3. *Соколов А.В., Шаньгин В.Ф.* Защита информации в распределенных корпоративних сетях и системах. – М.: ДМК Пресс, 2002. – 656 с.

4. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. — СПб.: «Наука и техника», 2004. — 384 с.

5. Юдін О.К. Захист інформації в мережах передачі даних / О.К.Юдін, Г.Ф. Конахович, О.Г. Корченко // Підручник МОН України. – К.: Видавництво *DIRECTLINE*, 2009.-714с., іл.

Надійшла 20.01.2010

УДК 004.056.55(043.2) **Стасюк А.И., Корченко А.А., Малофеев А.В.**

ИСПОЛЬЗОВАНИЕ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ ДЛЯ ВЫБОРА КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ШИФРОВАНИЯ

На сегодняшний день существует большое количество различных алгоритмов шифрования. Каждый из них имеет индивидуальные характеристики, такие как количество раундов, длинна ключа, сложность реализации и другие. Поэтому часто, при построении систем защиты информации, возникает проблема выбора криптографического алгоритма отвечающего определенным критериям.

Одним из общепринятых подходов при построении криптосистем в настоящее время является выбор понравившегося разработчикам алгоритма по одному из критериев, например криптостойкость и реализация этого шифроалгоритма без учета других характеристик. Такой однокритериальный подход не всегда является целесообразным и оправданным. В результате недостаточного или некачественного учета других факторов возможно создание нестойких криптосистем. Поэтому необходим другой синтетический многокритериальный подход.

В [6] автор приводит математический аппарат, который позволяет осуществить выбор алгоритма шифрования. Но автор учитывает немногочисленные критерии алгоритмов, в частности длину ключа. В [4] приведено сравнение алгоритмов относительно большого количества характеристик, выделены их слабые и сильные стороны. Однако автор не предоставляет инструменты выбора криптографического алгоритма по заданным критериям. Это важно при построении аппаратных или программных средств криптографической защиты информации.

В этой связи целью данной работы является разработка методики выбора алгоритма шифрования для средств защиты. Очевидно, что такие алгоритмы должны наиболее полно обеспечивать криптостойкость, производительность и эффективность реализации [2]. Однако удовлетворение наилучшим образом, приведенным требованиям, зачастую носит противоречивый и нечеткий характер. Поэтому для решения многокритериальной задачи выбора алгоритма шифрования использована теория нечетких множеств. В [1, 5] рассматривается соответственный математический аппарат, используемый в методах оценки альтернатив.

В данном случае критерии определяют некоторые свойства алгоритмов шифрования, а оценки альтернатив представляют собой степень соответствия этим свойствам. Таким образом, имеется множество альтернатив (алгоритмов шифрования) $X=\{x_1,...x_m\}$ (где x_i ($i=\overline{1,m}$) алгоритм шифрования, m ($m=\overline{1,k}$) – количество алгоритмов шифрования) и множество критериев (параметров алгоритмов шифрования) $Y=\{y_1,...y_n\}$ (где y_j ($j=\overline{1,n}$) критерий алгоритма, n ($n=\overline{1,s}$) – количество критериев) при этом оценки альтернатив по каждому j-му критерию представлены нечеткими множествами:

$$\underset{\sim}{Y}_j=\{\mu_{y_j}(x_1)/x_1,...\mu_{y_j}(x_m)/x_m\}=\bigcup_{i=1}^{m}\{\mu_{y_j}(x_i)/x_i\},\ j=\overline{1,n}. \quad (1)$$

Каждая альтернатива (алгоритм шифрования) X представляет из себя вектор критериев Y, нечетко определенный на множестве альтернатив по каждому из критериев с функциями принадлежности $\mu_{y_j}(x_i)$ к определенной частной цели (ресурс времени, ресурс памяти, криптостойкость и др.).

Нечеткое отношение $\underset{\sim}{R}$ между множествами альтернатив X и критериев Y есть функция $\underset{\sim}{R}:(X,Y)\to[0,1]$, которая ставит в соответствие каждой паре элементов $(x,y)\in X\times Y$ величину $\mu_R(x,y)\in[0,1]$. В случае сравнения алгоритмов шифрования все критерии имеют разную важность, поэтому их вклад в общее решение представлен как алгебраическое произведение нечеткого множества критериев по каждой альтернативе на нечеткое множество важности критериев $\mu_V(y)$:

$$\mu_{\underset{\sim}{R}_{мдф}}(x,y)=\mu_{\underset{\sim}{y}}(y)\mu_{\underset{\sim}{R}}(x,y). \quad (2)$$

Тогда задачу выбора алгоритма можно свести к нахождению функций принадлежности альтернатив к нечетким частным критериям $\mu_y(x)$. А выбор наилучшего варианта – как поиск альтернативы, имеющей максимальную принадлежность к нечеткой функции цели или же минимальное расстояние от нечеткой целевой функции. В этом случае наилучшей является альтернатива, которая обеспечивает более близкое приближение к множеству одновременно недостижимых значений (целей), т.е. минимальное растояние от альтернатив до целевой функции и определяемое на основании некоторой заранее выбранной нечеткой метрики. В качестве этой метрики используется расстояние Хемминга для нечетких множеств:

$$d(\underset{\sim}{G},\underset{\sim}{X})=\sum_{j=1}^{n}|\mu_{\underset{\sim}{G}}(y_j)-\mu_{\underset{\sim}{X}}(y_j)|, \quad (3)$$

где $\underset{\sim}{X}$ – нечеткое множество альтернатив по всем нечетким критериям, $\underset{\sim}{G}$ – нечеткое множество одновременно недостижимых целей, которое определяется как вторая проекция модифицированного отношения $\underset{\sim}{R}^{(2)}_{мдф}$ на множестве альтернатив и нечетком множестве критериев для данных альтернатив:

$$\mu_{\underset{\sim}{G}}(y)=\vee_x\mu_{\underset{\sim}{R}^{(2)}_{мдф}}(x,y). \quad (4)$$

В определении нечетких множеств могут быть использованы прямые методы, когда эксперт непосредственно может задать для каждого $x\in X$ значение $\mu_y(x)$. Как правило, эти методы задания функции принадлежности, используются для измеряемых понятий. Также могут быть использованы и косвенные методы, когда нет элементарных измеряемых свойств, через которое определяется интересующее нас нечеткое множество или очень сложно сделать количественную оценку, а проще всего сделать сравнительную оценку. Как правило, это методы парных сравнений. Одними из основных критериев, которые определяют выбор алгоритмов шифрования, обеспечивающих заданный уровень безопасности криптосистем, являются:

- запас криптостойкости;
- криптостойкость;
- временной ресурс;
- пространственный ресурс;
- сложность алгоритма;
- сложность программно/аппаратной реализации.

В качестве примера для предлагаемого синтетического подхода по этим критериям построим функции принадлежностей для трех наиболее распространенных алгоритмов шифрования: DES, AES и ГОСТ 28147-89.

В случае сравнения алгоритмов шифрования все критерии имеют разную степень важности. Эта степень важности может определяться одним из методов исследуемых в [1]. Для решения широкого круга практических задач в работе [1] предлагается метод количественного парного сравнения с определением частного (КПСЧ). Степень принадлежности элементов множеству определяется при помощи парных сравнений. По его оценке формируется матрица парных сравнений:

$$V=||v_{ij}||, \qquad (5)$$

где значение v_{ij} выбирается по табл.1 (оценка элемента y_i сравнительно y_j по свойствам V).

Таблица 1

Шкала для построения матрицы суждений

Оценка значимости	Качественная оценка	Примечание
1	Одинаковая значимость	Альтернативы, имеющие одинаковый ранг
3	Слабое преимущество	Преимущество одной альтернативы перед другой малоубедительно
5	Сильное или важное преимущество	Есть надежные доказательства существенного преимущества одной альтернативы над другой
7	Очевидное преимущество	Существуют убедительные свидетельства в пользу одной альтернативы
9	Абсолютное преимущество	Свидетельство в пользу преимущества одной альтернативы над другой с наибольшей мерой убедительности
2,4,6,8	Промежуточные значения	Используются, если необходим компромисс

То есть если i-й элемент доминирует над j-м элементом, то элемент матрицы, что соответствует i-й строке и j-му столбцу заполняется целым числом по девятибалльной шкале из табл.1, а симметричный элемент относительно главной диагонали, что соответствует j-й строке и i-му столбцу Vji заполняется обратным числом 1/Vij.

Для определения значений ФП согласно этого метода функция принадлежности определяется по следующей формуле:

$$\mu_{\underline{Y}}(y_i)=v_{ij}/\sum_{i=1}^{n} v_{ij}, \qquad (6)$$

где v_{ij} – коэффициенты матрицы парных сравнений, а исходные данные представляют собой сформированную на основе экспертного опроса матрицу парных сравнений V, $i,j \in I = \{1,2,...n\}$, причем j выбирается произвольно.

Другими словами для определения величин $\mu_{\underline{Y}}(y_i)$, $i \in I$, необходимо зафиксировать произвольно выбранный столбец j, $j \in I$, матрицы V и вычислить отношения величин элементов v_{ij} к сумме величин всех элементов столбца j.

Для приведения субнормальных нечетких множеств к нормальной форме используем такое выражение [1]:

$$\underset{\sim}{Y}=\bigcup_{i=1}^{n}\{(\mu_V(y_j):\max\mu_V(y_j))/y_j\},\ j=\overline{1,n}. \qquad (7)$$

Пусть Y множество характеристик (критериев) по которым определяется будущая криптосистема и будет выбран алгоритм шифрования. Y={y_1,…y_6}={Зкр, Кр, ИВР, ИПР, СА, СР}, где:

y_1 – запас криптостойкости (Зкр);
y_2 – криптостойкость (Кр);
y_3 – использование временных ресурсов (ИВР);
y_4 – использование пространственных ресурсов (память) (ИПР);
y_5 – сложность алгоритма (СА);
y_6 – сложность реализации (СР).

Нужно построить нечеткое множество $\underset{\sim}{Y}$, которое формализует понятие “Важность“ критериев.

Матрица парных сравнений критериев пронумерованных в порядке представления в множестве Y имеет следующий вид:

$$V=\begin{Vmatrix} 1 & 1/3 & 3 & 3 & 5 & 5 \\ 3 & 1 & 5 & 5 & 7 & 7 \\ 1/3 & 1/5 & 1 & 1 & 3 & 3 \\ 1/3 & 1/5 & 1 & 1 & 3 & 3 \\ 1/5 & 1/7 & 1/3 & 1/3 & 1 & 3 \\ 1/5 & 1/7 & 1/3 & 1/3 & 2 & 1 \end{Vmatrix}.$$

Тогда согласно формулы (6), для шести критериев имеем: i,j=$\overline{1,6}$, n=6; функция принадлежности будет иметь следующие значения:

$$\mu_{\underset{\sim}{Y}}(y_1)=3/(3+5+1+1+1/3+1/3)=0{,}281;$$
$$\mu_{\underset{\sim}{Y}}(y_2)=5/(3+5+1+1+1/3+1/3)=0{,}469;$$
$$\mu_{\underset{\sim}{Y}}(y_3)=1/(3+5+1+1+1/3+1/3)=0{,}094;$$
$$\mu_{\underset{\sim}{Y}}(y_4)=1/(3+5+1+1+1/3+1/3)=0{,}094;$$
$$\mu_{\underset{\sim}{Y}}(y_5)=(1/3)/(3+5+1+1+1/3+1/3)=0{,}031;$$
$$\mu_{\underset{\sim}{Y}}(y_6)=(1/3)/(3+5+1+1+1/3+1/3)=0{,}031.$$

После нормирования согласно формулы (7) получим функцию принадлежности:

$$\mu_{\underset{\sim}{Y}}(y_1)=0{,}599;$$
$$\mu_{\underset{\sim}{Y}}(y_2)=1;$$
$$\mu_{\underset{\sim}{Y}}(y_3)=0{,}2;$$
$$\mu_{\underset{\sim}{Y}}(y_4)=0{,}2;$$
$$\mu_{\underset{\sim}{Y}}(y_5)=0{,}066;$$
$$\mu_{\underset{\sim}{Y}}(y_6)=0{,}066.$$

Образованная функция принадлежности представлена на рис.1.

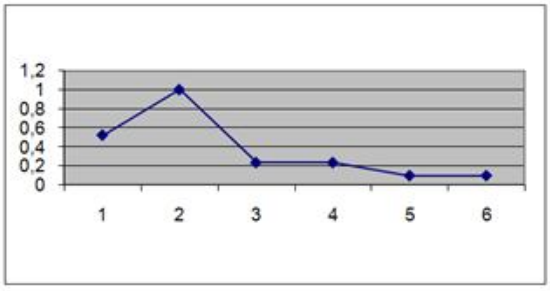

Рис.1. Нечеткое множество “Важность” образованное с помощью метода КПСЧ.

Построение нечеткого множества «Запас криптостойкости» производится с помощью метода КПСК, для альтернатив множества X ={x_1,x_2,x_3}={DES AES, ГОСТ}. Матрица парных сравнений алгоритмов пронумерованных в порядке представления на множестве X имеет вид:

$$Y_1 = \begin{Vmatrix} 1 & 1/3 & 1/5 \\ 3 & 1 & 1/3 \\ 5 & 3 & 1 \end{Vmatrix}.$$

В методе функцию принадлежности определяют через расчет среднего геометрического из соотношения:

$$\mu_{Y1}(x_i)=\omega_i=\sqrt[m]{\prod_{j=1}^{m} y1_{ij}}\ ;\ j=1,m, \qquad (8)$$

где $y1_{ij}$ – коэффициенты матрицы парных сравнений, а исходные данные представляют собой сформированную на основе экспертного опроса матрицу парных сравнений Y_1.

Тогда для трёх альтернатив имеем: n=m=3, а весовые коэффициенты определяются согласно формулы (8) следующим образом:

$$\omega_1 = \sqrt[3]{1\cdot 1/3\cdot 1/5} = 0,4054801;$$
$$\omega_2 = \sqrt[3]{3\cdot 1\cdot 1/3} = 1;$$
$$\omega_3 = \sqrt[3]{5\cdot 3\cdot 1} = 2,466212.$$

После нормирования в соответствии с формулой (7) при n=m=3 получим:

$$\mu_{\underset{\sim}{Y}1}(x_1) = 0,164414138;$$
$$\mu_{\underset{\sim}{Y}1}(x_2) = 0,405480133;$$
$$\mu_{\underset{\sim}{Y}1}(x_3) = 1.$$

Для построения множества «Криптостойкость» используем метод интервальных оценок [1]. В основу расчетов положен интервал длинны ключа (52-512 бит), который может обеспечить противостояние «экстенсивным» методам взлома:

$$\mu_{\underset{\sim}{Y}2}(x_i) = \begin{cases} 0, \text{ если } Y_x \le Y_{min}, \\ (Y\text{-}Y_{min})/(Y_{max} - Y_{min}), \text{ если } Y_{min} < Y_x < Y_{max}, \\ 1, Y_x \ge Y_{max}. \end{cases}$$

Для Y_{min}=52, Y_{max}=512, $i=\overline{1,3}$ имеем:

$$\mu_{\underset{\sim}{Y}2}(x_1)= 0,026;\ \mu_{\underset{\sim}{Y}2}(x_2)= 0,44;\ \mu_{\underset{\sim}{Y}2}(x_3)= 0,44.$$

После нормирования согласно (7) при n=3 получим:

$$\mu_{\underset{\sim}{Y}2}(x_1)= 0{,}06;\ \mu_{\underset{\sim}{Y}2}(x_2)= 1;\ \mu_{\underset{\sim}{Y}2}(x_3)= 1.$$

Для построения функции принадлежности нечеткому множеству «Временной ресурс» на основе сформированной матрицы парных сравнений используем метод количественного парного сравнения с нахождением частного (КПСЧ) [1].

В основу расчетов положены временные характеристики исследуемых алгоритмов, приведенные в табл.2.

Таблица 2

Временные характеристики алгоритмов

Алгоритм	Платформа	Скорость Мб/с	Оценка
DES	32 Bit	2,075	1
AES	32 Bit	9,36	4,51
ГОСТ	32 Bit	8,3	4

Матрица парных сравнений:

$$Y_3 = \begin{Vmatrix} 1 & 1/4{,}5 & 1/4 \\ 4{,}5 & 1 & 4{,}5/4 \\ 4 & 4/4 & 1 \end{Vmatrix}.$$

Тогда, согласно формулы (6), при n=3, функция принадлежности будет иметь следующие значения:

$\mu_{\underset{\sim}{Y}3}\ (x_1)= 1/(1+4{,}5+4)=0{,}105;\ \mu_{Y3}(x_2)= 4{,}5/(1+4{,}5+4)=0{,}475;\ \mu_{Y3}(x_3)= 4{,}5/(1+4{,}5+4)= 0{,}421.$

После нормирования согласно (7), для n=3, получим:

$$\mu_{\underset{\sim}{Y}3}\ (x_1)= 0{,}221;\ \mu_{\underset{\sim}{Y}3}(x_2)= 1;\ \mu_{\underset{\sim}{Y}3}(x_3)= 0{,}886.$$

Аналогичным способом определим функцию принадлежности нечеткому множеству «Пространственный ресурс» воспользовавшись данными из табл.3.

Таблица 3

Пространственные характеристики алгоритмов

Алгоритм	Платформа	Память Кб	Оценка
DES	32 Bit	1	1
AES	32 Bit	8,25	8,25
ГОСТ	32 Bit	4	4

Матрица парных сравнений Y_4 приведена ниже:

$$Y_4 = \begin{Vmatrix} 1 & 8{,}25 & 4 \\ 1/8{,}25 & 1 & 4/8{,}25 \\ 1/4 & 8{,}25/4 & 1 \end{Vmatrix}.$$

Тогда, согласно формулы (6), функция принадлежности будет иметь следующие значения при n=3:

$$\mu_{\underset{\sim}{Y}4}(x_1)=1/(1+1/8{,}25+1/4)= 0{,}73;$$

$$\mu_{\underset{\sim}{Y}4}(x_2)= (1/8{,}25)/ (1+1/8{,}25+1/4)=0{,}09;$$

$$\mu_{\underset{\sim}{Y}4}(x_3)= (1/4)/ (1+1/8{,}25+1/4)=0{,}18.$$

После нормирования согласно (7), при n=3, получим:

$$\mu_{\underset{\sim}{Y}4}(x_1)= 1;\ \mu_{\underset{\sim}{Y}4}(x_2)=0{,}12;\ \mu_{\underset{\sim}{Y}4}(x_3)= 0{,}25.$$

Для построения функции принадлежности нечеткому множеству «Сложность алгоритма» будем использовать метод КПСК. Матрица парных сравнений альтернатив пронумерованных в порядке представления на множестве X имеет следующий вид:

$$Y_5 = \begin{Vmatrix} 1 & 1/3 & 1/5 \\ 3 & 1 & 1/3 \\ 5 & 3 & 1 \end{Vmatrix}.$$

Весовые коэффициенты, в соответствии с формулой (6), при n=3, определяются следующим образом:

$$\omega_1 = \sqrt[3]{1 \cdot 1/3 \cdot 1/5} = 0{,}4054801;$$
$$\omega_2 = \sqrt[3]{3 \cdot 1 \cdot 1/3} = 1;$$
$$\omega_3 = \sqrt[3]{5 \cdot 3 \cdot 1} = 2{,}466212.$$

После нормирования получим по (7) при n=3:

$$\mu_{\underset{\sim}{Y}5}(x_1) = 0{,}164414138;$$
$$\mu_{\underset{\sim}{Y}5}(x_2) = 0{,}405480133;$$
$$\mu_{\underset{\sim}{Y}5}(x_3) = 1.$$

Для построения функции принадлежности нечеткому множеству «Сложность реализации» будем использовать метод КПСК. Матрица парных сравнений альтернатив пронумерованных в порядке представления на множестве X имеет следующий вид:

$$Y_6 = \begin{Vmatrix} 1 & 1/3 & 1/5 \\ 3 & 1 & 1/3 \\ 5 & 3 & 1 \end{Vmatrix}.$$

Весовые коэффициенты определяются следующим образом (8) при m=3:

$$\omega_1 = \sqrt[3]{1 \cdot 1/3 \cdot 1/5} = 0{,}4054801;$$
$$\omega_2 = \sqrt[3]{3 \cdot 1 \cdot 1/3} = 1;$$
$$\omega_3 = \sqrt[3]{5 \cdot 3 \cdot 1} = 2{,}466212.$$

После нормирования по (7), при n=m=3, получим:

$$\mu_{\underset{\sim}{Y}6}(x_1)= 0{,}164414138;\ \mu_{\underset{\sim}{Y}6}(x_2)= 0{,}405480133;\ \mu_{\underset{\sim}{Y}6}(x_3)= 1.$$

Таким образом, в результате проведенных расчетов было получено нечеткое множество "Важность" критериев:

$$\mu_{\underset{\sim}{Y}}(y) = \{0{,}599 / y_1;\ 1/y_2;\ 0{,}2/y_3;\ 0{,}2/y_4;\ 0{,}066/y_5;\ 0{,}066/y_6\}.$$

А также оценки альтернатив по заданным критериям, которые представлены следующими нечеткими множествами:

$$\mu_{\underset{\sim}{Y}_1}(x) = \{0{,}16 / x_1;\ 0{,}41 / x_2;\ 1 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_2}(x) = \{0{,}06 / x_1;\ 1 / x_2;\ 1 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_3}(x) = \{0{,}221 / x_1;\ 1 / x_2;\ 0{,}89 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_4}(x) = \{1 / x_1;\ 0{,}12 / x_2;\ 0{,}25 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_5}(x) = \{0{,}16 / x_1;\ 0{,}41 / x_2;\ 1 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_6}(x) = \{0{,}16 / x_1;\ 0{,}41 / x_2;\ 1 / x_3\}.$$

Для того чтобы учесть нечеткое множество важности критериев для каждой из альтернатив находим алгебраическое произведение множества критериев по каждой альтернативе на нечеткое множество важности критериев по формуле (2), тогда с учетом важности критериев функции принадлежности будут иметь следующие значения:

$$\mu_{\underset{\sim}{Y}_1}(x) = \{0{,}09584 / x_1;\ 0{,}24559 / x_2;\ 0{,}599 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_2}(x) = \{0{,}06 / x_1;\ 1 / x_2;\ 1 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_3}(x) = \{0{,}0442 / x_1;\ 0{,}2 / x_2;\ 0{,}178 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_4}(x) = \{0{,}2 / x_1;\ 0{,}024 / x_2;\ 0{,}054 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_5}(x) = \{0{,}1056 / x_1;\ 0{,}02706 / x_2;\ 0{,}066 / x_3\};$$
$$\mu_{\underset{\sim}{Y}_6}(x) = \{0{,}1056 / x_1;\ 0{,}02706 / x_2;\ 0{,}066 / x_3\}.$$

Нечеткое множество $\underset{\sim}{G}$ – функцию одновременно недостижимых целей (ФОНЦ) находим по формуле (4):

$$\mu_{\underset{\sim}{G}_1}(\underset{\sim}{Y}1) = \mathrm{MAX}\{\mu_{\underset{\sim}{Y}_1}(x)\} = \mathrm{MAX}\{0{,}09584 / x_1;\ 0{,}24559 / x_2;\ 0{,}599 / x_3\} = 0{,}599;$$
$$\mu_{\underset{\sim}{G}_2}(\underset{\sim}{Y}2) = \mathrm{MAX}\{(\mu_{\underset{\sim}{Y}_2}(x))\} = \mathrm{MAX}\{0{,}06 / x_1;\ 1 / x_2;\ 1 / x_3\} = 1;$$
$$\mu_{\underset{\sim}{G}_3}(\underset{\sim}{Y}3) = \mathrm{MAX}\{\mu_{\underset{\sim}{Y}_3}(x)\} = \mathrm{MAX}\{0{,}0442 / x_1;\ 0{,}2 / x_2;\ 0{,}178 / x_3\} = 0{,}2;$$
$$\mu_{\underset{\sim}{G}_4}(\underset{\sim}{Y}4) = \mathrm{MAX}\{\mu_{\underset{\sim}{Y}_4}(x)\} = \mathrm{MAX}\{0{,}2 / x_1;\ 0{,}024 / x_2;\ 0{,}054 / x_3\} = 0{,}2;$$
$$\mu_{\underset{\sim}{G}_5}(\underset{\sim}{Y}5) = \mathrm{MAX}\{\mu_{\underset{\sim}{Y}_5}(x)\} = \mathrm{MAX}\{0{,}1056 / x_1;\ 0{,}02706 / x_2;\ 0{,}066 / x_3\} = 0{,}066;$$
$$\mu_{\underset{\sim}{G}_6}(\underset{\sim}{Y}6) = \mathrm{MAX}\{\mu_{\underset{\sim}{Y}_6}(x)\} = \mathrm{MAX}\{0{,}1056 / x_1;\ 0{,}02706 / x_2;\ 0{,}066 / x_3\} = 0{,}066;$$

$$\mu_{\underset{\sim}{G}}(y) = \{0{,}599 / y_1;\ 1 / y_2;\ 0{,}2 / y_3;\ 0{,}2 / y_4;\ 0{,}066 / y_5;\ 0{,}066 / y_6\}.$$

Расчет расстояния Хемминга для нечетких множеств производим по формуле (3), при n=6, получим:

$d(\underset{\sim}{G}, \underset{\sim}{X}1)$ =|0,599-0,09584|+|1-0,06|+|0,2-0,0442|+|0,2-0,2|+|0,066-0,01056|+|0,066-0,01056|=1,7098;

$d(\underset{\sim}{G}, \underset{\sim}{X}2)$=|0,599-0,24559|+|1-1|+|0,2-0,2|+|0,2-0,024|+|0,066-0,02706|+|0,066-0,02706|=0,6072;

$d(\underset{\sim}{G}, \underset{\sim}{X}3)$ =|0,599-0,599|+|1-1|+|0,2-0,178|+|0,2-0,05|+|0,066-0,066|+|0,066-0,066|=0,172.

Тогда лучшая альтернатива определится как:

$\mathrm{MIN}\{\ d(\underset{\sim}{G}, \underset{\sim}{X}1);\ d(\underset{\sim}{G}, \underset{\sim}{X}2);\ d(\underset{\sim}{G}, \underset{\sim}{X}3)\ \}$= MIN {1,7098/x1;0,6072/x2;0,172/x3}=0,172.

В результате можно сделать вывод о том, что альтернатива X3 (алгоритм ГОСТ 28147-89) имеет минимальное расстояние Хемминга (0,172) и является наиболее предпочтительной

относительно заданных параметров. Альтернатива X1 (алгоритм DES) имеет максимальное расстояние т.е. имеет наихудшие характеристики.

Выводы

В итоге, приведенный математический аппарат дает возможность более эффективно осуществить задачу выбора алгоритма для данной криптосистемы, тем самым, оптимизируя работу этой системы, целью которой является шифрация информации. Использование предлагаемого подхода выбора алгоритма дает возможность в дальнейшем автоматизировать процесс принятия решения при построении криптосистем и последующего его применения в системах автоматизации проектирования. Возможность накопления базы знаний нечетких альтернатив и формализация процесса принятия решений позволит расширять спектр применения, включая как появление новых алгоритмов шифрования так и новых методов криптоанализа.

Список литературы

1. *Корченко О.Г.* Системи захисту _віязь_раф. Монографія / Корченко О.Г. – К. : НАУ, 2004. – 264 с.

2. *Шнайер Б.* Прикладная Криптография. 2-е изд. Протоколы, Алгоритмы и исходные тексты на языке Си / Шнайер Б. – М., "Триумф", 2002. – 816 с.

3. *Мао, Венбо*. Современная _віязь_рафія: _віязь и практика. Справочник / Мао, Венбо. – М. : Издательский дом «Вильямс», 2005. – 768 с.

4. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник / Панасенко С.П. – СПб. : БХВ-Петербург, 2009. – 576 с.

5. *Кофман А*. Введение в _віязь нечетких множеств / Кофман А. – М. : Радио и _віязь, 1982. – 432с.

6. Гаенко А.В. Рекомендации и выбор вида шифра для применения в сети доступа / Гаенко А.В., Шестак Н.А. // Вісник Українського будинку економічних та науково-технічних знань. – 2005. – №3. – 50-54 с.

Поступила 24.02.2010

УДК 003.26:621.39+530.145 **Василиу Е.В.**

АНАЛИЗ СТОЙКОСТИ К НЕКОГЕРЕНТНОЙ АТАКЕ ЧЕТЫРЕХ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С КУТРИТАМИ

Современное информационное общество постоянно испытывает необходимость в усовершенствовании методов защиты телекоммуникационных каналов от несанкционированного прослушивания. Предложенная в 80-х годах XX века идея применения принципов квантовой механики к криптографии привела к развитию нового мультидисциплинарного научного направления – квантовой криптографии [1–3]. Одно из направлений квантовой криптографии – квантовые протоколы распределение ключей (КПРК), где две удаленные стороны (Алиса и Боб) с использованием квантового коммуникационного канала могут сгенерировать общую случайную бинарную строку, которую затем используют как ключ для шифрования. При этом законы квантовой механики гарантируют безопасность передачи ключа – при выполнении легитимными сторонами определенных процедур, касающихся как передачи квантовых частиц (фотонов) по каналу связи, так и определенной классической или квантовой пред- и постобработки информации [1–3].

К настоящему времени предложены различные классы КПРК [2,3]. Два основных класса – это протоколы, основанные на передаче одиночных квантовых состояний, относящихся к неортогональным базисам (их называют также протоколами типа «приготовление – измерение») и протоколы, основанные на распределении перепутанных квантовых состояний между пользователями. При этом можно использовать двух-, трех- и т.д. мерные квантовые системы, соответственно каждая такая система позволяет передать один бит, один трит и т.д. информации.