Дубровина О.В., Повшко Е.В.
Белорусский государственный университет, Минск

ИСПОЛЬЗОВАНИЕ ДЕМОНСТРАЦИОННЫХ МЕДИАЭЛЕМЕНТОВ В УЧЕБНОМ КУРСЕ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Широкое внедрение медиаэлементов в демонстрационные материалы, используемые при чтении учебных дисциплин, постепенно захватывает и те из них, которые считаются в некоторой степени традиционными. Такие элементы обучения позволяют показать сложные алгоритмические конструкции, которые при обычном изложении трудны для понимания и последующего воспроизведения студентами.

Дисциплина «Криптографические методы и средства защиты информации» предлагается для изучения студентами 3-го курса специальности «Прикладная информатика» направления «Веб-дизайн и компьютерная графика». В соответствии с государственным образовательным стандартом [3] содержание курса направлено на ознакомление студентов с математическими основами теории шифрования, историей развития криптографии, включая современные тенденции, а также с основными алгоритмами шифрования, хэширования и электронной цифровой подписи, криптографическими протоколами обмена информацией, методами криптоанализа, стеганографическимим методами скрытия передаваемой информации, современными развивающимися тенденциями в криптографии.

Традиционно лекционный материал предлагается студентам в виде мультимейдийных презентаций, а лабораторные занятия включают в себя вычислительные, проектные и тестовые задания.

Для сопровождения данной дисциплины разработан дополнительный ресурс в виде приложения, иллюстрирующий некоторые разделы в виде рисунков-комиксов и анимационных роликов. Внедрение таких неформальных элементов как комиксы в насыщенный не самым простым математическим аппаратом учебный курс является нетрадиционным подходом.

Стилистика и основная идея созданного графического материала позаимствована с согласия автора у Джефа Мозера [6], автора известного графического представления шифра AES «в картинках». Усиливающим эффектом привлечения внимания является взаимодействие героя комикса с обучающимся через риторические вопросы, некоторые сцены содержат дополнительные персонажи, которые уточняют информацию путем постановки дополнительных вопросов. Упрощение восприятия осуществляется путем разделения комикса по тематикам на четыре акта, простота исполнения позволяет акцентировать внимание на важных элементах. Пример комикса, содержащего исторические сведения, приведен на рисунке 1.

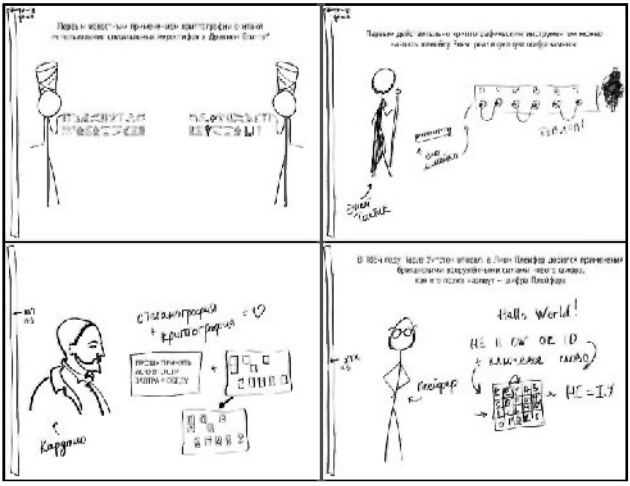

Рисунок 1. – Фрагмент комикса на тему «История криптографии»

Первый модуль приложения включает историческую справку, в которой представлены этапы становления криптографии как науки.

В рамках данного раздела проекта рассмотрены такие системы шифрования, как иероглифическое письмо Древнего Египта, линейка Энея, квадрат Полибия, шифр Цезаря, история возникновения шифров RSA, Диффи-Хеллмана, ГОСТ-28147, AES, DES, RC4, RC5, а также алгоритмы хеширования MD5, SHA-1 и алгоритмы симметричного шифрования DES, ГОСТ-218147.

Вторая часть иллюстративного материала представляет собой видеоролики, формирующие общее представление о системах шифрования. Главными героями анимационного видео являются традиционные в криптографии персонажи Боб и Алиса. Сюжет анимации сосредоточен на вопросе передачи зашифрованной информации. Для обработки графического материала использован инструментарий Adobe Photoshop [4], анимация проводилась в редакторе с помощью программы Motion5 [5]. В итоге, для проекта реализованы видеоролики, демонстрирующие общие идеи симметричных и асимметричных систем шифрования, а также государственный стандарт шифрования Республики Беларусь BelT [1].

Разработанные графические и видеоматериалы интегрированы в общую оболочку, реализованную на основе технологии Windows Presentation Foundation (WPF) [1], которая дополнительно содержит справочные текстовые описания шифров, функций хеширования и алгоритмов электронной цифровой подписи в соответствии с их стандартами, ссылки в сети Интернет на эти стандартны и полезные сетевые ресурсы, а также программно разработанные тестовые задания, позволяющие провести контрольные мероприятия.

Программное приложение предназначено при проведении практических занятий по учебным дисциплинам, содержащим разделы криптографии и защиты информации, а также для самостоятельной работы учащихся и контрольных мероприятий.

ЛИТЕРАТУРА

1. Алгоритм шифрования BelT: СТБ П 34.101.31 – 2011; введ. 30.01.2011. – Минск: Межгос. совет по стандартизации, метрологии и сертификации: Белорус. гос. ин-т стандартизации и сертификации, 2011. – 10 с.

2. Введение в WPF в Visual Studio 2015. – [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/ru-ru/library/aa970268(v=vs.110).aspx – Дата доступа: 12.04.2016.

3. Образовательный стандарт Высшего образования первой ступени. Специальность 1-31 03 07 Прикладная информатика (по направлениям); введ. 30.08.2013 – Минск: Министерство образования Республики Беларусь: РИВШ, 2013. – 45 с.

4. Adobe.com: официальный сайт. – [Электронный ресурс]. – Режим доступа: http://www.adobe.com/ru/products/photoshop. – Дата доступа: 20.01.2016.

5. Motion: официальный сайт. – [Электронный ресурс]. – Режим доступа: http://www.apple.com/final-cut-pro/motion. – Дата доступа: 18.01.2016.
6. Moserware: сайт разработчика Дж. Мозера. – [Электронный ресурс]. – Режим доступа: http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html. – Дата доступа: 08.02.2016.