УДК 37.012

***М.Н. Хуторова**, преподаватель кафедры оперативно-розыскной деятельности Могилевского института МВД Республики Беларусь*

ПРИМЕНЕНИЕ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ПРИ ОБУЧЕНИИ КУРСАНТОВ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Постоянный характер стремительного распространения инновационных информационных технологий активизирует интерес к ним преступного сообщества как к инструментам воплощения новых видов преступлений. В современном информационном обществе является актуальным вопрос организации кибербезопасности, вследствие чего возникает необходимость в подготовке высококвалифицированных кадров для органов внутренних дел. Курсанты высших учебных заведений Министерства внутренних дел специализируются в первую очередь на изучении гуманитарных дисциплин, но современные реалии требуют от них быть специалистом во всех областях, как в гуманитарном, так и в техническом направлении. В связи с чем перед преподавателями технических дисциплин, таких как «Информационные технологии», «Основы информационной безопасности» встает вопрос об объяснении сложного технического материала «простым» языком.

Нами предлагается рассмотрение темы блочного симметричного шифрования на примере построения моделей в табличном процессоре. Рассмотрим алгоритм сети Фейстела. Идея сети Фейстела состоит в том, что исходный блок делится на две части. Одна часть подвергается преобразованию, а второй подблок отдыхает в раунде и становится на место своего соседа. Данный процесс повторяется столько раз, сколько раундов в алгоритме Фейстела. Для шифрования и дешифрования используется один и тот же алгоритм.

Курсантам необходимо построить электронную таблицу, моделирующую шифрование 8-разрядного блока трехраундовой сетью Фейстела с раундовой функцией из трех примитивов:

A – добавление (по mod 2) 4-разрядного ключа;

S – подстановка в виде инверсии;

P – регистр циклического сдвига влево на 1 разряд.

Исходный блок X и ключ K задаются пользователем. Зашифрованный блок Y последовательно рассчитывается таблицей.

Курсантам предлагается оформить таблицу по образцу с уже имеющимися формулами (рис. 1).

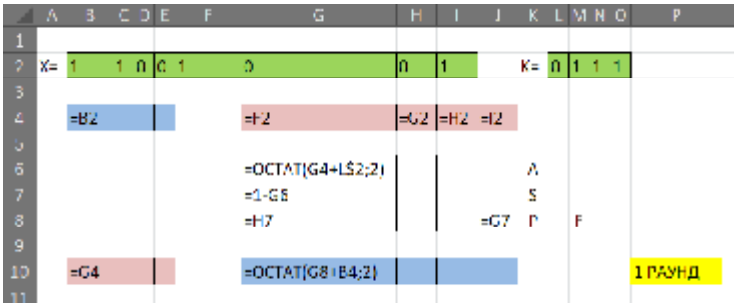

Рис. 1. Модель сети Фейстела (незаполненная)

Далее поясняется, что необходимо создать еще два раунда копированием первого. В итоге мы получим таблицу, представленную на рис. 2.

Для понимания выполненного задания курсантам предлагается внести пояснения по каждому пункту полученной таблицы, используя текст задания. Также предлагается проверить правильность построения сети Фейстела. Для этого необходимо полученный результат Y=01010101 ввести в X и на выходе мы должны получить Y=11001001.

Это свойство сети Фейстела определило на десятилетия популярность данного алгоритма блочного шифрования. В этом примере представлена упрощенная версия сети Фейстела.

Рис. 2. Модель сети Фейстела (заполненная)

Описываемое задание способствует формированию у курсантов четкого понимания организации блочного асимметричного шифрования. Выполнение практических упражнений, направленных на построение математических моделей способствует развитию технических качеств сотрудника правоохранительных органов.

УДК 378.635

***В.В. Цыбулько**, старший преподаватель кафедры тактики и вооружения войсковой противовоздушной обороны факультета противовоздушной обороны Военной академии Республики Беларусь*

ДЕЛОВАЯ ИГРА КАК ФОРМА ПОЛУЧЕНИЯ ЗНАНИЙ В ВЫСШЕМ ВОЕННОМ УЧЕБНОМ ЗАВЕДЕНИИ

В современных условиях развития профессиональной деятельности офицеров, при непрерывном повышении уровня ее сложности, внедрения новых подходов к ведению боевых действий, принятии на вооружение новых систем вооружения, определяющими становятся задачи по подготовке специалистов, обладающих глубокими знаниями, высоким уровнем образования и культуры, способных уверенно действовать в сложных условиях быстроменяющейся обстановки.

Современная методика преподавания дисциплин специальности в военном учебном заведении имеет богатый арсенал разнообразных способов, приемов и средств обучения, в том числе и инновационных. При этом исходя из современных требований, предъявляемых к системе образования, педагогам в своей деятельности следует максимально использовать инновационные технологии, так как традиционная лекционно-семинарская и классно-урочная формы обучения не всегда позволяют обеспечить достижения актуальных образовательных результатов, сформировать компетенции, и поэтому необходимы разработка, апробация и теоретическое осмысление принципиально новых дидактических решений.

Следует остановиться на такой инновационной форме получения знаний обучающимися, как деловая игра. Деловая игра является одним из видов активных методов обучения – методов, которые побуждают обучающихся к активной мыслительной и практической деятельности в процессе овладения учебным материалом. Активное обучение предполагает использование такой системы методов, которая направлена главным образом не на подачу педагогом готовых знаний, их запоминание и воспроизведение, а на самостоятельное овладение обучающимся зна-