

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. Современные 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 Гамала 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. Михненко 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-