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

перемешивание, обеспеченные комбинацией преобразований SubByte, ShiftRows и MixColumns, удаляют любую частотную закономерность в исходном тексте. AES может быть реализован в программном обеспечении, аппаратных средствах и программируемом оборудовании. Нынешние вычислительные технологии не способны за какое-либо приемлемое время справиться со взломом.

Наличие сложных алгебраических операций и невозможность использования алгоритма на блоках меньшей длины, как это делается в криптосистемах RSA, Эль Гамаля и других, требуют применения компьютерных средств для успешного изучения работы данного алгоритма. На кафедре высшей математики учреждения образования «Военная академия Республики Беларусь» разработана модель лабораторной работы со всем комплексом поддерживающих компьютерных программ для практического освоения стандартов AES курсантами IT-специальностей.

ОБЕСПЕЧЕНИЕ ПОДГОТОВКИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПЕРВОЙ СТУПЕНИ ВЫСШЕГО ОБРАЗОВАНИЯ В РАМКАХ СПЕЦИАЛЬНОСТИ «АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ»

А.В. Ломако

Согласно новому образовательному стандарту Республики Беларусь по специальности 1-53 01 02 «Автоматизированные системы обработки информации» (далее АСОИ) одним из основных требований к профессиональным компетенциям специалиста на первой ступени высшего образования является умение выявлять и устранять уязвимость систем обработки информации к угрозам безопасности. Учитывая специфику современных АСОИ, важно уметь обеспечивать безопасность данных, то есть защиту от преднамеренного или непреднамеренного нарушения их секретности, искажения или разрушения. Это особенно важно для АСОИ 4-го поколения, работающих в глобальных сетях в режиме коллективной работы с данными с использованием технологий распределенной и параллельной обработки и хранения информации и являющихся гибкими адаптивными интегрированными системами с элементами искусственного интеллекта.

Обеспечение информационной безопасности является сложной системной задачей, решению которой разработчики и пользователи АСОИ должны уделять большое внимание. Соответствующие компетенции, т.е. знания, умения и навыки, студенты специальности АСОИ получают в ходе изучения целого ряда общепрофессиональных и специальных учебных дисциплин, а также дисциплин специализации. В докладе приводится перечень и характеристика таких дисциплин, включенных в состав государственного компонента и компонента учреждения высшего образования учебного плана специальности АСОИ. При этом отмечается, что общие методологические основы информационной безопасности закладываются в рамках дисциплины «Основы защиты информации».

Качество подготовки студентов специальности АСОИ в области информационной безопасности будет проверено на практике в 2017 году, на который намечен первый выпуск молодых специалистов, обучавшихся по новому образовательному стандарту.

ПРИМЕНЕНИЕ ТРЕНАЖЕРНЫХ КОМПЛЕКСОВ ПРИ ПОДГОТОВКЕ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.С. Белый Е.И. Михненок Е.И. Хижняк

В настоящее время информационные технологии глубоко проникают во все сферы человеческой деятельности. Их применение позволяет упростить выполнение многих задач в процессе функционирования систем. Подготовка специалистов в области обеспечения безопасности информации в военной сфере является актуальной задачей.

С целью повышения качества подготовки специалистов в области защиты информации на кафедре автоматизированных систем управления войсками Военной академии Республики Беларусь в учебный процесс введен «Имитатор-тренажер безопасности информационно-