

Разработан сайт, на котором можно кратко ознакомиться с экспонатами, представленными в визуализаторе, и скачать сам виртуальный парк для Windows.

Наш проект также является прототипом возможного реального парка в нашем городе.

Минимальные системные требования программы: операционная система Windows 7; процессор: 2,5 ГГц; оперативная память: 4 Гб; видеокарта: 1 Гб; DirectX: Версии 9; место на диске: 500 Мб.

Программа сделана на движке Unity3D 5 — это инструмент для разработки двух- и трёхмерных приложений и игр, работающий под операционными системами Windows, Linux и OS X. Созданные с помощью Unity приложения работают под операционными системами Windows, OS X, Windows Phone, Android, Apple iOS, Linux, а также на игровых приставках Wii, PlayStation 3, PlayStation 4, Xbox 360, Xbox One.

Редактор Unity имеет простой Drag&Drop интерфейс, который легко настраивать, состоящий из различных окон, благодаря чему можно производить отладку игры прямо в редакторе. Движок поддерживает два сценарных языка: C#, JavaScript (модификация). Расчёты физики производит физический движок PhysX от NVIDIA.

Скрипты написаны на высокоуровневом, объектно ориентированном языке программирования C#. Пользовательский интерфейс создан с помощью Adobe Photoshop CC. 3D-модели создавались при помощи Blender и Cinema4D R16 с дальнейшим экспортом в формат FBX, который поддерживает Unity.

В программе использован принцип объектно ориентированного программирования. Реализованы классы: для работы с пользовательским интерфейсом, для обработки устройств ввода, для работы с 3D-моделями экспериментов, для связи пользовательского интерфейса и устройств ввода с функциями экспонатов парка.

Программа даст возможность интерактивно изучать некоторые разделы физики, что позволит увеличить интерес детей к этому предмету.

При входе в приложение вам предложат нажать кнопку «Начать прогулку», после чего вы сможете с помощью клавиш “WASD” ходить по виртуальному парку и взаимодействовать с различными смоделированными экспериментами.

Большинство объектов, с которыми вы столкнётесь, интерактивны, т. е. если подойти к одному из них и нажать соответствующую клавишу, то запустится анимация данного эксперимента. Как пример, эксперимент, который наглядно показывает движение по наклонной поверхности, где мы находимся непосредственно в шаре и можем почувствовать, как увеличивается ускорение. Необходимо забраться по лестнице до шара, нажать клавишу «E» для взаимодействия, и вы поместитесь в шар и будете скатываться с горы. Или ещё эксперимент с пушкой, стреляющей под углом к горизонту, где вы должны подобрать угол выстрела так, чтобы попасть в цель; в нашем случае целью является яма, в которую должно попасть ядро. Для взаимодействия нужно подойти к пушке, нажать «E», затем вы сможете с помощью клавиш «вверх», «вниз» выбрать угол выстрела и с помощью клавиши «пробел» сделать выстрел.

Очень много объектов неинтерактивных, они добавлены в приложение для визуального восприятия того, что мы находимся в парке, хоть и виртуальном. Например, скамейки, фонари, мусорки, деревья и т. д.

В дальнейшем планируется добавить игровую зону в виртуальный парк. В этой зоне будет расположен лабиринт с дверьми. Для того чтобы открыть дверь, надо будет решить задачи по физике или собрать простые электрические схемы. Задачи будут случайно генерироваться. Планируется добавить виртуальную обсерваторию.

Заключение. Разработан сайт, где вы уже можете скачать «Виртуальный парк экспериментов» для Windows и опробовать его сами [1].

Хотелось бы, чтобы проект получил дальнейшее развитие в виде реального парка экспериментов, который бы стал продуктом культурного и научно-образовательного туризма Вологодской области.

Список цитируемых источников

1. Виртуальный парк экспериментов [Электронный ресурс]. — Режим доступа: <https://experiments-park.ru/>. — Дата доступа: 16.10.2016.

УДК 004.9

А. Н. Саганович, С. А. Попова

Учреждение образования «Барановичский государственный университет», Барановичи

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ВЫПОЛНЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Введение. Электронно-цифровая подпись (ЭЦП) — это конечная цифровая последовательность, зависящая от самого сообщения или документа и от секретного ключа, известного только подписывающему субъекту, предназначенная для установления авторства. В настоящее время ЭЦП используется в основном для аутентификации автора (создателя) информации и для доказательства (проверки) того факта, что подписанное сообщение

или данные не были модифицированы при передаче информации в компьютерных сетях. Применение подобной цифровой подписи в качестве средства для идентификации и подтверждения юридической значимости документов становится стандартом цифрового мира [1].

Основная часть. Актуальность темы обусловлена тем фактом, что в настоящее время многие предприятия используют различные системы электронного документооборота, позволяющие значительно сократить время, затрачиваемое на обмен документацией, усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов. При этом встает вопрос авторства документа, достоверности и защиты от искажений [2].

Надо отметить, что большое число предприятий республики сегодня в основном используют те или иные методы бумажной обработки и обмена документами, что влечет за собой следующие недостатки: отсутствие необходимой квалификации у сотрудников при проведении бумажного документооборота; низкое качество образцов подписи, изменчивость подписи и возможность ее подмены; недоступность образцов подписи — при получении подписанного договора, счета или справки чаще всего отсутствует возможность сравнить подписи в этих документах с достоверными образцами.

Учитывая вышеизложенное, была поставлена цель — разработать программное средство для выполнения ЭЦП. В качестве алгоритмов шифрования данных выбран асимметричный алгоритм RSA, поскольку он надежнее, у него упрощенный механизм обмена ключами. Для разработки программного приложения использована среда программирования Microsoft Visual Studio.

Так как цифровая подпись строится на базе криптосистемы с открытым ключом, то необходимо иметь пару ключей — секретный и открытый. Секретный ключ используется для формирования цифровой подписи, поэтому его нужно хранить в тайне. А открытый ключ используется для проверки соответствия подписи документу, поэтому он должен быть опубликован, например, в общедоступном каталоге.

После запуска программы открывается форма генерации ключей, на которой требуется заполнить необходимые поля. Для этого вводятся данные первого пользователя: фамилия, имя, отчество, должность, табельный номер (уникальный номер). Для подтверждения действия следует нажать на кнопку «Сгенерировать ключи». Подобным образом создаются ключи для второго пользователя (рисунок 1).

Рисунок 1 — Форма генерации ключа для пользователя

Чтобы подписать файл, который будет передан по защищённому каналу, необходимо перейти на форму «Работа с файлом» (рисунок 2). Далее выбрать файл из предлагаемого списка, открытый ключ адресата на вкладке «Контейнер открытых ключей», также разновидность ЭЦП «Присоединенная электронная подпись» или «Присоединенная электронная подпись (с шифрованием)» и нажать на кнопку «Подписать файл». Шифрование методом «Присоединенная электронная подпись с шифрованием» более надёжное, так как сообщение будет дополнительно зашифровано.

Если файл не был поврежден или не были внесены изменения, то программа выдаёт сообщение об успешном подписании.

После того как файл подписан, он отправляется по защищенному каналу другому пользователю, у которого уже имеется открытый ключ отправителя, с помощью которого он сможет расшифровывать полученный файл. Выбираются пути к зашифрованному файлу (*.crypt), к сеансовому ключу (*.skey) и к зашифрованному вектору (*.siv). Представим форму расшифрования файла (рисунок 3).

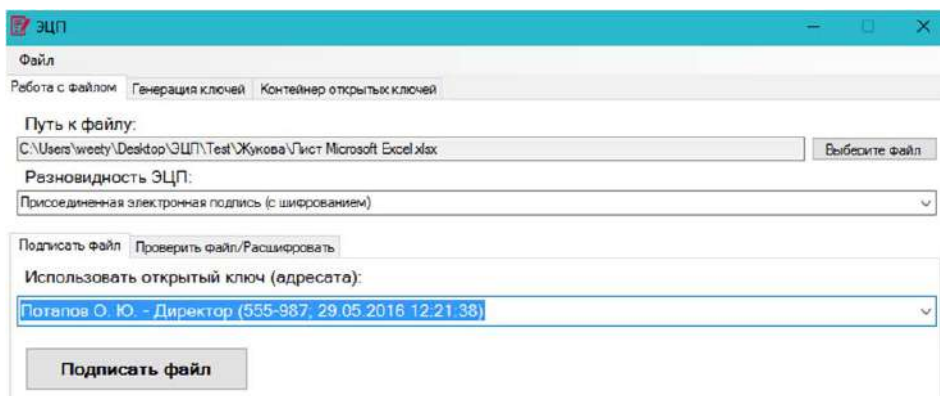


Рисунок 2 — Форма подписи файла методом шифрования

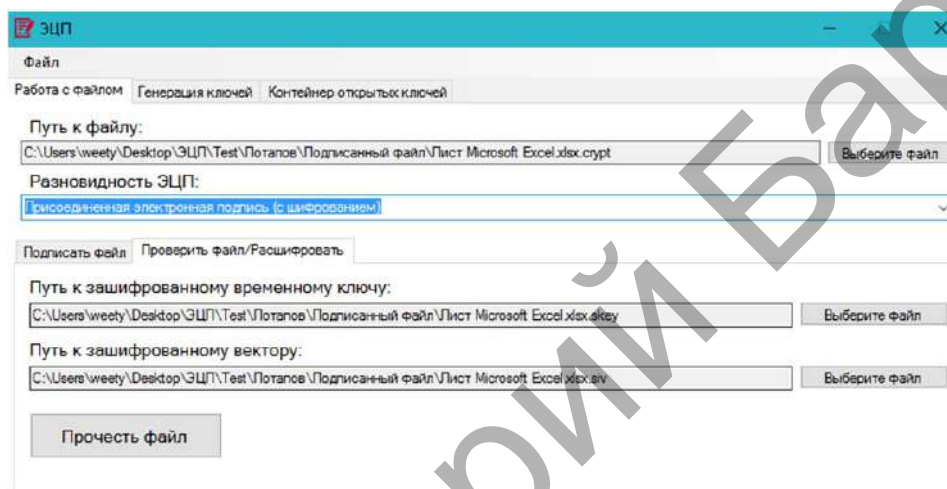


Рисунок 3 — Форма расшифрования файла

При нажатии на кнопку «Прочитать файл» программа предлагает сохранить в исходном формате зашифрованный ранее файл. После успешного расшифрования будет выдано сообщение, кем был подписан документ. На основании проведенного тестирования и анализа возможностей разработанного программного продукта можно сделать вывод, что он является вполне конкурентоспособным на рынке современных систем автоматизации.

Заключение. Электронная цифровая подпись является максимально перспективным и широко используемым в мире способом защиты электронных документов от подделки, обеспечивает высокую достоверность сообщения, позволяет однозначно идентифицировать отправителя сообщения и перенести свойства реальной подписи под документом в область электронного документа [3].

Список цитируемых источников

1. Обзор схем электронной цифровой подписи [Электронный ресурс]. — Режим доступа: <http://www.nestor.minsk.by/sr/2005/12/sr51218.html> — Дата доступа: 13.03.2017.
2. Об электронном документе : Закон Респ. Беларусь от 10.01.2000 г. № 357-3 // Нац. реестр правовых актов Респ. Беларусь. — 2000. — 2/132.
3. Основные этапы реализации электронной цифровой подписи [Электронный ресурс]. — Режим доступа: <http://lektcii.org/4-17422.html> . — Дата доступа: 13.03.2017.