Список литературы:

1. *К.Шеннон* "Теория связи в секретных системах". Москва: Иностранная Литература ,1963, с. 332 - 402.
2. *W. Diffie, M.E. Hellman* "New directions in cryptography". IEEE Trans.Informat.Theory, Vol. IT-22, pp, 644-654, Nov. 1976
3. *У.Диффи* "Первые десять лет криптографии с открытым ключом " В кн.: Тематический выпуск " Защита информации ". ТИИЭР , 1988 , № 5,с. 54-73.
4. *К.Ю. Гундарь., А.Ю. Гундарь, Д.А. Янишевский* "Защита информации в компьютерных системах". Киев: Корнейчук. 2000

5.Use of a taxonomy of security faults. COAST Laboratory, Purdue University, Technical report TR-96-051.

6.Abbott R.,Chin J. Security analysis and enhancements of computer operating system. NBSIR 76-1041, National Bureau of Standarts, ICST, April 1976.

7.Landwehr C, Bull A.,McDermott J A taxonometry of computer security flaws, with examples.Information Technology Division, code 5542, Naval research laboratory, Washington D.C., 20375-5337.

8.Leveson N., Turner C.S. An investigation of the Therac-25 accidents. UCI TR92-108, Inf. And Comp. Sci. Dept.,of Cal-Irvine, Irvine, CA.

Поступила 15.12.2001
После доработки 18.01.2002

УДК 621.391

Гороховский А.И.

ОБ ОДНОМ ПОДХОДЕ К КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ

Термин "компьютерная преступность" впервые появился в американских, а потом и в других зарубежных изданиях в начале 60-х годов. По мнению криминологов, ЭВМ в наше время многообещающее оружие проведения корыстных преступлений. Кроме преимуществ современных информационных технологий, компьютеризация несет в себе ряд отрицательных последствий, которые сегодня, к сожалению, практически остаются вне законодательного и правового поля Украины.

Перечень компьютерных преступлений в настоящее время стал значительно шире. Среди наиболее распространенных - воровство денег, материальных ценностей, машинной информации, машинного времени, несанкционированное использование системы, саботаж и вандализм. Воровство денег в электронных банковских системах взаиморасчетов составляет 45% всех преступлений, связанных с использованием ЭВМ. И только 10-15% компьютерных преступников становятся известными. Одной из причин этого становится то, что многие пострадавшие организации не сообщают о них из-за боязни потерять свою репутацию или совершения повторных преступлений.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Отдельно встает вопрос о защите авторских прав на информационные продукты: программы, алгоритмы, данные, результаты.

Частные фирмы и государственные учреждения вынуждены приобретать все более совершенные и, следовательно, более дорогие аппаратные и программные средства защиты информации, затраты на эти цели за последних годы возросли на 66%, а доходы от их продажи в начале 90-х годов составили порядка 1 млрд. долларов [1].

Несмотря на столь бурное развитие методов защиты конфиденциальной информации в этом направлении научных исследований и практических разработок есть множество не решенных проблем.

Проблемы защиты информации волновали человечество с незапамятных времен. Примеры достаточно сложных зашифрованных текстов встречают археологи и в русских памятниках XII - XIII вв. Так что наука, получившая название "криптология" (от греческих корней CRYPTOS - тайный и LOGOS - слово), имеет древние корни и традиции.

Задача криптографа - обеспечить как можно большую секретность и аутентичность (подлинность) передаваемой информации. Криптоаналитик, напротив, "взламывает" систему защиты, разработанную криптографом. Он пытается раскрыть зашифрованный текст или выдать поддельное сообщение за настоящее. Одним из основных допущений криптографии является то, что криптоаналитик имеет полный шифротекст и ему известен алгоритм шифрования, за исключением секретного ключа. При этом предполагается, что криптоаналитику доступен для анализа только шифротекст [4,5].

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Зарубежными специалистами сформулирована система требований к алгоритму шифрования, предназначенному для массового применения в вычислительных системах [6].

В настоящее время используются значительное количество алгоритмов шифрования, которые можно условно разделить на две группы [2]:

1. Профессиональные - открытые, но основательно проверенные на криптостойкость, обеспечивающие надежную шифровку информации путем использования секретного ключа.

2. Кустарные - часто весьма оригинальные и простые, дающие на внешний вид хорошую шифровку, но без гарантии, что нет простого средства их "взлома".

В результате плодотворного сотрудничества Национального бюро стандартов, Управления национальной безопасности и фирмы IBM подобный стандарт, получивший название DES (Data Encription Standart), был разработан и опубликован 17 марта 1975 года в специальном издании Federal Register.

Алгоритм DES был разработан в виде стандарта функциональной совместимости, предусматривающего полную спецификацию основной функции и в то же время независимость от физической реализации. Его публикация вызвала оживленную полемику среди специалистов в области защиты информации. После различных симпозиумов было принято решение оставить стандарт без изменений. В алгоритме не было установлено никаких "лазеек". Эффективная длина ключа в 56 бит вполне удовлетворяла потенциальных пользователей на ближайшие 10-15 лет, так как общее число ключей в этом случае оценивалось цифрой 7.6×10^{16}.

Необходимо подчеркнуть, что стандарт DES стал одним из первых "открытых" шифроалгоритмов. Все схемы, используемые для его реализации, были опубликованы и тщательно проверены. Секретным был только ключ, с помощью которого осуществляется кодирование и декодирование информации.

В DES стандарте используются перестановки и рассеивание. В качестве шифруемой единицы выступают восемь последовательных символов сообщения (64 бита). С помощью входной перестановочной таблицы осуществляется перемешивание исходной порции информации. Затем полученная последовательность из 64 бит разделяется на две равные части и итеративно, с помощью ключевой последовательности производится рассеивание. После этого опять осуществляют перестановки с помощью выходной перестановочной таблицы.

В бывшем СССР был установлен единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ. Алгоритм криптографического преобразования

данных предназначен для аппаратной или программной реализации. Он удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации [7].

Алгоритм криптографического преобразования предусматривает несколько режимов работы. Но в любом случае для шифрования данных используется ключ, который имеет разрядность 256 бит и представляется в виде восьми 32-разрядных чисел.

Расшифровка выполняется по тому же ключу, что и шифрование, но этот процесс является инверсией процесса шифрования данных.

Самым существенным недостатком DES-шифрования специалисты признают размер ключа, который считается слишком малым. Стандарт в настоящем виде не является неуязвимым, хотя и очень труден для раскрытия. Для дешифрования информации методом подбора ключей достаточно выполнить 2^{56} операций. Еще один недостаток метода DES заключается в том, что отдельные блоки, содержащие одинаковые данные, будут одинаково выглядеть в зашифрованном тексте, что с точки зрения криптоаналитика неправильно.

Перспективными системами криптографической защиты данных являются системы с открытым ключом. В таких системах для зашифровки данных используется один ключ, а для расшифровки - другой. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями, которые зашифровывают данные. Расшифровывание данных с помощью известного ключа невозможно. Для расшифровывания данных получатель зашифрованной информации использует другой ключ, который является секретным. Разумеется, ключ расшифровывания не может быть определен из ключа зашифровки [3]. В настоящее время наиболее развитым методом криптографической защиты информации с известным ключом является RSA.

Криптостойкость этого алгоритма основывается на предположении, что исключительно трудно определить секретный ключ по открытому, поскольку для этого необходимо решить задачу о существовании делителей целого числа. Данная задача является NP-полной и, как следствие этого факта, не допускает в настоящее время полиномиального, т.е. эффективного решения. Более того, сам вопрос существования эффективных алгоритмов решения NP-полных задач является до настоящего времени открытым. В связи с этим для чисел, состоящих из 20 цифр (а именно такие числа рекомендуется использовать), традиционные методы определения делителей требуют выполнения огромного числа операций (около 10^{23}), что делает весьма маловероятной возможность "взлома" защиты.

Алгоритм криптографического преобразования, определяемый ГОСТ 28147-89, обладает существенным недостатком, который заключается в том, что его программная реализация очень сложна и практически лишена всякого смысла из-за крайне низкого быстродействия. Хотя сейчас уже разработаны аппаратные средства, реализующие данный алгоритм преобразования данных, которые демонстрируют приемлемую производительность, все же складывается впечатление, что разработчики алгоритма совершенно не заботились об эффективности его программной реализации и о стоимости шифрования данных [3].

В силу ряда своих преимуществ все чаще используется RSA метод. Однако, в то же время, к этому методу относятся и с подозрительностью, поскольку в ходе дальнейшего развития может быть найден эффективный алгоритм определения делителя целых чисел, в результате чего метод шифрования станет абсолютно незащищенным. Кроме того, не существует строгого доказательства, что не существует другого способа определения секретного ключа, кроме как определения делителя целых чисел.

Предлагаемый алгоритм криптирования базируется на хорошо исследованном

DES-методе. Его модификация заключается в следующем:

- гибко изменяемый размер паролевой последовательности от 4 байт до 32;
- отсутствие входной и выходной перестановок символов в кодируемой серии;
- использование для зашифровки информации о положении символа в исходном документе;
- наличие возможности задания степени доступности к исходному тексту при его зашифровке.

Процедура криптирования имеет итеративный характер и состоит из обратимых поразрядных логических операций, перестановок и циклических сдвигов левых (**L**) и правых (**R**) четырех байтов, последовательно выбираемых из исходного файла (рис.1).

Функция криптирования **F** представляет собой суммирование по ***mod 2*** *i*-ой части ключа $\mathbf{K_i}$, правой части кодируемой порции $\mathbf{R_{i-1}}$ и функции **Pol** с последующим циклическим сдвигом влево. Аргумент **Pol** задает номера разрядов $\mathbf{R_{i-1}}$, в которых дополнительно суммируются единицы, в зависимости от порядкового номера криптируемого блока байтов. Это позволяет последовательность из одинаковых символов представлять различными шифросимволами.

Алгоритм криптирования построен таким образом, что для зашифровки одной порции входной информации из восьми байт необходимо осуществить восемь итераций с выбором соответствующего количества 32-ух разрядных последовательностей из 256-ти разрядной последовательности **KEY**. Причем, в зависимости от приоритета доступа к закрытой информации, величина паролевой последовательности **PAROL** может варьироваться от 4 до 32 байт. Чем короче пароль, тем больше перекрываются участки в 32-ух разрядных ключевых последовательностях. В таблице 1 указаны номера битов, с которых начинаются 32-ух разрядные последовательности, выбираемые для криптирования блока из восьми байт.

Особенностью алгоритма криптирования является обязательность сдвига криптируемой порции на четное количество разрядов, в противном случае значительно затягивается во времени процесс декриптирования. Это достигается формированием кода количества сдвигов из определенных разрядов i-*ой ключевой последовательности с последующим умножением его на два. Второй особенностью предлагаемого алгоритма является идентичность процессов криптирования и декриптирования. Это дает возможность сократить вдвое затраты при аппаратной реализации.*

Продолжение формирования этой таблицы позволяет выявить простую аналитическую зависимость номера начального бита ***i***-ой ключевой последовательности при ***k*** байтном пароле:

$$n[i,k] = (k-4)*(i-1).$$

Система построена на основе технологии клиент-сервер. Это позволяет повысить уровень безопасности зашифрованной информации в компьютерных сетях.

Табл.1. Определение номера бита при выборке *i*-ой ключевой последовательности

№итер/Дл.пар	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
3	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28
4	0	3	6	9	12	15	18	21	24	27	30	33	36	39	42
5	0	4	8	12	16	20	24	28	32	36	40	44	48	52	56
6	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70
7	0	6	12	18	24	30	36	42	48	54	60	66	72	78	84
8	0	7	14	21	28	35	42	49	56	63	70	77	84	91	98

Весьма уязвимым местом любой системы криптирования с закрытым ключом является знание пароля всеми пользователями. В этом случае возможна неконтролируемая утечка информации о структуре пароля. Поэтому необходимо предпринять дополнительные меры по сохранности секретности пароля.

Для решения данной задачи детализируем понятие пароля. Рассмотрим следующие пароли:

- системный пароль;
- пользовательский пароль;
- индивидуальный пароль.

Традиционно в системах криптирования трактуют все три пароля как единый. Если их разграничить, то можно добиться ряда положительных моментов.

Системный пароль - это секретная последовательность символов, по которой формируется ключевая последовательность. Он не известен ни одному пользователю.

Пользовательский пароль - это секретная последовательность символов, из которой в дальнейшем формируется системный пароль. Пользовательский пароль известен всему кругу зарегистрированных пользователей.

Индивидуальный пароль - это секретная, индивидуальная для каждого пользователя, последовательность символов, идентифицирующая его персонально.

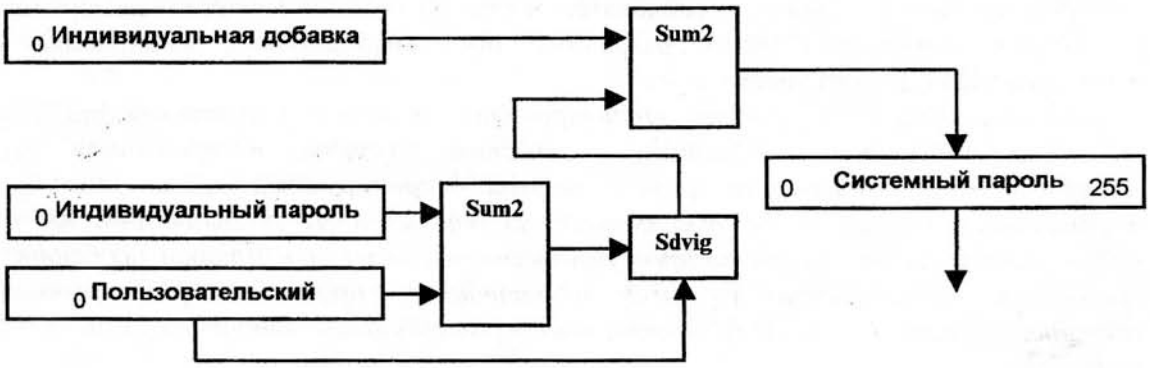

Рис.1. Структура предложенного метода шифрования

Системный пароль получается путем преобразования пользовательского, индивидуального паролей и специфичной добавки, индивидуальной для каждого пользователя. Эта добавка формируется при регистрации администратором системы пользователя таким образом, чтобы она в совокупности со стандартным пользовательским и индивидуальным паролями давала системный пароль.

Эта добавка записывается на индивидуальную дискету (или в специальный файл на сервере), без которой вход в систему криптирования-декриптирования невозможен. Таким образом, у каждого зарегистрированного пользователя имеется своя индивидуальная дискета, которая идентифицирует его по индивидуальному паролю. Такая мера приводит к тому, что каждый пользователь может сформировать правильный системный пароль только при наличии своей дискеты, т.е. для пользователя системный пароль является секретным, и он не имеет возможности его разгласить. На дискете фиксируются имена всех файлов, с которыми работал данный пользователь, время обращения к ним, а также все несанкционированные обращения. Данная дискета должна быть защищена от копирования и вся информация на ней должна быть также закриптирована. Структура процедуры формирования системного пароля приведена на рис.2.

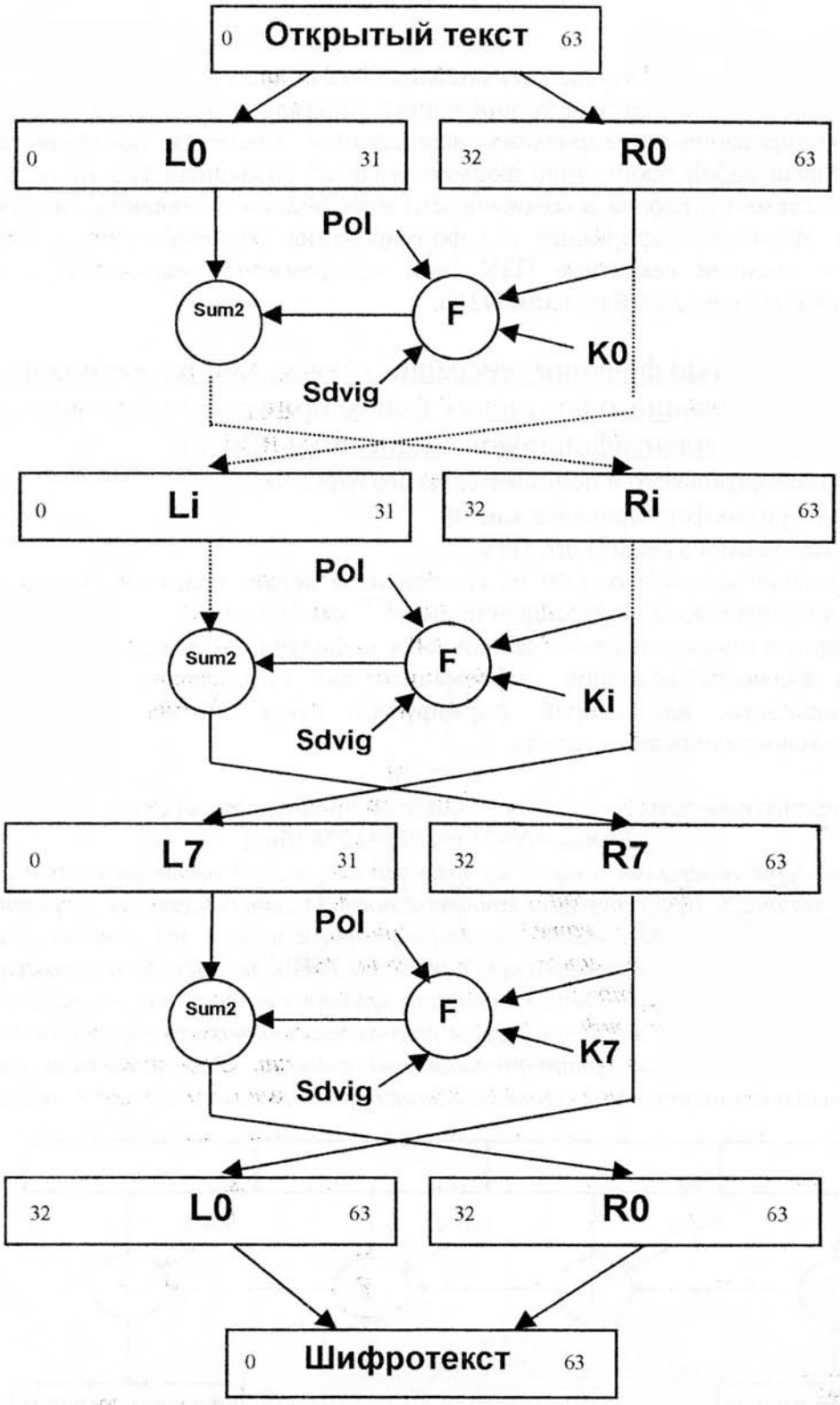

Рис.2. Процедура формирования системного пароля

Процедура формирования индивидуальной добавки аналогична процедуре формирования системного пароля, только вместо добавки подается системный пароль. Сохранность ключевой идентифицирующей дискеты должна обеспечиваться административными мерами:

- на руках у пользователя она должна находиться только на рабочем месте;
- в конце рабочего дня она должна сдаваться администратору для текущего

контроля.

Параметры записи на эту дискету должны быть индивидуальными и секретными, чтобы исключить возможность ее копирования и нелегального использования.

Для кодирования-декодирования используется ключевая последовательность, представляющая собой процедурно формируемый 2^K разрядный код на основании K байтового системного пароля и совокупности информации о значении числа месяца и дня недели. Исходная информация для формирования ключевой последовательности заносится в сменное секретное ПЗУ (при программной реализации - случайно генерируется в определенной области ОЗУ).

Особенностью функции генерации ключа является возможность его несанкционированного получения только при условии наличия своей идентифицирующей дискеты и знания:

- индивидуального и пользовательского паролей;
- алгоритма формирования ключа;
- содержимого секретного ПЗУ.

Отсутствие хотя бы одного из компонентов делает практически невозможной процедуру подбора ключа злоумышленником (2^{256} комбинаций).

Алгоритм генерации ключа заключается в следующем. Число (c) месяца и день (d) недели являются исходной информацией для определения начала двоичной последовательности, из которой формируется ключ. Номер начального бита последовательности определяется как

$$n=8*c+d.$$

Длина последовательности N=1024 бит. При этом предельная емкость ПЗУ составит

$$E=n_{max}+N=255+1023=1278 \text{ (бит)}.$$

Процедура генерации ключа из выделенной последовательности имеет вид, показанный на рис.3. При генерации ключевой последовательности из секретного ПЗУ извлекается битовая последовательность, начиная с адреса [n], *длиной 1024 бита. Эта последовательность записывается в регистр* ***РгКП****, из которого осуществляется выборка по 256 бит для выполнения операции криптирования* ***F*** *на основе системного пароля. После завершения этой процедуры получается секретная последовательность, которая используется для криптирования информации. Это позволяет ежедневно автоматически изменять ключ криптирования при неизменном пароле. Емкости*

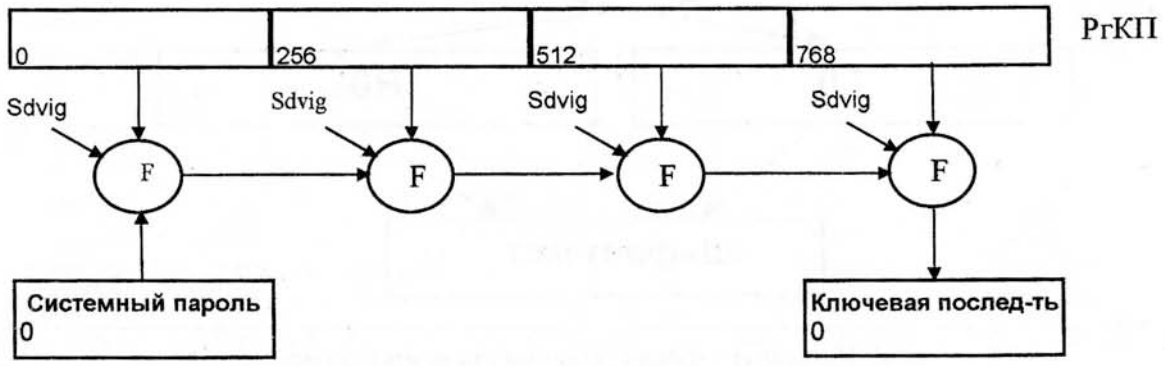

Рис.3. Процедура формирования ключевой последовательности

секретного ПЗУ 2 Кбит достаточно для ежедневной смены ключей в течение года.

Для начала работы с системой криптозащиты пользователю необходимо идентифицировать себя, при помощи его имени и индивидуального пароля. После получения подтверждения от сервера о его идентификации, возможно, начинать

работу с системой. При этом в зависимости от конкретных задач, возможно криптировать либо декриптировать информацию используя, или личный пароль, или выданный администратором, для коллективного использования. При этом пароль для доступа к коллективно используемым данным каждому пользователю выдаётся разный, хотя позволяет получить доступ к одной и той же информации.

Использование технологии клиент-сервер позволяет получить следующее:

- возможность вести протоколирование работы пользователей;
- ограничить доступ пользователей к данным по времени, дню недели, рабочему месту;
- при кадровых перестановках, возможность быстрого добавления, удаления пользователя;
- централизованное администрирование системы (смены паролей и т.д.);
- объединения пользователей в группы по уровню доступу к информации;

Качество криптирования можно оценить по виду гистограммы распределения вероятности появления символов в исходном и зашифрованном файлах. На рис.4 представлена гистограмма распределения вероятности появления символов в текстовом документе размерностью 171 Кбайт. На горизонтальной оси слева на право расположены коды символов от 0 до 255, а по вертикальной вниз - отрезки, длины которых пропорциональны количеству соответствующих символов, встречающихся в исходном тексте.

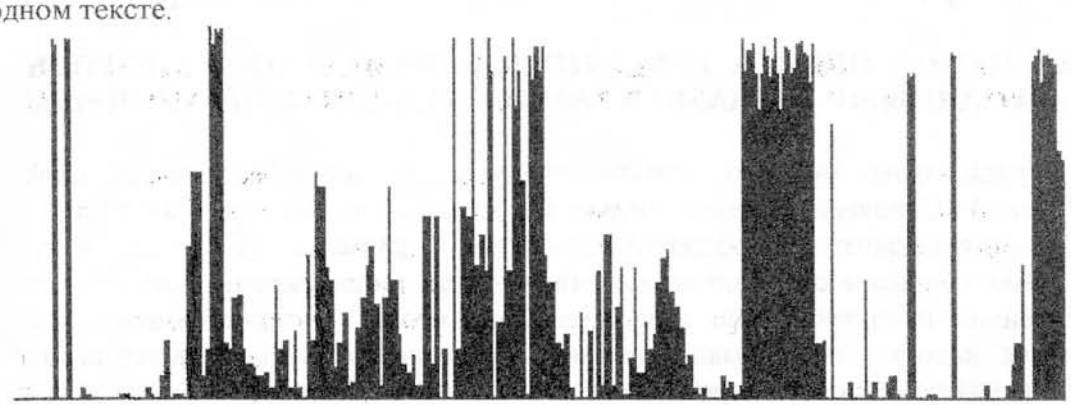

Рис.4. Гистограмма распределения символов в исходном тексте

На рис.5 представлена диаграмма распределения вероятностей появления символов в зашифрованном тексте, причем показана только верхняя ее часть. Видно, что распределение практически равномерное, а это свидетельствует о том, что декриптирование этого текста статистическими методами будет практически затруднено.

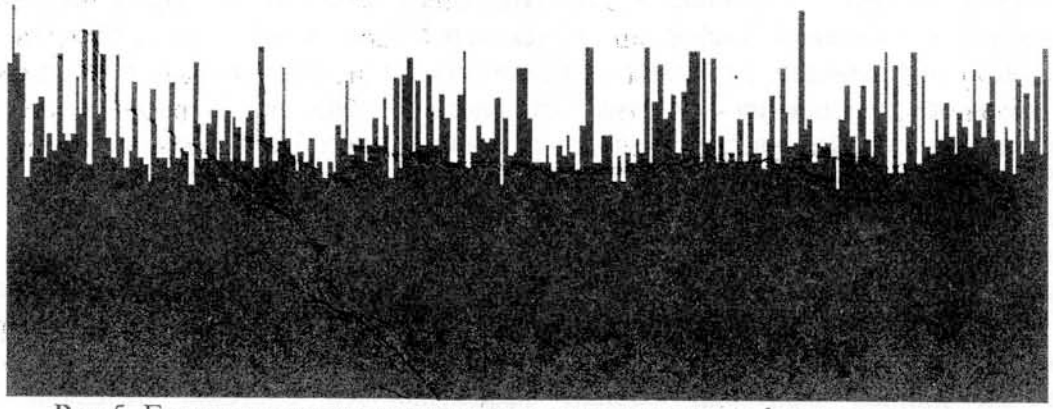

Рис.5. Гистограмма распределения символов в зашифрованном тексте

Список литературы:

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: - Санкт-Петербург, 2000. – 384 с.
2. Герасименко В.А., Размахнин М.К., Родионов В.В. Технические средства защиты информации // Зарубежная радиоэлектроника. 1989. № 12.
3. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
4. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Издательство "Диа-Софт", 1999. - 480 с.
5. Защита информации в персональных ЭВМ. / Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. – М.: Радио и связь, МП «Веста», 1992. – 192 с.
6. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ: Пер. с англ. – М.: Мир, 1082. – 264 с.

Поступила 10.01.2002

УДК 681.511:3

Маракова И.И, Мараков Д.А.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В РАМКАХ ЗАДАННЫХ ОГРАНИЧЕНИЙ

Традиционно принято считать, что криптография обеспечивает шифрование сообщений. С другой стороны, целью шифрования является обеспечение скрытия содержания секретных сообщений. Сокрытие информации (СИ) идет еще дальше, поскольку скрывает сам факт присутствия какого либо секрета. При этом секретные сообщения прячутся в не представляющих особый интерес данных, хранение и передача которых не вызывает никакого подозрения. Бурное развитие методов и средств СИ в настоящее время в частности объясняется весьма многообещающим практическим применением данного направления. СИ имеет несколько различных направлений: стеганография, водяные знаки, отпечатки пальцев, обеспечение анонимности. Предметом наших исследований являются только цифровые водяные знаки, основанные на компьютерных технологиях. В данном приложении основное сообщение должно быть соединено с другой информацией, а именно идентификатором собственника данных. Другими словами, водяные знаки - это такое направление СИ, где задача состоит не столько в сокрытии дополнительной информации, сколько в передаче с основной информации некоторой дополнительной (возможно и не секретной) информации, для которой нужно обеспечить невозможность удаления без значительного ухудшения качества основного сообщения. В работах по данной тематике, как правило, рассматривались различные способы погружения ВЗ без какой-либо теоретической оптимизации или исследования эффективности. Фундаментальные выкладки в данном направлении были сделаны в [2], где авторы описали способ сокрытия с верхними границами скоростей для надежной передачи ВЗ с точки зрения допустимого уровня искажений информации. К сожалению, это верно в асимптотике для покрывающих сообщений бесконечной длины, в то время, как на практике разработчики систем ВЗ имеют дело с основными покрывающими сообщениями конечной длины. Критерий оценки эффективности системы передачи ВЗ по вероятности пропуска ВЗ или вероятности ложного обнаружения были предложены в [3, 4]. Но в данных статьях не рассматривались все возможные случаи и прямая связь констант, характеризующих качество, с упомянутыми вероятностями.