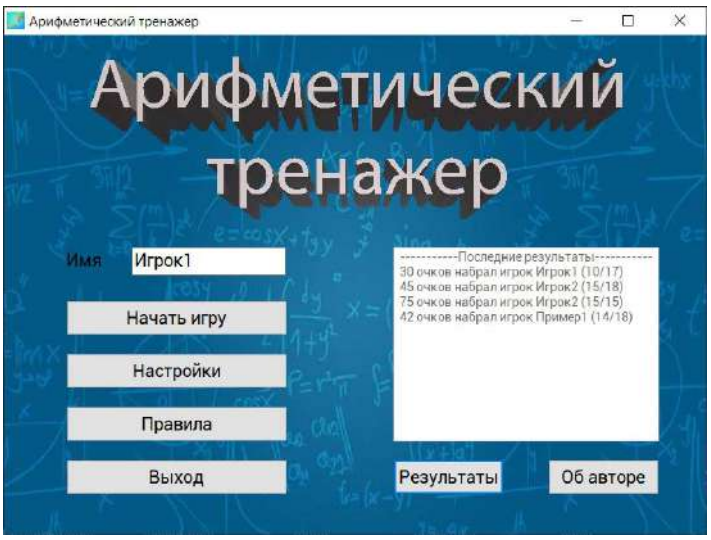

Рисунок 3 — Результат тестовой игры

Результатом игрового процесса становится количество баллов, которые набрал пользователь, его имя и отношение правильных ответов относительно общего количества вопросов. Все эти данные записываются в текстовый файл «Результаты.txt» и доступны в главном меню приложения.

Все результаты доступны по нажатию кнопки «Результаты» (рисунок 3).

Кроме этого из главного окна имеется возможность просмотра правил игры.

Заключение. Компьютерные тренажеры предназначаются для отработки практических умений и навыков, а также развития творческих способностей. Разработанный арифметический тренажер:

1. Развивает математические способности.
2. Производит обучение ментальной арифметике.
3. Увеличивает рабочую память обучающегося.

Данное приложение нацелено в первую очередь для детей школьного и дошкольного возраста, а также всех остальных людей любой возрастной категории, которые захотят улучшить навыки устного счета или проверить, на что они были способны до этого момента времени.

Список цитируемых источников

1. *Босова, Л. Л.* Теория и методика обучения информатике младших школьников : монография / Л. Л. Босова. — М. : МПГУ, 2020. — 296 с.

УДК 004.65

Н. А. Остапчук, О. Д. Кравчук
Учреждение образования «Барановичский государственный университет», Барановичи, Республика Беларусь

АВТОМАТИЗИРОВАННАЯ СИСТЕМА РАСЧЕТА ПОКАЗАТЕЛЕЙ БИЗНЕС-ПЛАНА

Введение. В условиях рыночной экономики важной областью стало информационное обеспечение, которое состоит в сборе и обработке информации, для использования результатов ее анализа в процессе своей деятельности, принятия обоснованных управленческих решений. При этом особое значение приобретает обеспечение оперативности и достоверности информации [1].

Данное исследование посвящено проблеме реализации методов и алгоритмов для создания и редактирования бизнес-планов.

Целью исследования является создание автоматизированной системы, осуществляющей создание и редактирование бизнес-планов, необходимых для открытия бизнеса. Средство должно быть пригодно к применению на современных компьютерах и в используемых на предприятии операционных системах.

Предметом исследования является создание автоматизированной системы разработки инновационных и бизнес-проектов.

Основная часть. Разработка бизнес-плана — сложное и трудоемкое занятие, поэтому исключительно актуальным является вопрос о ее компьютеризации. Только одна корректировка плана может повлечь за собой перерасчет всех показателей по всем разделам плана.