ВОПРОСЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В КУРСАХ ПЕРЕПОДГОТОВКИ СЛУШАТЕЛЕЙ

В.А. Полубок, А.А. Косак

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь*

Не секрет, что стремление защитить свои интересы было присуще человеку с давних пор. Еще в древности он использовал различные варианты кодирования информации, изобретал устройства, которые бы способствовали созданию более стойких шифров, и при этом обеспечивал легкость шифрования.

Существует множество протоколов программного шифрования, которые защищены от взлома в различной степени. Отличие криптографических алгоритмов защиты информации от всех других методов защиты основано на свойствах самой информации с исключением свойств материальных носителей. Самыми распространенными среди средств криптографической защиты являются следующие типы протоколов: симметричные, в которых для шифрования и расшифровки используется один и тот же ключ: DES, AES, ГОСТ 28147-89, Camellia, Blowfish, RC4 и т.д. [1].

Анализ обучения слушателей переподготовки по специальностям, связанным с информационными технологиями, свидетельствует о недостаточной подготовке в области обеспечения информационной безопасности. Результаты анализа показывают, что в информационные курсы необходимо вводить темы, связанные с криптографической защитой информации. Для этих целей была модернизирована лабораторная работа в рамках курса «Основы алгоритмизации и программирования на языках высокого уровня», которая знакомит слушателей с основными принципами криптографической защиты данных. Знания, полученные в рамках данной работы, повысят уровень теоретической и практической подготовки слушателей, и в дальнейшем помогут выпускникам переподготовки быть более конкурентоспособными на рынке труда.

Список литературы

1. Лебедев А.Н. Криптография с открытым ключом и возможности ее практического применения. Тем. сб. «Защита информации». 1992. Вып. 2.