ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ имени А.Ф.МОЖАЙСКОГО
Кафедра математического и программного обеспечения

УТВЕРЖДАЮ

Начальник 27 кафедры

полковник

С. Войцеховский

«___» _____ 20__ г.

Автор: старший преподаватель 27 кафедры
кандидат технических наук
подполковник С.Краснов

Лекция № 7

по учебной дисциплине
«Защита информации»
на тему

Тема: «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗИ»

по дисциплине: «Защита информации»

Рассмотрено и одобрено
на заседании кафедры № 27
« ___ » августа 202__ г.

протокол № __

Санкт-Петербург 2022

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Основные понятия и определения – 10 мин.
2. Симметричные алгоритмы шифрования. Асимметричные алгоритмы шифрования – 40 мин.
3. Функции хеширования. Алгоритм ЭЦП. Реализация криптографических методов – 30 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.

2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml

2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области криптографических методов защиты информации.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на криптографических методах ЗИ.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. В чем заключается суть криптографического метода ЗИ?
2. Перечислите методы шифрования с симметричным ключом?
3. Дайте определение понятию - шифр?
4. Дайте определение Электронной (цифровой) подписи (ЭЦП)…?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 6

«Криптографические методы защиты информации»

В. 1. Основные понятия и определения.

Одним из эффективных направлений защиты информации является криптография, широко применяемая в различных сферах деятельности в государственных и коммерческих структурах. Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

Суть криптографического метода защиты информации заключается в преобразовании открытых данных в зашифрованные при помощи шифра [12].

Почему проблема использования криптографических методов в информационных системах (ИС) стала в настоящий момент особо актуальна? С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

Проблемой защиты информации путем ее преобразования занимается **криптология** (kryptos – тайный, logos – наука). Криптология разделяется на два направления – криптоанализ и криптографию. Цели этих направлений прямо противоположны.

Суть криптоанализа – исследование возможности расшифровывания информации без знания ключей.

Криптография занимается поиском и исследованием математических методов преобразования информации.

Рассмотрим кратко основные понятия, используемые в криптографии, и охарактеризуем важнейшие её направления в соответствии с ГОСТ 28147-89.

Криптографическая защита – защита данных при помощи криптографического преобразования данных.

Криптографическое преобразование – преобразование данных при помощи шифрования и (или) выработки имитовставки.

Имитовставка – отрезок информации фиксированой длины, полученной по определенному правилу из открытых данных и ключа, и добавленный к зашифрованным данным для обеспечения имитозащиты.

Зашифрование данных – процесс преобразования открытых данных в зашифрованные при помощи шифра.

Имитозащита – защита системы шифрованной связи от навязывания ложных данных.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

- алфавит Z33 – 32 буквы русского алфавита и пробел;
- алфавит Z256 – символы, входящие в стандартные коды ASCII и КОИ-8;
- бинарный алфавит – Z2 = {0,1};
- восьмеричный алфавит или шестнадцатеричный алфавит.

Шифрование – преобразовательный процесс, когда исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Шифр - совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Криптоалгоритм считается идеально стойким, если для прочтения зашифрованного блока данных необходим перебор всех возможных ключей до тех пор, пока расшифрованное сообщение не окажется осмысленным.

Имеется несколько *показателей криптостойкости*, среди которых:

- количество всех возможных ключей;
- среднее время, необходимое для криптоанализа.

Основные направления использования криптографических методов:

- передача конфиденциальной информации по каналам связи, например с помощью электронной почты,
- установление подлинности передаваемых сообщений,
- хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Эффективность шифрования с целью защиты информации *зависит от* сохранения тайны ключа и криптостойкости шифра.

Современная микропроцессорная техника позволяет уже сегодня за достаточно приемлемое время взламывать симметричные блочные шифры с длиной ключа 40 бит. Для такого взлома используется метод полного перебора - тотального опробования всех возможных значений ключа (метод «грубой силы»).

До недавнего времени блочный алгоритм DES, имеющий ключ с эффективной длиной 56 бит (на самом деле его длина 64 бит, но только 56 бит являются значащими, остальные 8 – проверочные биты для контроля чётности), считался относительно безопасным алгоритмом шифрования. Он многократно подвергался тщательному криптоанализу в течение 20 лет, и самым практичным способом его взлома является метод перебора всех возможных значений ключа. Ключ шифра DES имеет 2^{56} возможных значений.

В настоящее время на рынок поступили процессоры, обладающие возможностью перебирать десятки и сотни милионов значений ключей в секунду. Стоимость этих чипов составляет всего лишь десятки долларов. Поэтому вполне актуальны оценки криптостойкости шифра DES, включающие ориентировочные расчеты времени и материальных средств, которые необходимо затратить на взлом этого шифра методом полного перебора всех возможных значений ключа с использованием, как стандартных компьютеров, так и специализированных криптоаналитических аппаратных средств.

В работе [16] приводятся результаты анализа трудоемкости взлома криптоалгоритма DES с длиной ключа 56 бит. Так для хакера одиночки с бюджетом в 500$ на это могут потребоваться десятки лет, крупная фирма с бюджетом в 300 тыс.$ потратит на это несколько дней, большая корпорация с бюджетом до 10 млн. $ – от 6 минут до 13 часов, специальные агентства – получат полный доступ немедленно.

В. 2. Симметричные криптосистемы

Криптосистемы разделяются на симметричные и асимметричные (с открытым ключом). В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. Это означает, что любой, кто имеет доступ к ключу шифрования, может расшифровать сообщение. Именно поэтому симметричные криптосистемы называют криптосистемами с секретным ключом – ключ шифрования должен быть доступен только тем, кому предназначено сообщение. Задача обеспечения конфиденциальности передачи электронных

документов с помощью симметричной криптосистемы сводится к обеспечению конфиденциальности ключа шифрования.

Недостатки симметричного шифрования:

1. Перед началом обмена зашифрованными данными необходимо обменяться секретными ключами со всеми адресатами.
2. Передача секретного ключа симметричной криптосистемы не может быть осуществлена по общедоступным каналам связи; секретный ключ надо передавать отправителю и получателю по защищенному каналу распространения ключей.
3. Предъявляются повышенные требования к службе генерации и распределения ключей, обусловленные тем, что для n абонентов при схеме взаимодействия «каждый с каждым» требуется P= n * (n - 1) / 2 ключей, то есть зависимость числа ключей от числа абонентов является квадратичной; например, для n = 1000 абонентов требуемое количество ключей будет равно: P=n*(n-1)/2 = 499500 ключей, для n=100 – P=4950 ключей.

Поэтому без эффективной организации защищенного распределения ключей широкое использование обычной системы симметричного шифрования в больших сетях, в частности глобальных, практически невозможно.

Методы шифрования с симметричным ключом

По способу преобразования информации выделяют следующие методы шифрования:

- методы замены;
- методы перестановки;
- аналитические методы
- аддитивные методы;
- комбинированные методы.

Методы замены

Суть методов замены (подстановки) заключается в замене символов исходной информации, записанных в одном алфавите символами из другого алфавита по определенному правилу. Самым простым является метод прямой замены. Символам S0i исходного алфавита A0, с помощью которых записывается исходная информация, однозначно ставятся в соответствие символы S1i шифрующего алфавита A1. В простейшем случае оба алфавита могут состоять из одного и того же набора символов. Например, оба алфавита могут содержать буквы русского алфавита.

Задание соответствия между символами обоих алфавитов осуществляется с помощью преобразования числовых эквивалентов символов исходного текста T0, длиной - K символов, по определенному алгоритму.

Алгоритм алфавитной замены может быть представлен в виде последовательности шагов.

Шаг 1. Формирование числового кортежа L0h путем замены каждого символа

$$S_{0i} \in T_0 (i = \overline{1,K})$$

представленного в исходном алфавите A_0 размера [1xR], на число $h_{0j}(S_{0i})$, соответствующее порядковому номеру символа S_{0i} в алфавите A_0.

Шаг 2. Формирование числового кортежа L_{1h} путем замены каждого числа кортежа L0h на соответствующее число h_{1i} кортежа L_{1h}, вычисляемое по формуле:

$h_{1i}=(k_1 * h_{0l}(S_{0i})+ k_2)(\text{mod } R)$,

где k_1 - десятичный коэффициент; k_2 - коэффициент сдвига. выбранные коэффициенты k_1, k_2 должны обеспечивать однозначное соответствие чисел h_{0i} и h_{1i} , а при получении $h_{1i} = 0$ выполнить замену $h_{1i} = R$.

Шаг 3. Получение шифртекста T_1, путем замены каждого числа h_{1i} (S_{1i}) кортежа L_{1h} соответствующим символом, алфавита $S_{1i} \in T_0 (i = \overline{1,K})$ шифрования A_1 размера [1xR].

Шаг 4. Полученный шифртекст разбивается на блоки фиксированной длины B. Если последний блок оказывается неполным, то в конец блока помещаются специальные символы-заполнители (например, символ *).

Пример. Исходными данными для шифрования являются:

Русский алфавит без букв ё, й, зато с добавлением символа _..

T_0 = <МЕТОД_ШИФРОВАНИЯ>;

A_0 = <АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_>;

A_1 = <ОРЩЬЯТЭ_ЖМЧХАВДЫФКСЕЗПИЦГНЪШБУЮ>;

R=32; k_1 =3; k_2 =15, b=4.

Пошаговое выполнение алгоритма приводит к получению следующих результатов.

Шаг 1. L_{0h} = <12,6,18,14,5,32,24,9,20,16,14,3,1,13,9,31>.

Шаг 2. L_{lh} = <19,1,5,25,30,15,23,10,ll,31,25,24,18,22,10,12>.

Шаг 3. T_1 = <СОЯГБДИМЧУГЦКПМХ>.

Шаг 4. T_2 = <СОЯГ БДИМ ЧУГЦ КПМХ>.

При расшифровании сначала устраняется разбиение на блоки. Получается непрерывный шифртекст T_1 длиной K символов. Расшифрование осуществляется путем решения целочисленного уравнения:

$k_1*h_{0i}+k_2=n*R+ h_{1i}$.

При известных целых величинах k_1, k_2, h_{1i} и R величина h_{0i} вычисляется методом перебора n.

Последовательное применение этой процедуры ко всем символам шифртекста приводит к его расшифрованию.

По условиям приведенного примера может быть построена таблица замены, в которой взаимозаменяемые символы располагаются одном столбце.

Использование таблицы замены (см. табл. 1) значительно упрощает процесс шифрования. При шифровании символ исходного текста сравнивается с символами строки S_{0i}; таблицы. Если произошло совпадение в i столбце, то символ исходного текста заменяется символом из строки S_{1i}, находящегося в том же столбце i таблицы.

Таблица замены. таблица 1

S_{0i}	А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р	С	Т	У	Ф
h_{0i}	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
S_{1i}	К	З	Ц	Л	Б	О	Ь	Э	М	А	Ы	С	П	Г	Ъ	У	Р	Я	_	Ч
h_{1i}	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2	5	8	11

Методы перестановки

Суть методов перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановке символов внутри каждого блока по определенному алгоритму.

Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры. Примером простейшей перестановки является запись блока исходной информации в матрицу по строкам, а считывание - по столбцам. Последовательность заполнения строк матрицы и считывания зашифрованной информации по столбцам может задаваться ключом. Криптостойкость метода зависит от длины блока (размерности матрицы). Так для блока длиной 64 символа (размерность матрицы 8x8) возможны $1{,}6x10^9$ комбинаций ключа. Для блока длиной 256 символов (матрица размерностью 16x16) число возможных ключей достигает $1{,}4x10^{26}$. Решение задачи перебора ключей в последнем случае даже для современных ЭВМ представляет существенную сложность.

Перестановки используются также в методе, основанном на применении маршрутов Гамильтона. Этот метод реализуется путем выполнения следующих шагов.

Шаг 1. Исходная информация разбивается на блоки. Если длина шифруемой информации не кратна длине блока, то на свободные места последнего блока помещаются специальные служебные символы-заполнители (например, *).

Шаг 2. Символами блока заполняется таблица, в которой для каждого порядкового номера символа в блоке отводится вполне определенное место (рис. 3.1).

Шаг 3. Считывание символов из таблицы осуществляется по одному из маршрутов. Увеличение числа маршрутов повышает криптостойкость шифра. Маршруты выбираются либо последовательно, либо их очередность задается ключом К.

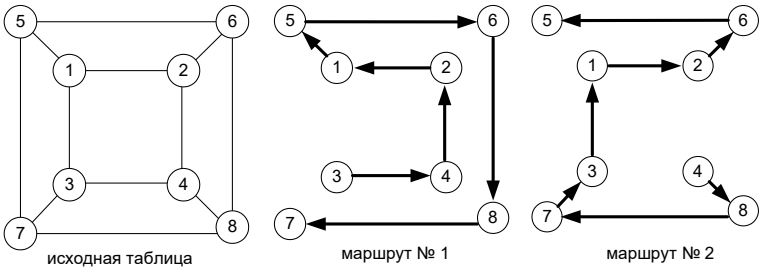

Рис.3.1. Вариант 8-элементной исходной таблицы и маршрутов Гамильтона

Шаг 4. Зашифрованная последовательность символов разбивается на блоки фиксированной длины L. Величина L может отличаться от длины блоков, на которые разбивается исходная информация на шаге 1.

Расшифрование производится в обратном порядке. В соответствии с ключом выбирается маршрут и заполняется таблица согласно этому маршруту.

Из таблицы символы считываются в порядке следования номеров элементов. Ниже приводится **пример** шифрования информации с использованием маршрутов Гамильтона.

Пусть требуется зашифровать исходный текст

Т0 = <МЕТОДЫ_ПЕРЕСТАНОВКИ>. Ключ и длина зашифрованных блоков соответственно равны: K=<2,1,1>, L=4. Для шифрования используются таблица и два маршрута, представленные на на рис. 3.1. Для заданных условий маршруты с заполненными матрицами имеют вид, показанный на рис. 3.2.

Шаг 1. Исходный текст разбивается на три блока:

Б1=<МЕТОДЫ_П>;

Б2 = <ЕРЕСТАНО>;

БЗ=<ВКИ*****>.

Маршрут №2

Маршрут №1

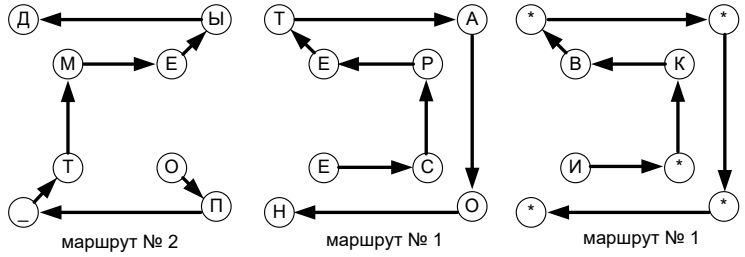

Рис.3.2. Пример шифрования с помощью маршрутов Гамильтона

Шаг 2. Заполняются три матрицы с маршрутами 2,1,1 (рис.6).

Шаг 3. Получение шифр текста путем расстановки символов в соответствии с маршрутами.

Ti = <ОП_ТМЕЫДЕСРЕТАОНИ*КВ****>.

Шаг 4. Разбиение на блоки шифр текста

Т,=<ОП_Т МЕЫД ЕСРЕ ТАОН И*КВ ****>.

В практике большое значение имеет использование специальных аппаратных схем, реализующих метод перестановок.

Аналитические методы шифрования

Для шифрования информации могут использоваться аналитические преобразования. Наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры. За шифрование k-го блока исходной информации, представленного в виде вектора $B_k = || b_j||$, осуществляется путем перемножения матрицы-ключа $A= || a_{ij} ||$ и вектора B_k. В результате перемножения получается блок шифртекста в виде вектора $C_k = ||c_i ||$, где элементы вектора C_k определяются по формуле: $c_i = \sum a_{ij} b_j$

Расшифрование информации осуществляется путем последовательного перемножения векторов C_k и матрицы A^{-1}, обратной матрице А.

Аддитивные методы шифрования

Суть аддитивных методов шифрования [4] заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому кортежу символов. Этот кортеж называется гаммой. Поэтому аддитивные методы шифрования называют также гаммированием.

Для данных методов шифрования ключом является гамма. Криптостойкость аддитивных методов зависит от длины ключа и равномерности его статистических характеристик. Если ключ короче, чем шифруемая последовательность символов, то шифр-текст может быть расшифрован криптоаналитиком статистическими методами исследования. Чем больше разница длин ключа и исходной информации, тем выше вероятность успешной атаки на шифр-текст. Если ключ представляет собой непериодическую последовательность случайных чисел, длина которой превышает длину шифруемой информации, то без знания ключа расшифровать шифр-текст практически невозможно. Как и для методов замены в качестве ключа могут использоваться неповторяющиеся последовательности цифр, например, в числах n, e и других.

На практике самыми эффективными и распространенными являются аддитивные методы, в основу которых положено использование генераторов (датчиков) псевдослучайных чисел. Генератор использует исходную информацию относительно малой длины для получения практически бесконечной последовательности псевдослучайных чисел.

Для получения последовательности псевдослучайных чисел (ПСЧ) могут использоваться специальные генераторы. Они вырабатывают псевдослучайные последовательности чисел, для которых могут быть строго математически определены такие основные характеристики генераторов как периодичность и случайность выходных последовательностей.

Среди генераторов ПСЧ выделяется своей простотой и эффективностью линейный генератор, вырабатывающий псевдослучайную последовательность чисел T(i) в соответствии с соотношением

$T(i+1) = (a - T(i) + c) \bmod m,$

где a и c - константы, T(0) - исходная величина, выбранная в качестве порождающего числа.

Период повторения такого датчика ПСЧ зависит от величин a и c. Значение m обычно принимается равным 2^S, где s - длина слова ЭВМ в битах. Период повторения последовательности генерируемых чисел будет максимальным тогда и только тогда, когда c – нечетное число и a (mod 4) = 1. Такой генератор может быть сравнительно легко создан как аппаратными средствами, так и программно.

Комбинированные методы представляют собой сочетание сразу нескольких вышеуказанных методов шифрования.

Алгоритмы симметричного шифрования.

Одним из распространённых симметричных криптоалгоритмов является упоминавшийся ранее **алгоритм DES** (Data Encryption Standard). Обобщённая схема шифрования которого показана на рис. 3.3.

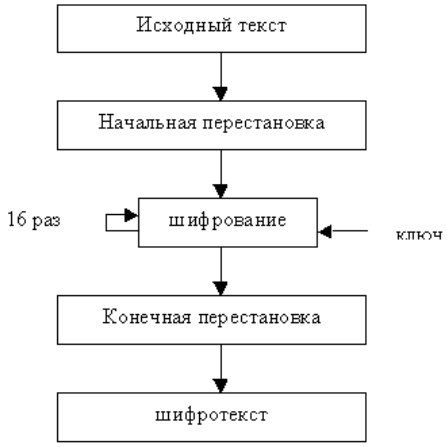

Рис.3.3. Обобщённая схема шифрования в алгоритме DES.

Для шифрования данных помимо алгоритма DES успешно применяется и ряд других блочных симметричных криптоалгоритмов:

Алгоритм IDEA (International Data Encryption Algorithm) - еще один 64-битовый блочный шифр с длиной ключа 128 бит. Этот европейский стандарт криптоалгоритма предложен в 1990 году. Алгоритм IDEA по скорости не уступает алгоритму DES, а по стойкости к криптоанализу превосходит его.

Алгоритм RC2 представляет собой 64-битовый блочный шифр с ключом переменной длины. Этот алгоритм приблизительно в два раза быстрее, чем DES. Может использоваться в тех же режимах, что и DES, включая тройное шифрование. Владельцем алгоритма является компания RSA Data Security.

Алгоритм RC5 представляет собой быстрый блочный шифр, который имеет размер блока 32, 64 или 128 бит, ключ длиной от 0 до 2048 бит. Выполняет от 0 до 255 проходов. Алгоритмом владеет компания RSA Data Security.

Алгоритм CAST представляет собой 64-битовый блочный шифр, использует ключи длиной от 40 до 64 бит, выполняет 8 проходов. Вскрыть этот шифр можно только путем прямого перебора, другие способы вскрытия неизвестны.

Алгоритм Blowfish - это 64-битовый блочный шифр, имеет ключ переменного размера до 448 бит, выполняет 16 проходов, на каждом из них осуществляются перестановки, зависящие от ключа, и подстановки, зависящие от ключа и данных. Этот алгоритм быстрее DES.

В нашей стране установлен единый алгоритм криптографического преобразования данных для систем обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ, который определяется **ГОСТ 28147-89**. Стандарт обязателен для организаций, предприятий и учреждений, применяющих криптографическую защиту данных, хранимых и передаваемых в сетях ЭВМ, в отдельных вычислительных комплексах и ЭВМ.

Этот алгоритм криптографического преобразования данных предназначен для аппаратной и программной реализации, удовлетворяет криптографическим требованиям и не накладывает ограничений на степень секретности защищаемой информации.

Стандартом определены следующие алгоритмы криптографического преобразования информации:

- простая замена;
- гаммирование;
- гаммировяние с обратной связью;
- выработка имитовставки.

Общим для всех алгоритмов шифрования является использование ключа размерностью 256 бит, разделенного на восемь 32-разрядных двоичных слов, и разделение исходной шифруемой двоичной последовательности на блоки по 64 бита.

Асимметричные криптосистемы

Наряду с традиционным шифрованием на основе секретного ключа в последние годы все большее признание получают системы шифрования с открытым ключом. В таких системах используются два ключа. Информация шифруется с помощью открытого ключа, а расшифровывается с использованием секретного ключа.

Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно. Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является закрытым (секретным). Разумеется, ключ расшифрования не может быть определен из ключа зашифрования.

В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций. Эти функции обладают следующим свойством. По известному x легко определяется функция $y = f(x)$. Но по известному значению y практически невозможно получить x. В криптографии используются односторонние функции, имеющие так называемый потайной ход. Эти функции с параметром z обладают следующими свойствами. Для определенного z могут быть найдены алгоритмы E_z и D_z. С помощью E_z легко получить функцию $f_z(x)$ для всех x из области определения. Так же просто с помощью алгоритма D_z получается и обратная функция $x = f^{-1}(y)$ для всех y из области допустимых значений. В то же время практически для всех z и почти для всех y из области допустимых значений нахождение $f^{-1}(y)$ при помощи вычислений невозможно даже при известном E_z. В качестве открытого ключа используется – y, а в качестве закрытого – x.

При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации.

Процесс передачи зашифрованной информации в асимметричной криптосистеме осуществляется следующим образом:

1. Подготовительный этап:
   - абонент B генерирует пару ключей: секретный ключ $k_в$ и открытый ключ $K_в$;
   - открытый ключ $K_в$ посылается абоненту A и остальным абонентам (или делается доступным, например, на разделяемом ресурсе).
2. Использование - обмен информацией между абонентами A и B:
   - абонент A зашифровывает сообщение с помощью открытого ключа $K_в$ абонента B и отправляет шифртекст абоненту B;
   - абонент B расшифровывает сообщение с помощью своего секретного ключа $k_в$. Никто другой (в том числе абонент A) не может расшифровать данное сообщение, так как не имеет секретного ключа абонента B.

Защита информации в асимметричной криптосистеме основана на секретности ключа $k_в$ получателя сообщения.

Криптосистемы с открытыми ключами различаются видом односторонних функций. К асимметричным криптоалгоритмам и криптосистемам относятся:

- алгоритм асимметричного шифрования RSA;
- алгоритм асимметричного шифрования Эль Гамаля;
- криптосистема Мак-Элиса;
- алгоритм цифровой подписи Digital Signature Algorithm (DSA);
- российский стандарт цифровой подписи ГОСТ Р 34.10-94;
- алгоритмы цифровых подписей Elliptic Curve Digital Signature Algorithm (ECDSA) и ГОСТ Р 34.10-2001 и др.

Первым и наиболее известным стал алгоритм асимметричного шифрования RSA математическая схема которого была разработана в 1977 г. В Массачуссетском технологическом институте США. Алгоритм получил свое название по первым буквам фамилий его авторов: Rivest, Shamir и Adleman. Надежность алгоритма заключается в трудности факторизации больших чисел.

Он основан на использовании операции возведения в степень модульной арифметики. Его можно представить в виде следующей последовательности шагов.

Шаг 1. Выбираются два больших простых числа p и q. Простыми называются числа, которые делятся только на самих себя и на 1. Величина этих чисел должна быть больше 200.

Шаг 2. Получается открытая компонента ключа n:

n=p-q.

Шаг 3. Вычисляется функция Эйлера по формуле:

f(p,q)=(p-1)*(q-1)

Функция Эйлера показывает количество целых положительных чисел от 1 до n, которые взаимно просты с n. Взаимно простыми являются такие числа, которые не имеют ни одного общего делителя, кроме 1.

Шаг 4. Выбирается большое простое число d, которое является взаимно простым со значением f(p,q).

Шаг 5. Определяется число e, удовлетворяющее условию:

e*d=1(mod f(p,q)).

Данное условие означает, что остаток от деления (вычет) произведения e*d на функцию f(p,q) равен 1. Число e принимается в качестве второй компоненты открытого ключа. В качестве секретного ключа используются числа d и n.

Шаг 6. Исходная информация, независимо от ее физической природы, представляется в числовом двоичном виде. Последовательность бит разделяется на блоки длиной L бит, где L - наименьшее целое число, удовлетворяющее условию: $L \geq \log_2 (n+1)$. Каждый блок рассматривается как целое положительное число X(i), принадлежащее интервалу [0, n-1]. Таким образом, исходная информация представляется последовательностью чисел X(i), $i=\overline{1, I}$. Значение I определяется длиной шифруемой последовательности.

Шаг 7. Зашифрованная информация получается в виде последовательности чисел Y(I), вычисляемых по формуле:

Y(i)=X(i)) e (mod n).

Шаг 8. Для расшифрования информации используется следующая зависимость:

X(i)=(Y(i)) d (mod n).

Пример *применения метода RSA* для криптографического закрытия информации. Примечание: для простоты вычислений использованы минимально возможные числа.

Пусть требуется зашифровать сообщение на русском языке "ГАЗ".

Для зашифрования и расшифрования сообщения необходимо выполнить следующие шаги.

Шаг 1. Выбирается p = 3иq=ll.

Шаг 2. Вычисляется n = 3*11=33.

Шаг 3. Определяется функция Эйлера

f(p,q)=(3-1)*(11-l)=20.

Шаг 4. В качестве взаимно простого числа выбирается число d=3.

Шаг 5. Выбирается такое число e, которое удовлетворяло бы соотношению: (e*3)*(mod 20) =1. Пусть e = 7.

Шаг 6. Исходное сообщение представляется как последовательность целых чисел. Пусть букве А соответствует число 1, букве Г - число 4, букве З - число 9. Для представления чисел в двоичном коде требуется 6 двоичных разрядов, так как в русском алфавите используются 33 буквы (случайное совпадение с числом n). Исходная информация в двоичном коде имеет вид:

000100000001001001.

Длина блока L определяется как минимальное число из целых чисел, удовлетворяющих условию:

$L \geq \log_2 (n+1)$, тогда $\log_2 (33+1) = \frac{\lg 34}{\lg 2} = \frac{1,53148}{0,30103} = 5,08747$ Отсюда L=6.

Тогда исходный текст представляется в виде кортежа X(i) = <4, 1, 9>.

Шаг 7. Кортеж X(i) зашифровывается с помощью открытого ключа {7, 33}:

$Y(1) = (4^7) \pmod{33} = 16384 \pmod{33} = 16$;

$Y(2) = (1^7) \pmod{33} = 1 \pmod{33} = 1$;

$Y(3) = (9^7) \pmod{33} = 4782969 \pmod{33} = 15$.

Получено зашифрованное сообщение Y(i) = <16,1,15>.

Шаг 8. Расшифровка сообщения Y(i) = <16, 1, 15> осуществляется с помощью секретного ключа {3, 33}:

$X(1) = (16^3) \pmod{33} = 4096 \pmod{33} = 4$;

$X(2) = (1^3) \pmod{33} = 1 \pmod{33} = 1$;

$X(3) = (15^3) \pmod{33} = 3375 \pmod{33} = 9$.

Исходная числовая последовательность в расшифрованном виде

X (I) = <4, 1, 9> заменяется исходным текстом "ГАЗ".

Более надежный и удобный для реализации на персональных компьютерах ассиметричный алгоритм был разработан в 1984 г. американцем арабского происхождения Тахером *Эль Гамалем* и получил название *El Gamal Signature Algorithm* (**EGSA**).

Идея EGSA основана на том, что для обоснования практической невозможности фальсификации ЭЦП может быть использована более сложная вычислительная задача, чем разложение на множители большого целого числа - задача дискретного логарифмирования. Кроме того Эль Гамалю удалось избежать явной слабости алгоритма RSA, связанной с возможностью подделки ЭЦП под некоторыми сообщениями без определения секретного ключа.

Основным недостатком систем RSA и Эль-Гамаля является необходимость выполнения трудоемких операций в модульной арифметике, что требует привлечения значительных вычислительных ресурсов.

Криптосистема Мак-Элиса использует коды, исправляющие ошибки. Она реализуется в несколько раз быстрее, чем криптосистема RSA, но имеет и существенный недостаток. В криптосистеме Мак-Элиса используется ключ большой длины, и получаемый шифр текст в два раза превышает длину исходного текста.

Алгоритм цифровой подписи *Digital Signature Algorithm (DSA)* предложен в 1991г. в США для использования в стандарте цифровой подписи DSS (Digital Signature Standard). Алгоритм DSA является развитием алгоритма ЭЦП EGSA. По сравнению с алгоритмом ЭЦП EGSA алгоритм DSA имеет ряд преимуществ: сокращен объем памяти и время вычисления подписи. Недостатком же является необходимость при подписывании и проверке подписи выполнять сложные операции деления по модулю большого числа.

Российский стандарт цифровой подписи обозначается как *ГОСТ Р 34.10-94.* Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к алгоритму DSA. Различие между этими стандартами заключается в использовании параметров ЭЦП разного порядка, что приводит к получению более безопасной подписи при использовании российского стандарта.

Алгоритмы цифровых подписей *Elliptic Curve Digital Signature Algorithm (ECDSA) и ГОСТ Р 34.10-2001* являются усовершенствованием цифровых подписей DSA и ГОСТ Р 34.10-94 соответственно. Эти алгоритмы построены на базе математического аппарата эллиптических кривых над простым полем Галуа.

Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП) необходима для однозначного и никем неоспоримого установления автора какого-либо документа. Фактически, ЭЦП служит аналогом обычной подписи, которая устанавливает подлинность какого-либо документа или договора. Но поскольку в последнее время огромное количество договоров и документов заключаются с использованием электронных и компьютерных средств, то поставить на них обычную подпись не представляется возможным. Именно для таких ситуаций и используется электронная цифровая подпись. Электронная цифровая подпись создана для того, чтобы избежать подделок, а также искажений

передаваемых сообщений.

Механизм цифровой подписи (digital signature) представляет собой дополнительную информацию, приписываемую к защищаемым данным.

Электронной (цифровой) подписью (ЭЦП) называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения. ЭЦП обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ).

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом.

ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Система ЭЦП включает две процедуры:

- формирование цифровой подписи;
- проверку цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи - открытый ключ отправителя.

Технология применения системы электронной цифровой подписи (ЭЦП) предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа. Иначе говоря, открытый ключ является необходимым инструментом, позволяющим проверить подлинность электронного документа и автора подписи. Открытый ключ не позволяет вычислить секретный ключ.

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи:

- задача факторизации (разложения на множители) больших целых чисел;
- задача дискретного логарифмирования.

Надежность цифровой подписи определяется стойкостью к криптоаналитическим атакам двух ее компонент: хэш-функции и самого алгоритма ЭЦП.

Стойкая схема цифровой подписи должна использовать хэш-функцию, обладающую следующими свойствами:

1. Односторонность. Пусть дано хэш-значение *H(M)* некоторого неизвестного сообщения *M.* Тогда вычислительно невозможно определить *M* по имеющемуся *H(M).*
2. Стойкость к столкновению (коллизии). Пусть дано сообщение *M* и его хэш-значение *H(M).* Тогда вычислительно невозможно определить *M'* такое, что *H(M) = H(M').* Это свойство эквивалентно свойству односторонности.
3. Строгая стойкость к столкновению (коллизии). Вычислительно невозможно найти два произвольных сообщения *M* и *M',* для которых *H(M) = H(M').*

Оценим вероятность взлома хэш-функции.

Для лобовой атаки на однонаправленные хэш-функции используют два метода. Первый направлен на взлом второго свойства, т.е. по известному значению хэш-функции H(M) противник хочет создать другой документ M', такой, что H(M') = H(M). Другой метод изящнее, он направлен на взлом третьего свойства: противник хочет найти два случайных сообщения M и M', таких, что H(M) = H(M').

В математической статистике известен стандартный парадокс «дней рождений», который заключается в следующем (Лапонина О.Р. Криптографические основы безопасности //

www.INTUIT.ru): сколько человек должно собраться в одной комнате, чтобы с вероятностью 1/2 хотя бы у одного из них был общий с вами день рождения? Ответ - 253. А сколько людей должно собраться, чтобы с вероятностью 1/2 хотя бы у двоих из них был общий день рождения? Ответ поразителен - 23. Обнаружение кого-нибудь с точно заданным днем рождения аналогично первому методу атаки, а обнаружение двух человек с произвольным, но одинаковым днем рождения аналогично второму методу. Вторая атака широко известна как *атака на основе парадокса "дней рождений" [2].*

Оценим, насколько успешными на практике могут быть атаки, основанные на двух описанных выше методах. Пусть одна MIPS (Million Instruction Per Second) машина хэширует миллион сообщений в секунду. При таких условиях число хэш-значений, вычисленных одной MIPS машиной за один год

составляет $L = 3{,}15 * 10^{13}$.

В таблице 1 приведена оценка вероятности взлома хэш-функции для двух рассмотренных методов атаки при различных значениях длины выходного хэш-значения.

Таблица 1

Длина хэш-значения, бит	Первый метод		Второй метод	
	Вероятность взлома	Продолжительность взлома, Ml PS-лет	Вероятность взлома	Продолжительность взлома, MlPS-лет
64	$1{,}08 \times 10^{-19}$	300000	$2{,}33 \times 10^{-10}$	1,19 часа
128	$5{,}88 \times 10^{-39}$	$5{,}4 \times 10^{24}$	$5{,}42 \times 10^{-20}$	600000
256	$1{,}73 \times 10^{-77}$	$1{,}8 \times 10^{63}$	$2{,}94 \times 10^{-39}$	$1{,}1 \times 10^{25}$
512	$1{,}49 \times 10^{-154}$	$2{,}1 \times 10^{140}$	$8{,}64 \times 10^{-78}$	$3{,}7 \times 10^{63}$

Таким образом, чтобы обезопасить хэш-функцию от взлома на определенное количество лет необходимо использовать большую длину хэш-значения сообщения. Так, при требовании обеспечить стойкость к взлому хэш-функции в течение 1,1 х 1025 MIPS-лет, необходимо использовать не 128-битное, а 256-битное значение хэш-функции.

Основываясь на полученных оценках, можно сделать вывод, что вероятность взлома хэш-функции *H (M)* первым методом ниже, чем вторым.

Российский стандарт хэш-функции ГОСТ Р 34.11-94 использует 256-битное хэш-значение сообщения, что позволяет утверждать, что при современных вычислительных мощностях его вскрытие вычислительно невозможно. Другими словами, для взлома хэш-функции ГОСТ Р 34.11-94 вторым, более эффективным методом, потребуется $1{,}1 \times 10^{25}$ MIPS-лет.

Стойкость стандарта ГОСТ Р 34.10-94 основана на сложности решения частной задачи дискретного логарифмирования в простом поле. Стойкость нового российского стандарта ГОСТ Р 34.10-2001 основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

В таблице 2 приведена оценка вычислительной сложности решения задач дискретного логарифмирования в простом поле и в группе точек эллиптической кривой.

Таблица 2 - Трудоемкость взлома российских стандартов ЭЦП

Порядок поля p и порядок *q* базовой точки P(в разрядах)	L_r	L_p
128	$1{,}35 \times 10^{10}$	$1{,}63 \times 10^{19}$
256	$1{,}12 \times 10^{14}$	$3{,}02 \times 10^{38}$
512	$1{,}76 \times 10^{19}$	$1{,}03 \times 10^{77}$
1024	$1{,}32 \times 10^{26}$	$1{,}19 \times 10^{154}$
1536	$1{,}31 \times 10^{31}$	$1{,}38 \times 10^{231}$
2048	$1{,}53 \times 10^{35}$	$1{,}59 \times 10^{308}$

Представим полученные результаты графически.

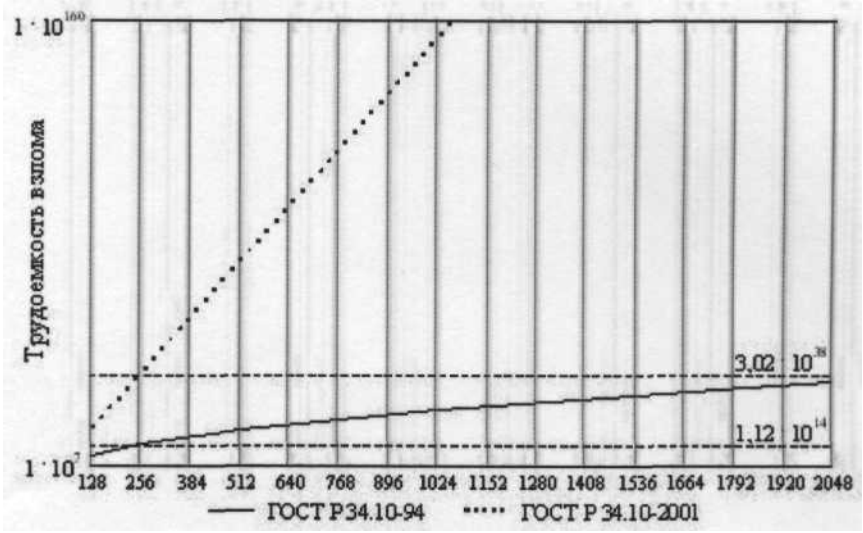

Рис. 2 - Трудоемкость взлома ЭЦП

По оси абсцисс отложен порядок циклической подгруппы группы точек эллиптической кривой q, для нового стандарта, и, соответствующий ему параметр p, из старого стандарта. По оси ординат отложено число операций в логарифмическом масштабе.

Из графика (рис. 2) видно, что, при одинаковом порядке параметров q и p, взлом нового российского стандарта, использующего вычисления в группе точек эллиптической кривой, потребует выполнения большего числа операций, чем взлом старого стандарта, который базируется на использовании несимметричных криптографических преобразований, выполняемых в кольцах. Так, при 256-разрядных q и p, трудоемкость взлома нового стандарта составляет 3,02 x 10^{38}, а старого - 1,12 x 10^{14}.

Также из графика (рис. 2) видно, что для обеспечения трудоемкость взлома ЭЦП, например, 1030 операций в ГОСТ Р 34.10-94 необходимо использовать 1536-разрядное p, а в ГОСТ Р 34.10-2001 достаточно использовать 256-разрядное q.

Основываясь на полученных оценках, можно сделать вывод, что схема ЭЦП ГОСТ Р 34.10-2001, базирующаяся на математическом аппарате эллиптических кривых, является более стойкой по сравнению со схемой ЭЦП ГОСТ Р 34.10-94, основанной на сложности решения задачи дискретного логарифмирования в простом поле. Другими словами в новом российском стандарте ЭЦП можно использовать меньшую длину ключа, чем в старом, без понижения безопасности всей системы.

Следует предположить, что в ближайшие несколько десятилетий получат распространение криптографические алгоритмы и протоколы, в основу построения которых будет положена математика эллиптических кривых.

Выводы:

1. Для всех методов шифрования с открытым ключом математически строго не доказано отсутствие других методов криптоанализа кроме решения задачи полного перебора. Если появятся методы эффективного решения таких задач, то криптосистемы такого типа будут дискредитированы.
2. Асимметричные криптосистемы обладают неоспоримым достоинством по сравнению с симметричными: они позволяют динамически передавать открытые ключи, тогда как при использовании симметричной криптосистемы необходим обмен секретными ключами до начала сеанса защищенной связи.
3. Асимметричные криптоалгоритмы позволяют преодолеть недостатки, присущие системам симметричного шифрования:

- не нужна секретная доставка ключей;
- исчезает квадратическая зависимость числа ключей от числа пользователей.

Однако у асимметричных криптосистем имеются и **недостатки**:

- на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах однонаправленных функций;
- по сравнению с симметричным асимметричное шифрование существенно медленнее, поскольку при зашифровании и расшифровании выполняются весьма трудоемкие операции (в частности, в RSA это возведение одного большого числа в степень, являющуюся другим большим числом). По этой же причине реализация аппаратного шифратора с асимметричным криптоалгоритмом существенно сложнее, чем аппаратная реализация симметричного криптоалгоритма;
- необходимо защищать открытые ключи от подмены.

Реализация криптографических методов зашиты информации.

Проблема реализации методов защиты информации имеет два аспекта:

- разработку средств, реализующих криптографические алгоритмы,
- методику использования этих средств.

Каждый из рассмотренных криптографических методов может быть реализован либо программным, либо аппаратным способом.

Возможность программной реализации обуславливается тем, что все методы криптографического преобразования формальны и могут быть представлены в виде конечной алгоритмической процедуры. Основным достоинством программных методов реализации защиты является их гибкость, т.е. возможность быстрого изменения алгоритмов шифрования. Основным же недостатком программной реализации является существенно меньшее быстродействие по сравнению с аппаратными средствами (примерно в 10 раз).

При аппаратной реализации все процедуры шифрования и дешифрования выполняются специальными электронными схемами. Наибольшее распространение получили модули, реализующие комбинированные методы.

При этом непременным компонентом всех аппаратно реализуемых методов является гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных. Это объясняется тем, что метод гаммирования удачно сочетает в себе высокую криптостойкость и простоту реализации.

Большинство зарубежных серийных средств шифрования основано на американском стандарте DES. Отечественные же разработки, такие как, например, устройство КРИПТОН, используют отечественный стандарт шифрования ГОСТ 28147-89.

Имеются также *комбинированные средства шифрования*, так называемые программно-аппаратные средства. В этом случае в компьютере используется своеобразный «криптографический сопроцессор» – вычислительное устройство, ориентированное на выполнение криптографических операций (сложение по модулю, сдвиг и т.д.). Меняя программное обеспечения для такого устройства, можно выбирать тот или иной метод шифрования. Такой метод объединяет в себе достоинства программных и аппаратных методов.

Таким образом, выбранный комплекс криптографических методов должен сочетать удобство, гибкость и оперативность использования и надежную защиту от злоумышленников циркулирующей в АС информации.

Литература:

[4] Головко Н.И., Новожилов С.В. Методы и средства защиты компьютерной информации. – Череповец: изд. ЧВИИРЭ, 2004г.

[12] Основы современных компьютерных технологий: Учебник/ под ред. Проф. А.Д.Хомоненко – СПб.: КОРОНА принт, 2005г.

[16] Соколов А.В., Шаньгин В.Ф. Защита информации в распределённых корпоративных сетях и системах. – М.: ДМК Пресс, 2002г.