результаты. Алгоритмы RSA-3072 и AES-128 значительно (примерно в 3 раза) меньше используют память программ по сравнению с ECIES-256. Однако для памяти данных AES-128 уже не имеет такого значительного преимущества по сравнению с ECIES-256 (выигрыш приблизительно в полтора раза). RSA-3072 требует в 3,5 раз больше памяти данных по сравнению с ECIES-256 и в 5,4 раза больше по сравнению с AES-128. Для успешного запуска RSA-3072 требуются микроконтроллеры с минимум 32 КБ памяти.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОРГАНАХ И ПОДРАЗДЕЛЕНИЯХ ПО ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ РЕСПУБЛИКИ БЕЛАРУСЬ

С.Ю. Воробьёв, В.А. Русак

В XXI веке трудно найти какую-либо область из жизни общества, где бы не использовались способы обработки и передачи информации [1]. Информационная сфера Республики Беларусь стремительно развивается. По мере совершенствования и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых информационных технологий [2]. Наибольшую общественную опасность представляют правонарушения, связанные с неправомерным доступом к компьютерной информации. Требования к обеспечению технической защиты информации в органах и подразделениях по чрезвычайным ситуациям Республики Беларусь изложены в приказе МЧС от 11.03.2016 № 64 «Об информационной безопасности». Необходимо отметить усиление опасности несанкционированного доступа к компьютерной информации в связи с ростом различного способа использования компьютерных систем и сетей в органах государственного управления и государственных организациях.

Список литературы

1. Лемешевский О.О. Актуальные вопросы информационной безопасности на факультете внутренних войск МВД Республики Беларусь // Матер. междунар. науч.-практ. конф. «Теоретические и прикладные проблемы информационной безопасности». Минск, 18 мая 2018 г. С. 36–38.

2. Чижиков Э.Н. Защита информации в информационных системах МЧС России // Темат. сб. «Информационные технологии, связь и защита информации МВД России». Москва, 2012. С. 14–17.

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ БЕЗОПАСНОСТИ

А.А. Гавришев, А.П. Жук

Авторами в работе [1] разработан обобщенный алгоритм защищенного информационного обмена в беспроводных системах безопасности. В работе [2] на основании работы [1] разработан усовершенствованный алгоритм защищенного информационного обмена с усложненной имитовставкой, состоящий из следующих шагов. 1. Инициализация генератора ПСП-1 управляющего блока. 2. Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока, и его отправка на генератор ПСП-2 блока контроля и в блок логической операции XOR. 3. Выбор из таблицы уникальных идентификационных данных (УИД) одного уникального значения, присвоенного каждому контролируемому объекту. 4. Сложение по правилу XOR значений первой ПСП-1 блока контроля и УИД выбранного контролируемого объекта. 5. Отправка полученного значения в накопитель хаотической последовательности (НХП), где оно перемножается с хаотическим сигналом (ХС), и передача полученного произведения на контролируемый объект. 6. Декодирование в контролируемом объекте полученного сигнала с помощью накопителя копии хаотической последовательности (НКХП), идентичного НХП в управляющем блоке. 7. Поступление декодированного сигнала в блок логической операции XOR контролируемого объекта, в который одновременно с этим приходит индивидуальное