персональных данных и клиентских баз; защиты интеллектуальной собственности; применения целевых политик контроля персонала, входящего в т.н. «группы риска»; расследования инцидентов информационной безопасности и пр.

Выполнена настройка конфигурации его баз контекстной фильтрации, шаблонов, цифровых отпечатков в соответствии с требованиями системы менеджмента университета, ведется формирование и отслеживание учебной базы данных инцидентов.

О ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВОЕННОМ ВУЗЕ

Л. В. Михайловская, Е. В. Валаханович

Современные тенденции развития инженерных технологий требуют адекватной корректировки содержания процесса преподавания дисциплин, изучающих средства и методы информационной безопасности, формирующих высокий уровень подготовки будущего специалиста.

В военно-инженерном вузе в большей степени, чем в гражданском вузе, необходимо создание особой педагогической технологии, позволяющей по возможности снизить неблагоприятное влияние факторов, связанных с особенностями обучения курсантов, таких как: объективной необходимости пропуска занятий курсантами, ограничением времени на самостоятельную подготовку, приоритетом физической подготовки по отношению к общеобразовательной.

В целях уменьшения влияния вышеперечисленных факторов на процесс обучения в области информационной безопасности в Военной академии Республики Беларусь на кафедре высшей математики разработан электронный учебно-методический комплекс (ЭУМК) по дисциплинам «Прикладная математика» и «Защита информации».

В частности, ЭУМК содержит цикл лабораторных работ, позволяющий курсантам закрепить теоретический курс и самостоятельно совершенствовать свои силы по взлому современных криптографических систем различной степени сложности. ЭУМК является сетевым ресурсом, доступным в полном объеме для обучаемых, позволяющий курсантам самостоятельно изучить учебные вопросы, следуя подсказкам и пояснениям. Данный комплекс, кроме того, служит действенным инструментом для углубленного изучения предмета. Следует отметить возможности оперативной модификации учебного материала в ЭУМК и построения индивидуальной траектории обучения для каждого курсанта, что позволяет осуществлять качественную подготовку военных инженерных кадров адекватно требованиям времени и современным тенденциям развития технологий.

СТАНДАРТ ШИФРОВАНИЯ AES В УЧЕБНОМ ПРОЦЕССЕ

В. А. Липницкий, Л. В. Михайловская

В 2001 году в западном мире стандарт шифрования DES канул в лету и был заменен новым стандартом AES (Advanced Encription Standart). Почти пятнадцатилетний практический опыт работы с этим стандартом демонстрирует его полную надежность и криптографическую стойкость.

DES и AES относятся к одному классу систем шифрования с закрытыми ключами. Это - поточные шифры, применяемые в быстрых системах передачи информации. В отличие от DES, который работает с небольшими блоками информации в 32 бит, AES за один такт обрабатывает в 4 раза больший блок двоичной информации. Основу DES составляют комбинаторные преобразователи, в криптосистеме AES задействованы методы, ориентированные на применение современной вычислительной техники. Обрабатываемый блок разбивается в матрицу 4x4, элементы которой в процессе работы алгоритма представляются в виде двоичных байт, двузначных шестнадцатеричных чисел, полиномами с коэффициентами из Z/2Z – элементами поля Галуа из Z/2Z. Каждая форма соответствует своему классу криптографических преобразований. Сильное рассеивание и