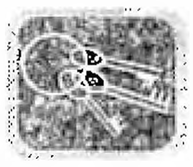

Администратор заглянул под стол и в который раз убедился, что ящик из-под пива пуст. "А хорошо погуляли, когда инвентаризацию с девчонками из бухгалтерии обмывали. Жалко только, что больше такого повода не будет". Тем не менее мысль о том, что ему больше не придётся бродить в составе инвентаризационной комиссии по всем закоулкам нескольких зданий, приносила ему удовольствие. Он даже стал забывать о том, что инвентаризационные данные автоматически поступают из базы Директора в бухгалтерию.

"А все-таки наше пиво лучше, чем немецкое". Немецким пивом его угощали в дочерней организации, когда он приезжал в командировку помочь настроить Директора. Да и теперь иногда Администратор через Интернет помогал коллегам управлять Директором. Он быстро развеял сомнения службы безопасности на этот счет, спросив, сколько времени понадобится, чтобы поломать ключ длиной в 1024 бит.

В бегущей строке консоли появилось сообщение: "Обнаружен новый объект управления, идет установка стандартного пакета приложений, создана учетная запись в базе данных Domino". Администратор ткнул мышкой в пункт меню View Inventory и удовлетворенно пробормотал: "Это хорошо, что Etherexpress Pro стали ставить. Ее родной модуль Директору обо всем расскажет".

"Какой все-таки буржуи ленивый народ", - посетовал про себя Администратор, устроился поудобнее в офисном кресле и задремал…

Н.В. ПАЦЕЙ, П.П. УРБАНОВИЧ

Белорусский государственный технологический университет
(г. Минск)

МЕТОД ПОСТРОЕНИЯ КРИПТО-КОРРЕКТИРУЮЩИХ СИСТЕМ НА ОСНОВЕ СВЕРТОЧНЫХ КОДОВ

1. Для установления конфиденциальной и целостной коммуникационной связи к криптографической системе защиты информации добавляют механизмы помехоустойчивого кодирования. В большинстве случаев распространена упаковка зашифрованных данных в корректирующий ошибки конверт. Однако, по-прежнему мало изучена интеграция алгоритмов шифрования и корректирующих кодов.

2. Авторами предлагается метод построения корректирующей крипто-системы, при котором корректирующее кодирование будет являться частью спецификации криптосистемы.

Система основана на несистематическом линейном древовидном коде (n_0, k_0). задаваемом множеством порождающих многочленов $g_{ij}(x), i = 1,\ldots,k_0, j = 1,\ldots,n_0$.

Тогда операция кодирования/шифрования выглядит следующим образом:

$$c_j(x) = \sum_{i=1}^{k_0} d_i(x) F(k_m(x)) g_{ij}(x),$$

где $d_i(x), i = 1,\ldots,k_0$ - входной инфор-мационный многочлен;

$k_m(x), m \le i$ - многочлен ключевой последова-

довательности;

$c_j(x)$ - избыточный шифротекст.

Отличительной чертой данной крипто-корректирующей системы является функция расширения F, которая является своего рода криптографическим элементом системы.

Объединение функции расширения F с порождающими многочленами $g_{ij}(x)$ эквивалентно новым порождающим многочленам, в дальнейшем обозначаемым как $\Phi = \|\phi_{ij}(x)\|$, а выход кодера/шифратора Φ дает шифротекст c, который передается по каналам связи.

В результате передачи в зашумленной среде к исходному шифротексту добавляется аддитивная шумовая последовательность z:

$$\nu = c + z.$$

Поступающая на приемник версия шифротекста ν рассматривается как искаженная помехами выходная последовательность эквивалентного сверточного кодера $\Phi = [\phi_{ij}(x)] = \sum_{i=0}^{k_0} F(k_m(x))g_{ij}(x)$.

Последовательное декодирование/дешифрование, корректирующее и восстанавливающее исходную информационную последовательность $d_i(x)$, основано на алгоритме Фано, преобразованном с учетом функции расширения F.

3. Достоинствами криптокорректирующей системы является ее способность восстановления сильно искаженного шифротекста без необходимости повторной передачи информации. Схемы прямого и обратного преобразования легко аппаратно реализуются на регистрах сдвига и логических схемах.

Основной недостаток представленной системы: увеличение размера зашифрованного и закодированного текста в результате введения избыточности, что влияет на стойкость криптокода и быстродействие системы. Однако учитывая скорость современных коммутируемых и выделенных абонентских каналов, такое преобразование данных будет прозрачным для пользователей.

4. Для оценки рассмотренной техники преобразований была рассчитана количественная величина эффективности на основе сравнения систем, выполняющих более или менее одинаковые функции. Сравнение проводилось с программно-аппаратной системой "ШИП" МО ПНИ. В рассмотрение вводились различные параметры с выбранными весовыми коэффициентами. В данном случае к наиболее важным параметрам системы отнесли пропускную способность и помехоустойчивость - они в достаточной степени определяют общетехническую характеристику системы и их можно считать равно существенными. Согласно выполненным расчетам эффективность крипто-корректирующей системы в зашумленной среде на 17-21% превосходит эффективность системы "ШИП", использующей криптографические преобразования без коррекции ошибок.

5. Таким образом, построенные на основе данного метода крипто-корректирующие системы могут использоваться вместо традиционных систем и протоколов защиты информации в критических участках сети, что подтверждается получаемым при этом эффектом.