УДК 681.3

Кравцов Г.А., директор ООО «НВФ «БКП-Консалтинг», г.Киев.

Криптографическая защита банковских чеков

Методы криптографической защиты доказали свою необходимость в эпоху всеобщей информатизации. Сегодня нам известно, что криптографию применяют в защищенных системах связи независимо от среды и способа передачи. Однако этим не ограничивается область применения математических методов защиты информации.

Рост технологий способствует росту изощренных методов подлога банковских документов, таких как денежные купюры, чеки, векселя.

Обратимся к открытой печати: «Рост убытков от подделки чеков побудил британскую Ассоциацию межбанковских расчетных служб (Association for Payment Clearing Services, APACS) разработать и внедрить через компанию Cheque and Credit Clearing Company (CCCC) схему аккредитации изготовителей чеков (Cheque Printer Accreditation Scheme). Цель этого шага - обеспечить соответствие всех чеков, которые будут печататься с начала 1996 г., "стандарту 3" APACS, регламентирующему их дизайн. Компаниям и типографиям рассылаются приглашения присоединиться к этой схеме.

За период с 1991 по 1993 г. убытки от подделки чеков составили 40 млн. ф. ст., и еще на 280 млн. подделок было раскрыто. Убытки от подделки чеков за 1994 г. оцениваются в 13 млн. ф. ст. (хотя некоторые специалисты считают, что эта цифра занижена), а раскрыто было подделок на 55 млн., причем число подделок чеков в 1994 г. было примерно вдвое больше, чем в 1993 г. »

В статье рассматривается один из вариантов применения криптографии для чеков.

Какое же количество степеней защиты с точки зрения криптографии должно быть у чека? Ответить на данных вопрос помогут обыкновенные расчеты. Пусть на 2050 год население Земли составит 9 млрд.человек. Пусть каждый обеспечен компьютером с тактовой частотой 2 ГГц, что по максимальным показателям соответствует 100 млн. итераций в секунду. Количество секунд в году по грубым подсчетам составляет $4 \cdot 10^7$ секунд. Один такой компьютер может совершить $3{,}2 \cdot 10^{15}$ итераций за год. Общее число итераций 9 млрд. компьютеров за 100 лет составляет $3{,}6 \cdot 10^{22}$ итераций. Легко показать, что количество степеней защиты эквивалентно $\log_2(3{,}6 \cdot 10^{22}) \approx 74$.

Итак, стало известно, что для полноценной защиты чека на 100 лет необходимо предусмотреть минимум 74 степени защиты. Как же обеспечить такое большое число степеней защиты на небольшом по линейным размерам чеке.

Для реализации указанного выше числа степеней защиты достаточно использовать признак присутствия в виде отверстия, достаточного для считывания сканером. Так, если R радиус отверстия присутствия, то линейные размеры защитной области можно определить по формуле: $L = 3R(n-1) + 2R$, где n-количество позиций. Например, если радиус признака присутствия 2 мм, то для реализации 100 признаков (10 строк и 10 столбцов) необходимо задействовать площадь 60x60 мм. Однако концентрация признаков присутствия не обязательна в одном сосредоточенном месте. Участков для нанесения такой защиты может быть несколько. В 100 признаках присутствия с плотностью 30% может быть записано 11 чисел от 0 до 9. Если в зашифрованном виде, используя дополнительно функцию Уолша, разместить номер чека, то необходимо перебрать 10^{30} вариантов, что невозможно сделать и за 120 лет.

Такую защиту могут наносить в Главных офисах банков и хранить код к каждому чеку для проверки не только на стандартных бланках чеков, но и на бланках корпоративных чеков, которые могут принести банкам дополнительную прибыль от легализации таких чеков и их учета.

Библиография.

1.Дерек Остин. APACS вводит стандарты на чеки. Издание в Интернет (http://www.bizcom.ru/rus/bt/1995/nr4/05.htm).

Григорий А. Кравцов

Digitally signed by Григорий А. Кравцов
DN: cn=Григорий А. Кравцов, ou=SMTP, dc=org
Reason: I am the author of this document
Date: 2006.01.18 11:29:56 +02'00'