УДК 681.3+681.5:007

И.Н. АЛИПОВ, Л.Н. РЕБЕЗЮК, канд. техн. наук

ПОСТАНОВКА ЗАДАЧ СИНТЕЗА НОВЫХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Информация всегда была, есть и будет одной из самых больших ценностей. Создание ЭВМ и их использование в любых областях науки и производства дают возможность хранить и передавать значительные объемы информации. Однако "возрастающие объемы хранимых и передаваемых данных; расширение круга пользователей, имеющих доступ к ресурсам ЭВМ, программам и данным; усложнение режимов эксплуатации вычислительных систем"[1] привели к тому, что информация становится все более уязвимой. Поэтому защита информации в ЭВМ и сетях ЭВМ приобретает все большее значение [2].

В работе [1] под защитой информации понимается защита от несанкционированного доступа (НСД) при передаче и хранении. Она включает совокупность мероприятий, методов и средств, обеспечивающих: исключение НСД к ресурсам ЭВМ, программам и дискам; проверку целостности информации; исключение несанкционированного использования программ. Далее термин "защита информации" использован именно в этой трактовке.

Первоначально для защиты данных при хранении и передаче применялось несколько групп методов. Так, для защиты информации в статистических базах данных использовались методы, основанные на выдаче на запрос некоторого числа, которое представляло собой сумму интересующего значения и значения случайной величины, распределенной по определенному закону [3; 4]. Использовались также пароли [5], генерация которых осуществлялась датчиком псевдослучайных чисел [6].

Для защиты информации при ее передаче применялись криптографические методы [7 – 9]. В работе [10] впервые отмечено, что хищение информации при ее передаче предотвращается только криптографическими методами. Их можно использовать при защите баз данных. В настоящее время эти методы применяются как при хранении информации, так и при ее передаче [8; 11]. Далее в основном рассматриваются именно криптографические методы.

К ним предъявляют следующие требования [10]:

— надежность (невозможность восстановления текста без ключа);
— небольшой объем ключа;
— простота шифрования и дешифрования;

— объем шифротекста не может быть значительно больше объе-
ма открытого текста;

— ошибки текста не должны размножаться.

Развитие техники передачи и преобразования информации зна-
чительно смягчило все эти требования, кроме первого. В то же время
требования к надежности ужесточились в силу использования быстро-
действующих ЭВМ при попытках НСД [10]. Применение ЭВМ выдви-
нуло и новые требования [12]:

— шифрование и дешифрование каждой записи должно произ-
водиться независимо от других записей;

— все операции с файлом необходимо производить в зашифро-
ванном виде.

Криптографические методы включают перестановки, подста-
новки и аддитивные методы [13].

При подстановках по некоторому правилу блок открытого тек-
ста заменяется блоком шифротекста. Так, шифр Цезаря заключался в
том, что каждая буква в сообщении заменялась буквой алфавита,
отстоящей от нее на фиксированное число букв. Этот шифр довольно
просто разгадывали: достаточно было узнать лишь величину цикли-
ческого сдвига (ключ), которая постоянна для всех букв.

В 1926 г. инженер Б. Вернам (Германия) предложил нераскры-
ваемый шифр [14]. Идея шифра состоит в том, что для каждой новой
подстановки выбрано новое значение циклического сдвига. Другими
словами, секретный ключ должен применяться только один раз. Если
такой ключ выбирается случайным образом, то, как доказал Шеннон
в 1949 г., шифр является нераскрываемым [15]. Но длина данного клю-
ча соизмерима с длиной открытого текста и наряду с шифротекстом
необходимо передать ключ. Обмен ключами размером с шифруемую
информацию не всегда практически возможен. Поэтому чаще испол-
зуют псевдослучайную последовательность, вырабатываемую датчи-
ком псевдослучайных чисел (ПСЧ). В этом случае ключом является
начальное значение датчика ПСЧ [16]. Однако наличие длинных псев-
дослучайных последовательностей затрудняет извлечение отдельных
записей из файлов и внесение новых изменений, поскольку в этих
случаях нельзя обойтись без дешифрования и шифрования всего
файла. Поэтому в системах защиты применяют более короткие ключи
[1; 17]. Поскольку генераторами ключей служат датчики ПСЧ, возни-
кает необходимость при повторном обращении к датчику изменять
его начальное состояние. В современных системах защиты [11; 16; 18]
распространены так называемые корректные датчики ПСЧ. Датчик
называется корректным, если наблюдение фрагментов его выхода не
позволяет восстановить пропущенные части или всю последователь-
ность при известном алгоритме, но неизвестном начальном значении.

При этом возможны [16] следующие варианты использования датчика ПСЧ. Цифровой ключ является начальным значением датчика ПСЧ, выходной поток бит суммируется по модулю два с исходной цифровой информацией; побитовое шифрование потока данных осуществляется с обратной связью по шифротексту или исходному тексту. Такое управление датчиком ПСЧ хотя и вносит некоторую неопределенность, но не настолько, чтобы шифр считался нераскрываемым.

При перестановках элементы открытого текста (буквы, биты, символы, фрагменты) переставляются в некотором новом порядке. В этом случае ключом является порядок замены элементов друг на друга. Надежность такого способа не выше, чем при употреблении простых паролей. В современных криптографических системах, как правило, используют и перестановки, и подстановки [1].

При аддитивных методах (гаммировании [1]) на открытый текст накладывается псевдослучайная последовательность по определенному правилу. Обычно применяют поэлементное сложение по модулю два. При расшифровании на шифротекст накладывается известная псевдослучайная последовательность, которая вырабатывается датчиком ПСЧ. При этом так же, как при перестановках, возникает проблема управления датчиком ПСЧ: необходимо каким-то образом передавать его начальное значение (ключ). Надежность этого метода шифрования не выше, чем надежность пароля (паролем в данном случае служит начальное состояние датчика ПСЧ).

Рассмотренные методы называют симметричными. Существуют и несимметричные методы с открытым ключом (Диффи-Хеллмана, Райвеста-Шамира-Алдермана, Эль-Гамаля). Однако в правительственных и военных системах связи используют лишь симметричные методы. Федеральный стандарт США DES [8; 18] на шифрование данных и стандарт России включают описанные алгоритмы шифрования. Стандарт России на шифрование информации реализован программно и аппаратно [19; 20].

Направления совершенствования методов защиты информации следуют из формулы Шеннона [15]

$$N_1 = H(z)/r \log_2 N,$$

где N_1 – количество знаков шифротекста, получив которые криптоаналитик при неограниченных ресурсах может восстановить ключ; $H(z)$ – энтропия ключа z; r – избыточность открытого текста; N – объем алфавита.

Первое направление (как это видно из формулы) связано с уменьшением избыточности открытого текста; второе — с увеличением энтропии ключа. Существующие системы защиты информации в

основном реализуют методы, дающие с уменьшение избыточности, увеличение размера ключа и количества циклов шифрования [1]. Методы защиты информации второго направления недостаточно хорошо развиты (увеличивают размер ключа и количество циклов шифрования). В рамках второго направления одним из перспективных является поднаправление, связанное с теорией конечных автоматов [21].

Как следует из работы [22], функционирование конечного (дискретного) автомата задается алгоритмом в виде направленного графа. Последний должен иметь одну вершину, отождествленную с начальным состоянием автомата, и N вершин, однозначно поставленных в соответствие конечным состояниям автомата; каждое конечное состояние автомата взаимно однозначно соответствует определенному символу входного алфавита. Такие автоматы в работе [23] названы деревообразными. Их функционирование осуществляется на основании алгоритмов одномерного поиска точки на отрезке единичной длины в условиях помех [24]. Поскольку в процессе поиска действуют помехи, переход деревообразного автомата из начального состояния в одно конечное выполняется различными маршрутами. Каждому маршруту соответствует определенная совокупность значений выходного сигнала индикаторного элемента (компаратора) [24]. В том случае, когда в процессе поиска используется один компаратор, совокупность его значений представляет собой двоичную кодовую комбинацию. Эти двоичные комбинации имеют разную длину, зависящую от того, на каком шаге действовала помеха [25]. Следовательно, одному и тому же символу отвечает множество двоичных комбинаций различной длины. Выбор комбинаций осуществляется псевдослучайным образом. Все это способствует повышению энтропии ключа.

Особая важность (оригинальность) в описанных алгоритмах заключается в том, что помеха, накладываемая на процесс поиска, физически не существует (программно данный недостаток восполним). Уже известны некоторые такие помехи, называемые A_1, A_2 - последовательностями [25]. Поэтому задача синтеза новых помехоустойчивых алгоритмов одномерного поиска точки экстремума унимодальной функции разделяется на ряд подзадач синтеза алгоритмов, помехоустойчивых к определенному классу виртуальных помех. Решением задачи синтеза помехоустойчивых алгоритмов поиска являются оптимальные алгоритмы поиска, отличающиеся высокой логической сложностью. Последняя вносит значительную неопределенность, что повышает энтропию ключа. Для защиты менее ценной информации можно использовать более простые алгоритмы, называемые логически несложными. Поэтому возникает новая задача — синтеза логически несложных помехоустойчивых алгоритмов одномерного поиска точки экстремума унимодальной функции.

В работе [25] показано, что любой помехоустойчивый алгоритм поиска точки на отрезке единичной длины порождает свои избыточные системы представления десятичных чисел. Названные системы могут быть использованы также для защиты информации (они определяются параметрами виртуальных помех). Поэтому возникают новые задачи: синтеза методов защиты информации на основе дискретных автоматов, задаваемых алгоритмами поиска, и методов на основе труднопредставимых избыточных систем, порождаемых помехоустойчивыми алгоритмами поиска.

Список литературы: 1. *Новосельский А.* Алгоритмы шифрования // Компьютеры + прогр. 1996. № 5. С. 70 — 77. 2. *Казаров М.С.* Защита информации в банках данных // Зарубеж. радиоэлектроника. 1979. № 12. С. 46 — 67. 3. *Beck L.L.* A security mechanism for statistical databases // ACM trans. database systems. 1980. V. 5, N 3. P. 316 — 338. 4. *Stonebraker M.* Retrospection on a database system // ACM trans. database systems. 1970. N 2. P. 225 — 240. 5. *Anderson J.P.* Information security in multi-user computer environment // Advances in computer. 1972. V. 12. P. 53 — 67. 6. *Saltrer T.H.* Protection and control of information sharing in multics // Communs. ACM. 1974. V. 17, N 7. P. 388 — 402. 7. *Герасимов В.С., Владиславский В.А.* Криптографические методы защиты информации в автоматизированных системах // Зарубеж. радиоэлекроника. 1975. № 6. С. 53 — 58. 8. *Защита* информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков и др. М.: Радио и связь, 1992. 280 с. 9. *Kent S.T.* Encryption based protection protocols for interactive user — computer communication. Cambridge: Massachusetts Inst. of technology, 1976. 121p. (Lab. computer sci. technologies rep.; N 102). 10. *Файстель Х., Нотц У.А., Смит Дж.А.* Криптографические методы в межмашинном обмене информацией // ТИИЭР. 1975. Т. 63, № 11. С. 10 — 21. 11. *ГОСТ 28147 - 89.* Система обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. Введ. 01.01.90. 12. *Budes E., Koch H.S., Stahl F.A.* Theapplication of cryptography for database security // AFIPS conf. proc. 1976. V. 45. P. 97 — 107. 13. *Burris H.R.* Computer networkcryptography engineering // AFIPS conf. proc. 1976. V. 45. P. 91 — 96. 14.*Vernam B.S.* Cipher printing telegraph systems for secret wire and radio-telegraphic communication // Amer. just. eleer. eng. 1926. V. 42, N 2. P. 109 — 115. 15. *Шеннон К.* Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике: Пер. с англ. М.: Иностр. лит., 1963. С. 333 — 402. 16. *Мафтин С.* Механизмы защиты в сетях ЭВМ: Пер. с англ. М.: Мир, 1993. 310 с. 17. *Курмит А.А.* Криптографические методы защиты информации в системах ЭВМ // Зарубеж. радиоэлектроника. 1979. № 7. С. 17 —41. 18. *Водолазский В.В.* Коммерческие системы шифрования: основные алгоритмы и их реализация Ч. 1 // Монитор. 1992. № 6 —7. С. 14 — 19. 19. *Игнатенко Ю.И.* Как сделать так, чтобы?.. // Мир ПК. 1994. № 8. С. 52 — 54. 20. *Шмелева А.* Грим — что это? // Hard'n'soft. 1994. № 5. С. 22 — 26. 21. *Ecker A.* Abstrakte kryptographische Maschinen // Angew. Informatik. 1975. Bd. 17, Nr 5. S. 201 — 205. 22. *Глушков В.М.* Синтез цифровых автоматов. М.: Физматгиз, 1962. 476 с. 23. *Стахов А.П., Алипов Н.В.* Метод структурного синтеза деревообразных автоматов // Приборы и системы автоматики. Х., 1969. Вып. 12. С. 86 — 91. 24. *Алипов Н.В.* Алгоритмы измерения напряжений в условиях действия флуктуационных помех // Преобразование и передача информации: Сб. науч. тр. К., 1973. С. 3 — 16. 25. *Арифметика,* принципы организации диагностики и формализованное проектирование вычислительных структур и устройств / В.П. Тарасенко, Н.В. Черкасский, Ю.С. Каневский и др. К.: Выща шк., 1989. 343 с.

Поступила в редколлегию 25.03.97