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

значение УИД контролируемого объекта. 8. Получение в блоке логической операции XOR контролируемого объекта значения ПСП-1 блока контроля и его поступление в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока. 9. Выработка в генераторе ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока, последовательности ПСП-2. 10. Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок. 11. Декодирование в управляющем блоке полученного сигнала с помощью НКХП, идентичного НХП в контролируемом объекте. 12. Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в УС. 13. Выработка ПСП-2 управляющего блока и ее поступление в УС. 14. Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта. 15. Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма. 16. Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 17 алгоритма. 17. Вмешательство в работу беспроводной системы безопасности персонала (ответственных лиц).

Список литературы

1. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена // Вестник СибГУТИ. 2018. № 1. С. 33–40.

2. Гавришев А.А., Жук А.П. Обобщенный алгоритм защищенного информационного обмена для беспроводных систем безопасности с усложненной имитовставкой // Вестник НГУ. 2019. Т. 17, № 1. С. 18–27.

ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРОЕКТИРОВАНИЮ УСТАНОВОК ДЫМОУДАЛЕНИЯ

В.Е. Галузо, В.В. Мельничук, А.И. Пинаев

При проектировании в соответствии с [1] установок дымоудаления (ДУ) в составе систем противодымной защиты (ПДЗ) в первую очередь определяется весовой, а затем объемный расход удаляемой газодымомвой смеси $L_Д$. Значение последнего определяется при нормированном [1] значении температуры удаляемых газов (более 300 °С) для подбора вентилятора. Кроме $L_Д$ для подбора вентилятора необходимо значение падения давления в сети $P_С$ установки ДУ. Давление $P_С$ рассчитывается в соответствии с [1] с учетом естественного давления газов $P_{ЕС}$, определяемого разностью удельных весов наружного воздуха и дыма (при температуре более 300 °С) и высотой шахты. При высоте шахты (здания) 50 м $P_{ЕС} \approx 300$ Па. Это давление вычитается из расчетного давления $P_С$ установки ДУ. Аэродинамические испытания установок ДУ проводятся при нормальной температуре в помещении (менее 30 °С) и параметрах Б [2] для теплого периода года для данного региона (26 °С для г. Минска). При таких температурах удельные веса удаляемого из помещения и наружного воздуха отличаются незначительно и давление $P_{ЕС}$ составляет единицы Па, и им можно пренебречь. То есть измерения объемного расхода газа, удаляемого установкой ДУ проводятся при давлении в сети отличающегося от проектного значения, а значит производительность вентилятора и объемные расходы будут отличаться, что может привести к тому, что измеренное значение объемного расхода воздуха $L_В$ будет существенно отличаться от проектного $L_Д$ (более 20 % [3]), что может быть причиной принятия решения о непригодности установки ДУ для эксплуатации.

Предлагается при проектировании установок ДУ выбор вентилятора осуществлять с учетом давления газов $P_{ЕС}$ при нормируемой температуре дыма (более 300 °С). Затем по аэродинамической характеристике выбранного вентилятора определять объемный расход удаляемого установкой воздуха при давлении в сети без учета давления $P_{ЕС}$ газов (воздуха). На основании чего определять объемный расход удаляемого через клапан ДУ воздуха $L_В$.