ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ТОШКЕНТ ДАВЛАТ ИҚТИСОДИЁТ УНИВЕРСИТЕТИ

ОЛИЙ ИҚТИСОДИЙ ТАЪЛИМНИ МОДЕРНИЗАЦИЯЛАШ: ДОЛЗАРБ МАСАЛАЛАР, УСТУВОР ЙЎНАЛИШЛАР ВА ИСТИҚБОЛЛАР

халқаро илмий-услубий анжумани

ТЕЗИСЛАР ТЎПЛАМИ

19 - 20 март

MODERNIZATION OF HIGHER ECONOMIC EDUCATION: CHALLENGES, PRIORITIES AND PROSPECTS

Theses of the International

Scientific-methodical conference

March 19-20

ТОШКЕНТ- 2007

бухгалтерия ҳисоби бўйича вақтинчалик қоидаларда Самарқанд вилояти маҳаллий бюджети ҳисобининг ягона счётлари рўйхати келтирилган. Бу счётлар рўйхатига бюджет ижросининг банк тизимида қўлланилиб келинган счётлар ва айрим янги вақтинчалик иккинчи тартибли счётлар қўшилган.

Ҳозирги вақтда тажриба ўтказилаётганлиги ва «Ўзбекистон Республикаси Давлат бюджети ғазна ижроси бухгалтерия ҳисобининг ягона счётлар режасини қўллаш бўйича йўриқнома»нинг йўқлигини ҳисобга олган ҳолда «Бюджет ҳисоби» фани бўйича маъруза ва амалий машғулотлар ўтказилиши керак бўлади.

Д.М. Расулев, А.К. Машарипов, М.А. Мусаева,
ТГЭУ

К вопросу технологии обучения на лекциях

Из образовательной технологии по предмету «Безопасность информации в компьютерных системах и сетях» остановимся на вопросах технологии обучения на лекциях темы «Методы и моде́ли защиты информации», где рассматриваются вопросы криптографических методов и шифры, ключи, шифрование и дешифрование, их характеристики и требования.

В технологии обучения указывается учебное время, отведенное для этой лекции, количество обучающихся в каких-то пределах (для данной лекции – 2 часа, и не ≥ 50 человек), но это не требует особо точный выдержки этих требований. Кроме того, озвучиваются вопросы лекции с записью в конспекты слушателей, а также цели учебного занятия. Так как форма учебного занятия – информационная лекция, необходимо при изложении целей учебного занятия сформулировать целостное представление о предмете лекции, в нашем случае, о криптографических методах и о шифровании и дешифровании.

Что значит целостное представление? В нашем случае необходимо показать, что криптография, это не только шифрование, но и стеганография, кодирование и сжатие, и что при шифровании и дешифровании основной являются ключи, как симметричные, так и асимметричные. Следует напомнить принципы организации ключей по способу преобразования, также как при методах замены (подстановки), методах перестановки, аналитических, аддитивных и комбинированных методах.

Целостное представление ставится в разделах педагогических задач и результатах учебной деятельности, технологии и обучении на лекции методам защиты информации, освещении понятий о шифре и ключе, о шифровании и дешифровании, показе их характеристик и требований.

Что касается объяснения криптографических методов защиты информации, особо рекомендуется остановиться на методе стеганографии, который позволяет скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается.

При раскрытии понятий о шифре и ключе, шифровании и дешифровании, характеристик и требований к указанным понятиям необходимо особо

подчеркнуть, что шифрование - это процесс преобразования открытой информации в закрытую, а дешифрование – это процесс обратный.

Так как методы замены и перестановки излагаются в раздаточных лекционных материалах достаточно подробно, следует остановиться на методах аналитических, аддитивных и комбинированных.

Аналитические методы шифрования основаны на использовании алгоритмов из сложных математических преобразований исходного текста. Многие из них используют нерешенные математические задачи. Например, широко используемый в Интернете алгоритм шифрование RSAоснован на свойствах простых чисел (причем очень больших). Простыми называются также числа, которые не имеют делителей, кроме самых числа, не имеющие общих делителей, кроме единицы. Если на Вашем компьютере не установлена программа Unix Ssh – keygen (В Узбекистане программные средства в основном корпорации Microsoft) можно показать решение алгоритма RSA на маленьких простых числах ≥ 7. Решение алгоритма связано с модульной арифметикой.

Аддитивные методы шифрование (гаммирование) основаны на том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности как положение). Имеются различные способы гаммирования. Одним из важнейших требований, предъявляемых к системе шифрования, является её высокая стойкость. Однако повышение стойкости приводит к существенному усложнению самого процесса шифрования и увеличению использования ресурсов (времени, аппаратных средств, уменьшению пропускной способности и т. д.).

Комбинированное использование нескольких различных способов шифрования является достаточно эффективным средством повышения стойкости. Практика показывает, что стойкость комбинированного шифрования не ниже произведения стойкости используемых способов.

Типичный пример комбинированию шифра является национальный стандарт США криптографического закрытия данных DEC – (Data Encryption Standart).

При наличии времени в структуре лекционных занятий данного курса рекомендуется проводить занятия с конкретными примерами.

В технологии обучения на информационной лекции важны также средства обучения, методы обучения, форма обучения, условия обучения, мониторинг и оценка. По возможности рекомендуется их придерживаться.

Т. Б. Хамдамов, М.М. Ходжаханов,
ТГЭУ

Некоторые вопросы совершенствования обучения студентов экономической терминологии

В настоящее время, когда наша республика стоит на пути развития рыночной экономики, как никогда остро встаёт вопрос о совершенствовании подготовки высококвалифицированных экономистов. Обучение терминологии