Литература

1. ИСП ЗАО «Международный деловой альянс» IBA [Электронный ресурс]. – Режим доступа: http://belarus.iba.by/iba_web/main.nsf/home/ru.index.html. – Дата доступа:25.02.2011.
2. «Системные технологии» [Электронный ресурс]. – Режим доступа: http://www.st.by/rus/products/– Дата доступа: 25.02.2011.
3. ЗАО «БиСмарт» [Электронный ресурс]. – Режим доступа: http://www.besmart.by/– Дата доступа:25.02.2011.
4. «Надежные программы» [Электронный ресурс]. – Режим доступа: http://www.belarus.su/relsoft/index_r.htm – Дата доступа: 25.02.2011.
5. Информационные технологии Беларуси [Электронный ресурс]. – Режим доступа: http://it-belarus.net/ – Дата доступа: 25.02.2011.
6. SoftClub [Электронный ресурс]. – Режим доступа: http://www.softclub.by/– Дата доступа: 25.02.2011.

КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ: ОДНОРАЗОВЫЕ БЛОКНОТЫ

А.А. Коновалова
БГЭУ, ф-т МЭО, студентка 2-го курса
Ю.А. Магазинщикова
БГЭУ, ф-т МЭО, студентка 2-го курса

Научный руководитель: Т.А. Ткалич, к.ф.-м.н., доцент

Криптография имеет многовековую историю развития и использования. Она представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей.

Выделяют множество различных алгоритмов шифрования, однако существует такой, который невозможно вскрыть, – одноразовый блокнот (шифр Вернама). Он представляет собой большую неповторяющуюся последовательность символов ключа, распределенных случайным образом. Шифрование состоит в сложении буквы открытого текста и буквы из одноразового блокнота по модулю N, где N – количество букв в алфавите. После зашифрования отправитель уничтожает использованный одноразовый блокнот. Чтобы отправить новое сообщение, ему придётся изготовить или найти новый одноразовый блокнот. Получатель, владеющий копией одноразового блокнота, которым воспользовался отправитель сообщения, получает открытый текст путём сложения букв шифротекста и букв, извлечённых из имеющейся у него копии одноразового блокнота. После данной операции копия уничтожается [1].

В 1949 году Клодом Шенноном была доказана абсолютная стойкость данного шифра. Однако шифр Вернама обладает определёнными недостатками:

– Длина блокнота ограничена.
– Нельзя использовать страницу шифровального блокнота повторно.
– Сложно распространять блокноты.
– Избыточность шифра.
– Сложно построить шифровальную сеть [2].

Несмотря на перечисленные недостатки, в настоящее время одноразовые блокноты активно используются для шифрования сверхсекретных сообщений как в Республике Беларусь, так и в других странах (например, США). Не имея в своём распоряжении соответствующего блокнота, эти сообщения невозможно прочитать вне зависимости от того, насколько быстро работают суперкомпьютеры, которые используются в ходе криптоаналитической атаки [3].

В данный момент времени в Республике Беларусь действует Белорусский государственный институт стандартизации и сертификации, который также разрабатывает криптографические средства защиты информации. К его основным функциям относятся научно-исследовательские и опытно-конструкторские работы по методологии технического нормирования, стандартизации, кодированию, разработка программ технического нормирования и стандартизации и др.

Литература
1. Анин, Б.Ю. Защита компьютерной информации / Б.Ю. Анин. – СПб.: БХВ – Санкт-Петербург, 2000. – 384 с.: ил.
2. Венбо, Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice / Мао Венбо. – М.: Вильямс, 2005. – 768 с. – 2 000 экз.
3. Конхейм, А.Г. Основы криптографии / А.Г. Конхейм. – М.: Радио и связь, 1987.

ОРГАНИЗАЦИЯ ТЕСТИРОВАНИЯ В ЭУМП ДЛЯ САМООБУЧЕНИЯ

Т.П. Корнюшко
МИУ, магистрант

Научный руководитель: В.В. Гедранович, к.п.н., доцент

Переход от принципа «обучение на всю жизнь» к принципу «обучение всю жизнь» требует внедрения современных технологий, автоматизации, модернизации существующих педагогических концепций, развития педагогических технологий обучения. В роли таких технологий могут выступать информационно-коммуникационные, которые позволяют гармонизировать учебное взаимодействие между преподавателем и студентом, принимая на себя роль интеллектуального «помощника» преподавателя [1]. В качестве такого помощника может выступать электронное учебно-методическое пособие (ЭУМП) для самообучения.

В соответствии с учебной программой основная цель дисциплины «Основы информационных технологий» для специальности 1-23 01 04 «Психология» – формирование компьютерной грамотности и подготовка студентов к использованию современных информационных технологий в качестве инструмента для решения **практических** задач в своей предметной области. Поэтому при разработке ЭУМП по этой дисциплине должна учитываться её практическая направленность, уделяться большое внимание заданиям, позволяющим приобрести навыки работы с программным обеспечением. Особое внимание следует уделить организации самоконтроля.

Для организации самоконтроля планируется использовать тестирование как одну из самых прогрессивных форм оценки учебных достижений. Однако прежде чем предлагать тест студентам и надежно полагаться на его результаты, расценивая их как отражение уровня знаний тестируемых, необходимо оценить качество самих тестов [2].

В ЭУМП предлагается следующая технология тестирования. Для ответа на вопросы теста студенту представляются две попытки. Если студент ошибается третий раз, автоматически будет осуществляться переход на соответствующее практическое задание. При этом студенту необходимо обязательно проделать часть задания, что будет способствовать тому, что он будет запоминать не только конкретное определение, а понимать смысл работы в целом. После этого студент возвращается назад к тестовым заданиям и продолжает проверку своих знаний. По окончанию выполнения теста дается общая оценка проделанной работы, есть возможность просмотреть свои ошибки, а также основные моменты и определения по пройденной теме.

Перейти к работе со следующей главой возможно только после того, как будут выполнены все пункты текущей темы и пройден тест на положительную оценку. Тем самым, такая обязательная последовательность выполнения заданий и тестов будет способствовать более качественному усвоению программного материала.

Возможность самоконтроля и проверки знаний на любом этапе обучения весьма существенна, так как успех изучения любой дисциплины зависит от степени усвоения тех понятий, терминов и положений, которые изучались на предшествующих этапах обучения. Тесты в наиболее конкретной форме выражают эти требования, стимулируют познавательную активность и позволяют оперативно корректировать свое самообучение.

Литература
1. Гедранович, В.В. Управление учебно-познавательной деятельностью студентов на основе ИКТ / В.В. Гедранович // Модернізація освіти: пошуки, проблеми, перспективи: Матеріали II