ВЕСТНИК ЮЖНОГО НАУЧНОГО ЦЕНТРА РАН, Том 1, № 3, 2005, стр. 100–108

ЗАЩИТА ИНФОРМАЦИИ

УДК 621.391.037.372

НОВЫЙ ПОДХОД К РЕШЕНИЮ ЗАДАЧ ЗАЩИТЫ ИНФОРМАЦИИ С ПОЗИЦИЙ ВИРТУАЛЬНОГО ШИФРОВАНИЯ

© 2005 г. В.В. Котенко[1], К.Е. Румянцев[1]

Рассматривается новый подход к решению задач защиты информации, основанный на виртуализации процессов шифрования. На основании вывода теоремы шифрования и ее следствий обосновывается возможность обеспечения абсолютной недешифруемости путем виртуализации выборочных пространств. Применение данного подхода в части виртуализации ансамблей ключа открывает принципиально новый вид защиты информации – виртуальное шифрование. Приведенные варианты возможной реализации виртуального шифрования и результаты исследования созданных на этой основе программных комплексов показывают эффективность предложенного подхода.

Среди основных проблем обеспечения информационной безопасности в настоящее время следует обозначить, во-первых, отсутствие действенных подходов, открывающих возможность абсолютной защиты информации; во-вторых, невозможность количественной оценки эффективности самой защиты.

Из определения абсолютной недешифруемости [1] следует, что для ее обеспечения необходимо создать условия, при которых абсолютно исключается возможность получения каких-либо сведений о сообщениях и ключах при несанкционированном доступе к криптограммам. С позиций классической теории информации эта задача сводится к задаче определения условий существования шифра, способного формировать криптограммы, в которых отсутствует информация о соответствующих им сообщениях и ключах, то есть условий теоретической недешифруемости (ТНДШ). Однако с позиций практики нельзя исключать ситуацию, когда цель информационного анализа криптограмм при несанкционированном доступе может не ставиться. Таким образом, для определения условий абсолютной недешифруемости требуется:

1) определить условия существования шифра, способного исключить информацию о сообщении и ключе из криптограммы, то есть условия ТНДШ;

2) установить условия, при которых любой продуктивный прогноз ключа становится невозможным.

Для определения путей выполнения этих требований представим защиту информации некоторого источника U, как инъективное отображение вида

$$\begin{array}{c} \Phi: U^* \rightarrow E^* \\ \uparrow \\ K^* \end{array} \qquad (1)$$

Выражение (1) показывает, что выборочное пространство ансамбля криптограмм (E^*) является результатом инъективного отображения выборочных пространств ансамблей сообщений U^* и ключей K^*, одно из которых (U^*) является исходным, а другое (K^*) – определяющим. Такое представление процесса защиты информации позволяет снять существующую в настоящее время неоднозначность в определении видов защиты информации. С его позиций они могут быть определены как:

– шифрование, ансамбли $X^*K^*E^*$ дискретные;

– аналоговое скремблирование, ансамбли X^* и E^* непрерывные, ансамбль K^* дискретный;

– цифровое скремблирование, ансамбль X^* непрерывный, ансамбли K^* и E^* дискретные.

Кроме этого, предложенное представление (1) устраняет значительную неопределенность в соотношении понятий шифрования и кодирования для дискретных источников. Из него следует, что шифрование можно рассматривать как кодирование с изменяющимся по закону ключа кодовым словарем. Это также во многом объясняет принятое в практических приложениях включение в состав понятия ключа таких понятий, как ключевые данные (исходный ключ) и развернутый (рабочий) ключ.

[1] Таганрогский государственный радиотехнический университет, г. Таганрог.

Учитывая введенное определение шифрования как кодирования с изменяющимся кодовым словарем, вполне логичным путем определения условий выполнения первого требования для дискретных источников является вывод теоремы шифрования. Что касается второго требования, то для определения условий его выполнения с позиции теории информации вполне достаточно проведения анализа факторов, влияющих на изменение энтропии ансамбля ключа. Полученные таким образом результаты в последующем могут быть обобщены для непрерывных источников.

Процесс защиты информации при кодировании источника U^* на основании (1) можно представить следующим образом. На каждом i-м шаге шифрования Φ^* сообщение $u(i) = (u_{i1}...u_{iLi})$ преобразуется в криптограмму $e(i) = (e_{i1}...e_{ini})$. Данное преобразование однозначно определяется ключом $k(i) = (k_{i1}...k_{iri})$. Сообщения, криптограммы и ключи определяются соответствующими ансамблями, то есть $u(i) \in U^*$, $e(i) \in E^*$ и $k(i) \in K^*$. При этом составляющие их буквы являются буквами соответствующих алфавитов, то есть $u_{ij} \in A$, $e_{ij} \in B$ и $k_{ij} \in C$, где $A = (a_1...a_{m1})$ – алфавит источника, $D = (d_1...d_{m2})$ – алфавит криптограмм, $C = (c_1...c_N)$ – алфавит ключа. Ансамбль ключа представляет собой совместный ансамбль X^*Y^*, где X^* – ансамбль ключевых данных, а Y^* – ансамбль ключевых последовательностей.

Теорема шифрования для дискретного источника. Пусть шифрование Φ дискретного источника U^* определяется некоторыми ансамблями ключей K^* и криптограмм E^*. Тогда, если среднее количество взаимной информации равно

$$I[U^*K^*; E^*] = 0, \qquad (2)$$

то всегда существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Доказательство. Из определения теоретической недешифруемости следует, что

$$J[u(i)k(i); e(i)] = 0 \text{ для всех } i, \qquad (3)$$

то есть количество информации об i-м сообщении и i-м ключе, содержащееся в i-й криптограмме, должно быть равным нулю.

Среднее количество взаимной информации о сообщениях и ключах в криптограмме определяется как

$$I[U^*K^*; E^*] = M[J[u(i)k(i); e(i)]], \qquad (4)$$

где $M[J[u(i)k(i); e(i)]]$ – функция математического ожидания. Так как количество информации всегда неотрицательная величина, то есть $J[u(i)k(i); e(i)] \geq 0$, то равенство (4) будет однозначно свидетельствовать о выполнении (3). Что и требовалось доказать.

Из данной теоремы может быть получен ряд практически важных следствий [1].

Следствие 1. Если при шифровании Φ дискретного источника ансамбли сообщений U^* и ключей K^* статистически не связаны с ансамблем криптограмм E^*, то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Следствие 2. Если при шифровании Φ дискретного источника ансамбли сообщений U^* и ключевых последовательностей Y^* статистически не связаны с ансамблем криптограмм E^*, то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Здесь необходимо отметить, что обычно ансамбль ключа принято представлять как совместный ансамбль X^*Y^* ключевых данных и ключевых последовательностей. Кроме того, из (1) следует, что определенному значению ключевых данных из множества X^* должно соответствовать строго определенное подмножество ключевых последовательностей из множества Y^*. Отсюда следует, что ключевые данные определяют разбиение множества Y^* на подмножества. Принимая во внимание требования однозначности дешифрования, можно считать, что аналогичному разбиению подвергается и совместный ансамбль U^* X^* E^*. Такое представление процесса шифрования приводит (2) к виду

$$I[U^*K^*; E^*] = \sup_{X^*} I[U^*_p Y^*_p; E^*_p], \qquad (5)$$

где $I[U^*_p Y^*_p; E^*_p]$ – среднее количество взаимной информации разбиений ансамблей U^*, Y^* и E^*.

Следствие 3. Если при шифровании Φ дискретного источника формирование криптограмм сопровождается увеличением средней неопределенности ключей при условии их статистической зависимости от сообщений, причем

$$H[K^*/U^*E^*] - H[K^*/U^*] = I[U^*; E^*], \qquad (6)$$

то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Данное следствие показывает возможность существования теоретически недешифруемых шифров при статистической зависимости сообщений и криптограмм. При этом изначально допускается, что ансамбли U^* и K^* статистически связаны и отсутствие этой статистической зависимости рассматривается лишь как частный случай, при котором (6) принимает вид

$$H[K^*/E^*] - H[K^*] = I[U^*; E^*], \qquad (7)$$

откуда с учетом того, что $I[K^*; E^*] = H[K^*] - H[K^*/E^*]$, следует

$$I[K^*; E^*] = -I[U^*; E^*]. \qquad (8)$$

Из равенства (8) видно, что при статистически независимых ансамблях сообщений U^* и ключей K^* существование теоретически недешифруемых

шифров допускает наличие в криптограммах информации о сообщениях и ключах. Однако при этом среднее количество взаимной информации $I[K^*; E^*]$ должно быть точно равно среднему количеству взаимной информации $I[U^*; E^*]$ с обратным знаком. Знак минус при $I[U^*; E^*]$ в (8) можно трактовать как введение в криптограммы ложной информации о сообщениях путем установления статистической зависимости между ключами и криптограммами при шифровании. В свою очередь, если в выражении (6) учесть, что $H[K^*/U^*]–H[K^*/U^*E^*] = I[K^*; E^*/U^*]$ и в соответствии с этим привести его к виду

$$–I[K^*; E^*/U^*] = I[U^*; E^*], \qquad (9)$$

то становится понятным и общий физический смысл следствия 3. Оказывается, что теоретически недешифруемые шифры могут существовать и при статистической зависимости ансамблей сообщений, ключей и криптограмм, если шифрование предполагает увеличение средней условной неопределенности ключей. Причем это увеличение должно сопровождаться введением ложной информации о сообщениях в формируемые криптограммы.

Применение в качестве ансамбля ключей K^* совместного ансамбля X^*Y^* ключевых данных и ключевых последовательностей требует конкретизации рассмотренного выше следствия теоремы шифрования.

Следствие 4. *Если при шифровании Ф дискретного источника формирование криптограмм сопровождается увеличением средней неопределенности ключевых последовательностей при условии их статистической зависимости от сообщений, причем значение этого увеличения точно соответствует значению среднего количества взаимной информации сообщений и криптограмм, то есть*

$$H[Y_p^*/U_p^*E_p^*] - H[Y_p^*/U_p^*] = I[U_p^*; E_p^*], \qquad (10)$$

то существует шифр Φ_0, обеспечивающий теоретическую недешифруемость.

Следствия 3 и 4 теоремы шифрования показывают возможность существования принципиально нового подхода к решению задач защиты информации, состоящего в допущении теоретически недешифруемых шифров при статистической зависимости ансамблей сообщений, криптограмм и ключей. Взгляд на защиту информации с этих позиций открывает принципиально новую область исследований в направлении практической реализации шифров, потенциально способных обеспечить абсолютную недешифруемость.

Теорема шифрования и ее следствия открывают возможность аналитического определения показателей качества шифрования. В виде такого показателя может выступать эффективность шифрования. Эффективность шифрования Ф дискретного источника U^* определим как

$$D(Ф, U^*) = C(Ф, U^*)–H[K^*/U^*], \qquad (11)$$

где $C(Ф, U^*)$ – стойкость шифрования,

$$C(Ф,U^*) = H[K^*/U^*E^*]. \qquad (12)$$

Исходя из теоремы шифрования и следствия 3, можно выделить две области возможных значений эффективности шифрования:

1) область неотрицательных значений $D(Ф, U^*) \geq 0$, соответствующих теоретически недешифруемым шифрам;

2) область отрицательных значений $D(Ф, U^*) < 0$, при которых теоретическая недешифруемость не обеспечивается.

Равенство $D(Ф, U^*)$ соответствует нулю согласно следствию 1, случаю статистической независимости ансамблей ключей K^* и сообщений U^* от ансамбля криптограмм E^*. При этом изменение $D(Ф, U^*)$ в области отрицательных значений от $– H[K^*/U^*]$ до нуля характеризует уменьшение статистической зависимости U^* и K^* от E^*.

В частном случае, когда ансамбли U^* и K^* статистически независимы, выражение (11) принимает вид

$$D(Ф,U^*) = C(Ф,U^*)–H[K^*], \qquad (13)$$

где $C(Ф,U^*) = H[K^*/E^*]$.

С позиции традиционного подхода, предполагающего обязательное выполнение неравенства $H[K^*] \geq H[K^*/E^*]$ при шифровании Ф, диапазон возможных значений $D(Ф, U^*)$ в данном случае определяется как

$$–H[K^*] < D(Ф,U^*) \leq 0. \qquad (14)$$

При этом диапазон значений стойкости шифрования находится в пределах

$$0 < C(Ф, U^*) \leq H[K^*]. \qquad (15)$$

Как в (14), так и в (15) теоретическая недешифруемость обеспечивается только при достижении $D(Ф, U^*)$ и $C(Ф, U^*)$ верхних границ отмеченных диапазонов, то есть при $D(Ф, U^*) = 0$ и $C(Ф, U^*) = H[K^*]$. Не трудно заметить, что в этом случае шифр, недешифруемый теоретически, на практике таковым может не оказаться. Так, дискретный ансамбль предполагает конечную энтропию, которая при несанкционированном доступе может быть сведена к минимуму путем простого последовательного перебора элементов выборочного пространства K^*. Вывод достаточно очевиден. Абсолютно исключить эту возможность позволит бесконечная энтропия ансамбля ключа $H[K^*] = \infty$, когда $D[Ф, U^*] = \infty$ и $C(Ф, U^*) = \infty$. Этот вывод согласуется со следствием 3 и введенными на его основании диапазо-

нами эффективности шифрования (11). С этих позиций становится понятным физический смысл проблемы, перед которой стоит теория и практика защиты информации сегодня. С одной стороны, выясняется, что теоретическая недешифруемость и абсолютная недешифруемость – это не идентичные понятия. При этом для достижения абсолютной недешифруемости требуется выполнение одного из двух условий:

1) обеспечение бесконечной энтропии ансамбля ключа;

2) обеспечение при конечной энтропии ансамбля ключа неравенства

$H[K^*/E^*] > H[K^*]$, где $H[K^*/E^*]$ стремится к бесконечности.

С другой стороны, оказывается, что с позиции существующих подходов в теории защиты информации выполнение этих условий не представляется возможным. Образно говоря, существующая теория не в состоянии обеспечить более или менее понятной и убедительной целью постоянно возрастающие запросы практики защиты информации. Обобщая данную проблему на случай статистической зависимости ансамблей сообщений и ключей, на основании (11) и теоремы шифрования можно выделить два возможных направления ее решения:

1) поиск подходов, позволяющих вывести $D(\Phi, U^*)$ в область положительных значений, где $D(\Phi, U^*) > 0$;

2) поиск подходов, предусматривающих возможность смещения верхней границы диапазона изменения энтропии ключа в область бесконечно больших значений.

В случае представления ансамбля ключей в виде совместного ансамбля X^*Y^* ключевых данных и ключевых последовательностей эффективность шифрования определяется выражением вида

$$D(\Phi, \underset{X^*}{U^*}) = \sup D_p(\Phi, U_p^*), \qquad (16)$$

$$D_p(\Phi, U^*) = \sum_{ijn} P(U_i Y_j E_n) \log \frac{P(Y_j / U_i)}{P(Y_j / U_i E_n)}, \qquad (17)$$

где верхняя грань берется по всем разбиениям ансамбля U^*, всем разбиениям ансамбля E^* и всем разбиениям ансамбля Y^*, заданных ансамблем X^*.

Аналогично (16) стойкость шифрования в данном случае может быть определена как

$$C(\Phi, \underset{X^*}{U^*}) = \sup_{X^*} C_p(\Phi, U_p^*), \qquad (18)$$

$$C_p(\Phi, U^*) = \sum_{ijn} P(U_i Y_j E_n) \log \frac{1}{P(Y_j / U_i E_n)}, \qquad (19)$$

где верхняя граница берется по всем разбиениям ансамбля U^*, всем разбиениям ансамблей E^* и Y^*, заданных ансамблем X^*.

Преобразовав (19) к виду

$$C_p(\Phi, U_p^*) =$$

$$= \sum_{ijn} P(U_i Y_j E_n) \log \frac{P(U_i E_n)}{P(Y_j) P(U_i / Y_j) P(E_n / U_i Y_j)}, \qquad (20)$$

получаем

$$C_p(\Phi, U_p^*) = H[Y_p^*] - I[U_p^* Y_p^*] - I[E_p^*; Y_p^* / U_p^*]. \qquad (21)$$

При статистической независимости ансамблей сообщений, криптограмм и ключевых последовательностей выражение (21) принимает вид

$$C_p(\Phi, U_p^*) = H[Y_p^*],$$

что свидетельствует о том, что в данном случае стойкость шифрования однозначно определяется энтропией ключевых последовательностей, относящихся к определенному значению ключевых данных из выборочного пространства ансамбля X^*. Принимая во внимание (21), на основании (18) нетрудно прийти к выводу, что абсолютная недешифруемость ($C_p(\Phi, U_p^*) = \infty$) в случае совместного X^*Y^* ансамбля ключей возможна:

1) при бесконечно больших значениях энтропий ансамблей ключевых последовательностей разбиений ($H[Y_p^*] = \infty$);

2) при бесконечной энтропии ансамбля ключевых данных.

С позиции современной теории информации этот вывод применительно к шифрованию дискретных источников на первый взгляд может показаться по меньшей мере проблематичным. Прежде всего это относится к допущению самой возможности существования бесконечной энтропии дискретных ансамблей.

Данную проблему позволяет решить подход, основанный на применении виртуальных выборочных пространств. Отличительной особенностью этого подхода является наличие этапов виртуализации и девиртуализации. В данном случае под виртуализацией понимается переход от дискретных выборочных пространств к непрерывным, которые определяются как виртуальные. Отсюда девиртуализация представляет обратный переход от виртуальных выборочных пространств к дискретным, которые определяются выбранной целью исследований. С позиций теории связи данный подход можно интерпретировать как преобразование цифрового процесса в аналоговый, обработку последнего выбранным способом и последующее цифровое преобразование результатов обработки. Известно, что основным методом такого цифрового преобразования является метод импульсно-кодовой модуляции (ИКМ). К особенностям ИКМ относится возможность изменения характеристик

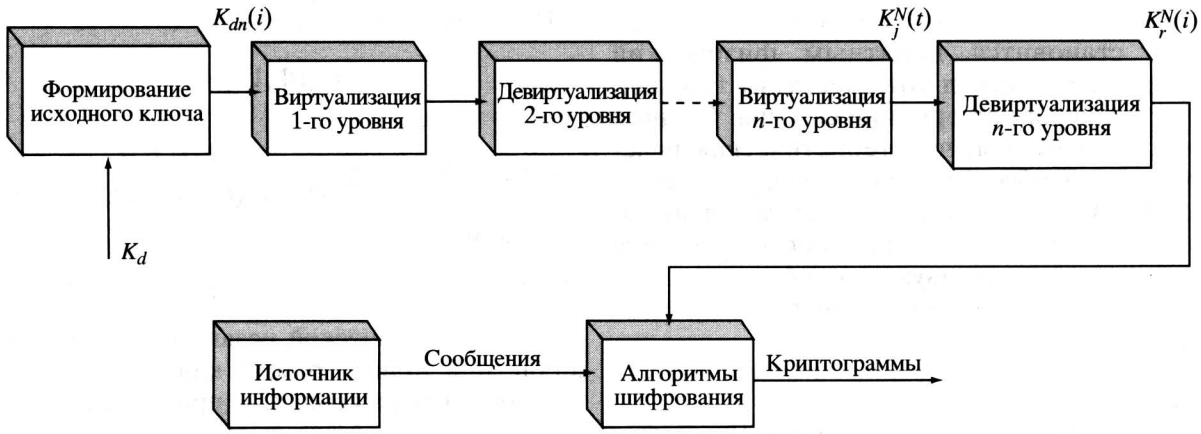

Рис. 1. Схема алгоритма последовательного усложнения виртуальных выборочных пространств ансамблей ключа

формируемого цифрового процесса путем подбора параметров цифрового представления. Именно эта особенность объясняет физический смысл возможностей предложенного подхода. Переход к виртуальным выборочным пространствам означает снятие ограничений на изменение энтропии дискретных ансамблей, что открывает возможность выполнения условий абсолютной недешифруемости. Естественно, что полученные при этом результаты будут выходить за границы современных представлений о возможности их практической реализации. Согласование с этими границами требует введение определенных ограничений в ходе девиртуализации. При этом оптимизация такого согласования всегда может быть достигнута путем подбора определенной совокупности ограничений.

Применение данного подхода при решении задач защиты информации дискретных источников в части виртуализации ансамблей ключа открывает новый вид шифрования, который можно назвать виртуальным. Виртуальным шифрованием будем считать шифрование, при котором ансамбли сообщений и криптограмм являются дискретными, а ансамбль ключа формируется путём виртуализации исходного дискретного ансамбля в непрерывный и девиртуализации последнего в квазинепрерывный. При этом не накладывается никаких ограничений на выбор процедур виртуализации и девиртуализации. Это открывает широкий спектр возможностей одновременного (параллельного) или поэтапного (последовательного) применения различных процедур виртуализации и девиртуализации при формировании результирующего квазинепрерывного ансамбля.

Виртуализация выборочных пространств ансамблей ключа на основе их многомерного представления занимает особое место среди возможных вариантов применения рассматриваемого подхода. В данном случае под многомерным представлением понимается представление в виде совокупности процедур виртуализации VIR_j, каждая из которых рассматривается как отдельное измерение. С этих позиций процесс формирования виртуального ключа $K_V^M(t)$ может быть представлен как виртуализация исходного ключа в некотором М-мерном пространстве, одновременно или последовательно по всем его измерениям, с последующей унификацией результатов виртуализации в некоторую функцию этого пространства, которая будет представлять собой виртуальный ключ:

$$K_V^M(t) = UNIF(K_V^j(t)), \qquad (22),$$

где $UNIF$ (.) – процедура унификации; VIR_j (.) – процедура виртуализации, определяющая j-е измерение; $K_V^j(t)$ – проекция виртуального ключа на j-е измерение.

Развернутый ключ формируется путем девиртуализации $DVIR_j$ полученного виртуального ключа:

$$K_r^M(i) = DVIR_M(K_V^M(t)). \qquad (23)$$

Выражения (22) и (23) определяют общий алгоритм формирования развернутого ключа при многомерном представлении виртуальных выборочных пространств ансамблей ключа. Можно выделить два основных направления реализации данного алгоритма.

Первым из них является шифрование, основанное на последовательном усложнении виртуальных выборочных пространств ансамблей ключа. Его основу составляет рекуррентный алгоритм формирования виртуального ключа:

$$K_V^j(t) = VIR_j(DVIR_{j-1}(K_V^{j-1}(t))), \quad j = 1 \ldots N, \quad (24)$$

где j – порядок уровня последовательного усложнения.

Полученный алгоритм предполагает многократную последовательную виртуализацию и девиртуализацию ансамбля ключа (рис. 1). При этом на каждом шаге виртуализации в качестве

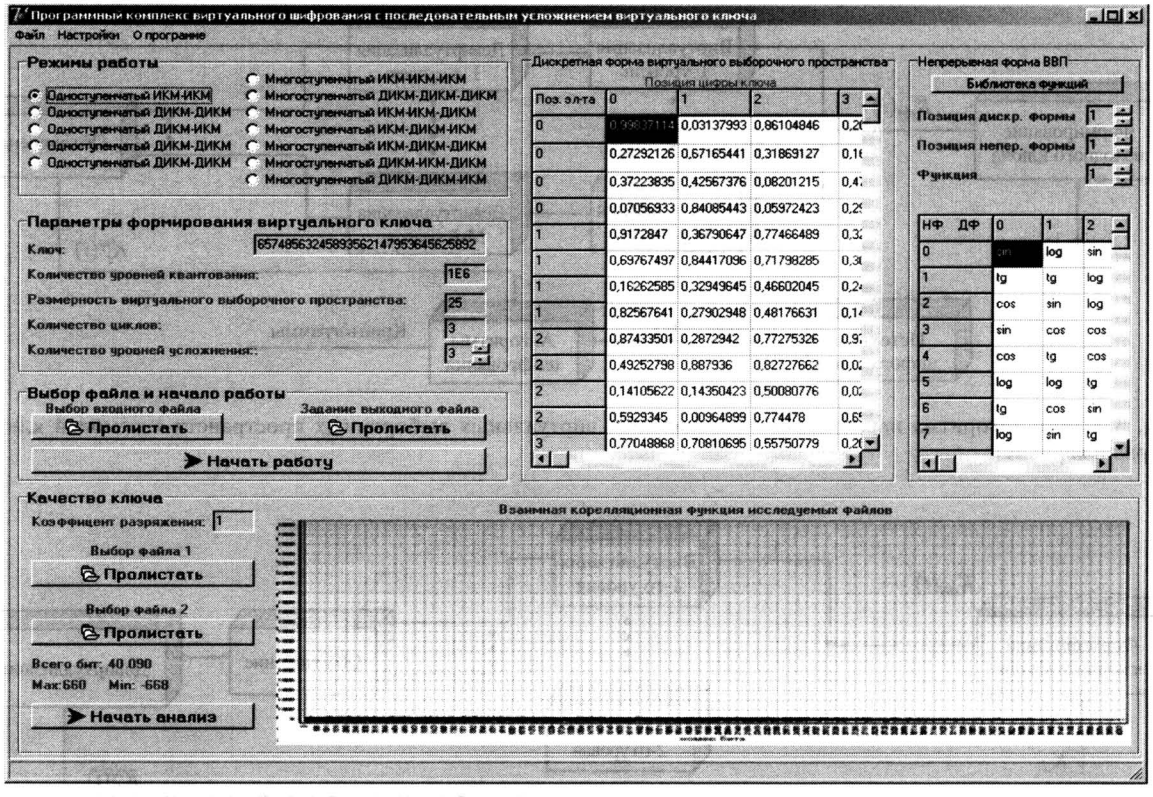

Рис. 2. Программный комплекс шифрования с последовательным усложнением виртуального ключа

исходного ключа выступает результат девиртуализации виртуального ключа, полученного на предыдущем шаге.

Начальным условием $DVIR_0(K_V^0(t))$ функционирования данного алгоритма является исходный ключ $K_{nd}(i)$, формируемый на основании заданных ключевых данных K_d:

$$DVIR_0(K_V^0(t)) = K_{nd}(i). \qquad (25)$$

Развернутый ключ $K_n^N(i)$ формируется путем девиртуализации виртуального ключа, полученного на конечном N-м шаге усложнения:

$$K_n^N(i) = DVIR_N(K_V^N(t)) \qquad (26)$$

На основании приведенного подхода было получено семейство способов шифрования с последовательным усложнением виртуального ключа, открывающих возможность обеспечения абсолютной недешифруемости. Реализация данных способов позволила создать программный комплекс шифрования (рис. 2), обладающий уникальными возможностями. Экспериментальные исследования показали высокую надежность и эффективность данного комплекса.

Вторым направлением реализации общего алгоритма (22)–(23) является параллельное усложнение виртуальных выборочных пространств. Под параллельным усложнением в данном случае понимается формирование виртуального ключа и его девиртуализация одновременно по M-независимым каналам. При этом развернутый ключ может формироваться двумя путями: во-первых, путем объединения (унификации) результатов девиртуализации используемых каналов; во-вторых, путем объединения (унификации) результатов виртуализации используемых каналов и последующей девиртуализации результата унификации.

Первый путь приводит к варианту (рис. 3) алгоритма формирования рабочего ключа (первый вариант) вида

$$K_r^M(i) = UNIF_R(DVIR_j(K_V^i(t)))$$

$$K_V^j(t) = VIR_j(K_{nd}(i)) \qquad (27)$$

где $UNIF\ (\ .\ )$ – процедура объединения (унификации), $VIR_j\ (\ .\ )$ – процедура виртуализации j-го канала; $DVIR_j\ (\ .\ )$ – процедура девиртуализации j-го канала; $K_V^j(t)$ – виртуальный ключ j-го канала; $K_{nd}(i)$ – исходный ключ, формируемый на основании заданных ключевых данных K_d.

Порядок усложнения виртуального выборочного пространства в данном случае определяется числом параллельно используемых каналов j.

Второй путь приводит к варианту (рис. 4) алгоритма формирования рабочего ключа (второй вариант) вида

$$K_r^M(i) = DVIR_M(UNIF_R((K_V^j(t))),$$

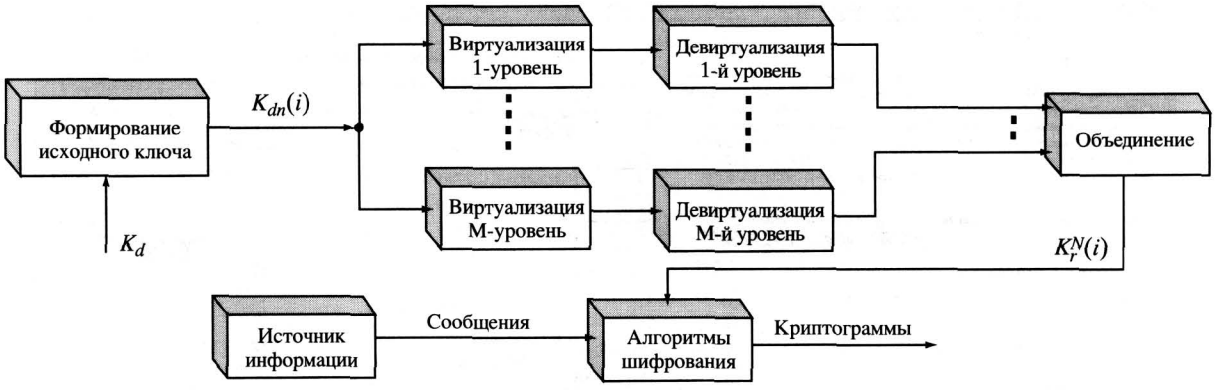

Рис. 3. Схема алгоритма параллельного усложнения виртуальных выборочных пространств ансамблей ключа (первый вариант)

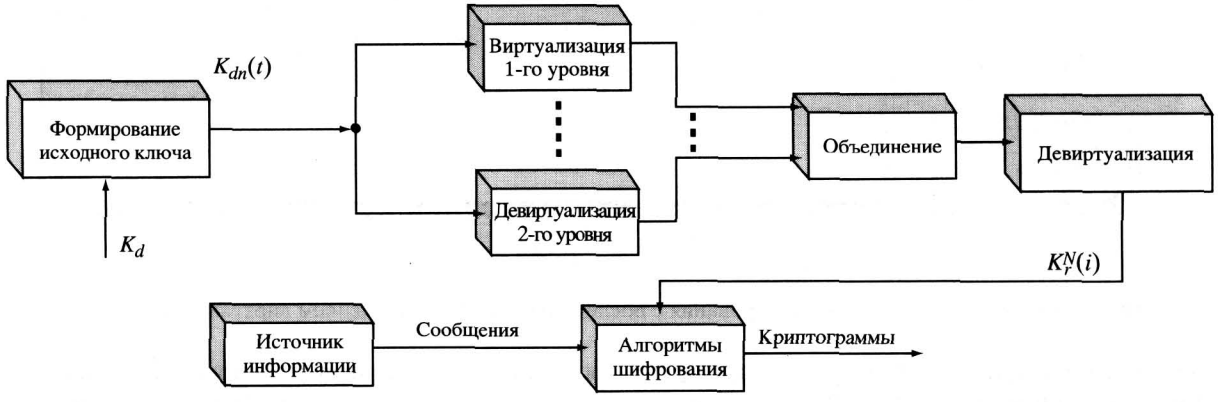

Рис. 4. Схема алгоритма параллельного усложнения виртуальных выборочных пространств ансамблей ключа (второй вариант)

$$K_V^j(t) = VIR_j(K_{nd}(i)). \qquad (28)$$

Порядок усложнения в данном случае также определяется числом параллельно используемых каналов j.

Приведенные алгоритмы является общими. Их конкретизация производится путем выбора процедуры унификации. Необходимо подчеркнуть, что здесь для исследователя открывается широкое поле деятельности. Например, в качестве этой процедуры могут быть использованы суммирование и произведение результатов девиртуализации каналов. В первом случае алгоритм формирования развернутого ключа принимает вид, представленный выражением (29), во втором – выражением (30):

$$K_r^M(i) = \prod_{j=1}^{M} DVIR_j(K_V^j(t)), \qquad (29)$$

$$K_r^M(i) = \sum_{j=1}^{M} DVIR_j(K_V^j(t)). \qquad (30)$$

Компьютерная реализация приведенных алгоритмов позволила создать программный комплекс шифрования (рис. 5), потенциально способный обеспечить абсолютную недешифруемость. Исследования характеристик данного комплекса дают обнадеживающие результаты, представляющие научный и практический интерес.

Экспериментальное исследование эффективности этого комплекса, проведенное с использованием набора статистических тестов NIST STS (табл. 1), показало его преимущество по отношению к существующим шифрам, в том числе и по отношению к шифру Rijndael, разработанному в рамках AES и рекомендованному в качестве стандарта шифрования XXI века. Так, даже при длине ключа 1 бит (примитивный вариант) обеспечивается качество шифрования, аналогичное качеству современных шифров с длиной ключа 128 бит и более. Причём даже незначительное увеличение длины ключа до 4 бит (простой вариант) позволяет значительно улучшить эти показатели.

В целом из результатов исследования представленных комплексов следует, что их реализация в режиме генератора случайных последовательностей потенциально способна обеспечить показатели, значительно превосходящие показатели из-

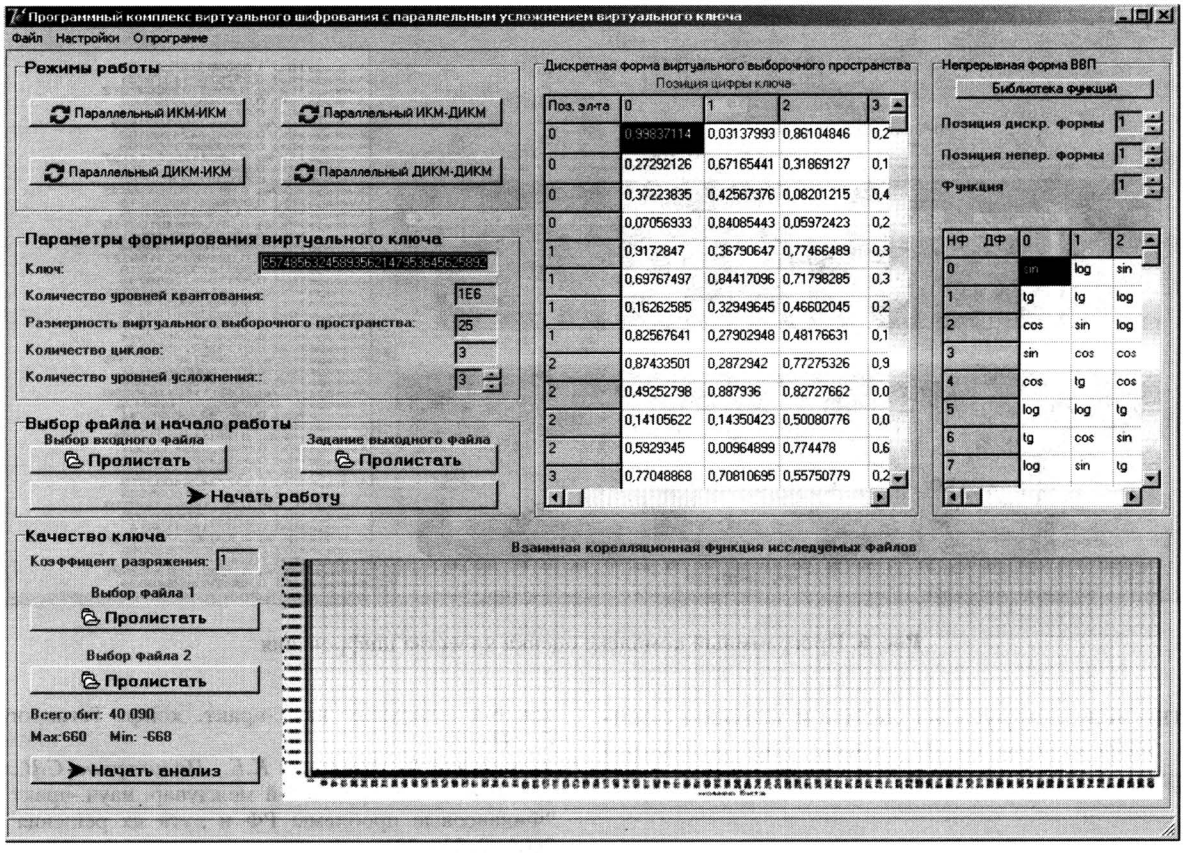

Рис. 5. Программный комплекс шифрования с параллельным усложнением виртуального ключа

вестных аналогов. Учитывая, что выработка случайной (псевдослучайной) последовательности составляет основу формирования развернутого ключа, характеристики которого в конечном итоге определяют качество шифрования, данный вывод может быть обобщен на все режимы применения разработанных программных комплексов. Это является наглядным подтверждением эффективности и практической значимости предложенного подхода.

Кроме этого необходимо отметить еще одну замечательную особенность данного подхода. Его теоретическое обоснование открывает возможность количественной оценки качества защиты информации. Так, выражения (16)–(19) можно рассматривать как математическую модель оценки качества шифрования с позиции теории информации. Данная модель послужила основой разработки универсальной компьютерной технологии количественной оценки качества шифров. Результатом этого явилось создание семейства программных комплексов, позволяющих получать объективную оценку эффективности применяемых шифров, в том числе и в реальном масштабе времени (рис. 6).

Приведенные результаты получены в ходе исследований, проводимых авторами при поддержке гранта Министерства образования РФ Т02-03.1-816. Они открывают принципиально новую область исследований в направлении создания аб-

Таблица 1. Результаты экспериментального исследования эффективности набором статистических тестов NIST STS

Генератор	Количество тестов, в которых тестирование прошли более 99% последовательностей	Количество тестов, в которых тестирование прошли более 96% последовательностей
BBS	134 (70,8%)	189 (100%)
Гряда-1М	130 (68,8%)	184 (97,4%)
Примитивный вариант	134 (70,8%)	189 (100%)
Простой вариант	150 (79,4%)	189 (100%)

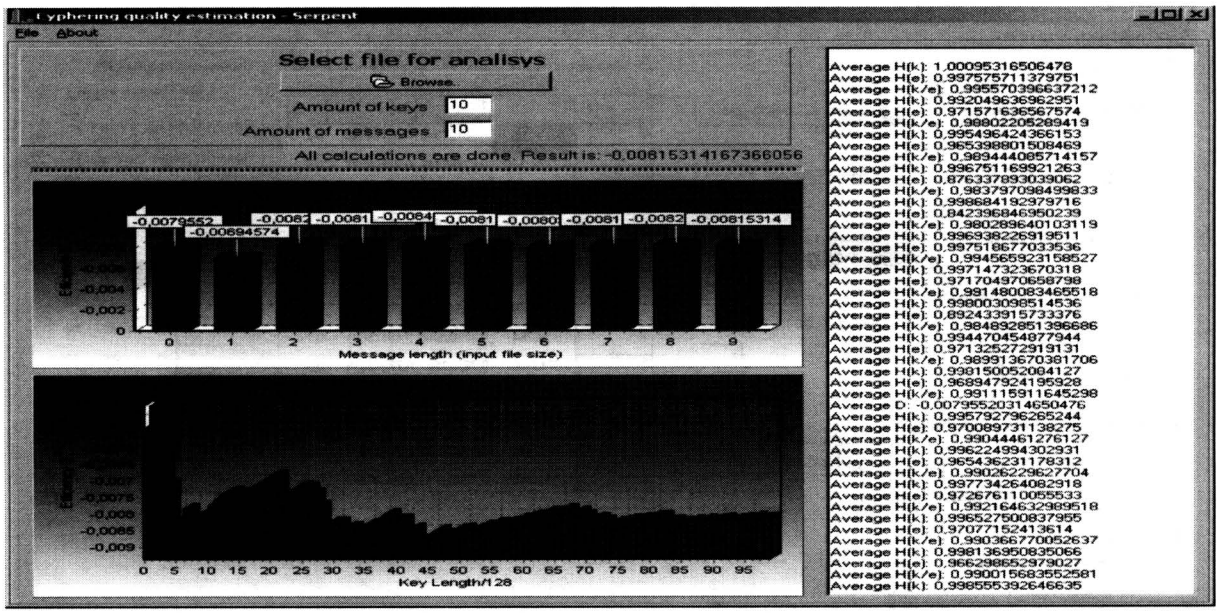

Рис. 6. Программный комплекс оценки качества шифрования

солютно недешифруемых систем и методов оценки их эффективности на основе виртуализации информационных потоков.

ЛИТЕРАТУРА

1. *Котенко В.В., Румянцев К.Е., Поликарпов С.В.* // Вопросы защиты информации, 2004. № 1. С. 16–22.
2. *Котенко В.В., Поликарпов С.В.* // Вопросы защиты информации, 2002. № 2. С. 47–52.
3. *Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б.* // Современные наукоемкие технологии, 2004. № 2. С. 42.
4. *Котенко В.В.* // Информационная безопасность: Сб. трудов 6-й междунар. науч.-практ. конф. Таганрог, 2004. С. 144–151.
5. *Котенко В.В., Румянцев К.Е., Поликарпов С.В., Левендян И.Б.* // Сб. трудов 5-й междунар. науч.-практ. конф. "Финансовые проблемы РФ и пути их решения". СПб, 2004. С. 230–231.
6. *Котенко В.В., Румянцев К.Е, Левендян И.Б., Поликарпов С.В.* // Информационная безопасность: Сб. трудов 6-й междунар. науч.-практ. конф. Таганрог, 2004. С. 295–297.
7. *Котенко В.В., Румянцев К.Е., Левендян И.Б., Поликарпов С.В.* // Сб. трудов 5-й междунар. науч.-практ. конф. "Современные информационные и электронные технологии" (СИЭТ-2004). Одесса, 2004. С. 145.
8. *Kotenko V.V., Rumjantsev K.E., Polycarpov S.V., Levendyan I.B.* // Proc. of the International Scientific Conference "Manufacturing technologies". Rome, 2004. P. 42–43.

NEW APPROACH TO INFORMATION SECURITY PROBLEMS SOLVING FROM VIRTUAL CIPHERING POSITIONS

V.V. Kotenko, K.E. Rumjantsev

New approach to information security problems solving based on ciphering processes virtualization is considered. On the base of ciphering theorem and its conclusions possibility of absolute undecodable capability is given based on selective spaces virtualization. Using of this approach in the case of key ensembles virtualization opens new way of information security – virtual ciphering. Given variants of possible realization of virtual ciphering and results of based software researches shows efficiency of given approach.

REFERENCES

1. Kotenko V.V., Rumyantsev K.E., Polikarpov S.V. 2004. *Voprosy zashchity informatsii*. (1): 16−22. (In Russian).
2. Kotenko V.V., Polikarpov S.V. 2002. *Voprosy zashchity informatsii*. (2): 47−52. (In Russian).
3. Kotenko V.V., Rumyantsev K.E., Polikarpov S.V., Levendyan I.B. 2004. *Sovremennye naukoemkie tekhnologii*. (2): 42. (In Russian).
4. Kotenko V.V. 2004. *Informatsionnaya bezopasnost'. Sb. trudov 6-y mezhdunar. nauch.-prakt. konf.* [*Information Security. Proceedings of the 6th International Scientific and Practical Conference*]. Taganrog: 144–151. (In Russian).
5. Kotenko V.V., Rumyantsev K.E., Polikarpov S.V., Levendyan I.B. 2004. *Finansovye problemy RF i puti ikh resheniya. Sbornik trudov 5-y mezhdunar. nauch.-prakt. konf.* [*The financial problems of the Russian Federation and their solutions. Proceedings of the 5th Intern. scientific and practical. conf.*]. St. Petersburg: 230–231. (In Russian).
6. Kotenko V.V., Rumyantsev K.E., Levendyan I.B., Polikarpov S.V. 2004. In: *Informatsionnaya bezopasnost'. Sb. trudov 6-y mezhdunar. nauch.-prakt. konf.* [*Information Security. Proceedings of the 6th International Scientific and Practical Conference*]. Taganrog: 295–297. (In Russian).
7. Kotenko V.V., Rumyantsev K.E., Levendyan I.B., Polikarpov S.V. 2004. In: *Sovremennye informatsionnye I elektronnye tekhnologii. Sb. trudov 5-y mezhdunar. nauch.-prakt. konf., Odessa, 2004* (*SIET-2004*). [*Modern information and electronic technologies. Coll. works of the 5th Intern. scientific and practical. conf., Odessa, 2004*. (*SIET 2004*)]. P. 145. (In Russian).
8. Kotenko V.V., Rumjantsev K.E, Polycarpov S.V., Levendyan I.B. 2004. In: *Proc. of the International Scientific Conference* "*Manufacturing technologies*". *Rome, 2004*. P. 42–43.