Литература: 1. Norton AntiVirus Corporate Edition. Руководство по применению. 2. Kaspersky AntiVirus – руководство пользователя.

УДК 681.3.06

ОПРЕДЕЛЕНИЕ МНОЖЕСТВА МЕХАНИЗМОВ ЗАЩИТЫ, ОБЕСПЕЧИВАЮЩИХ ОПТИМАЛЬНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Алексей Новиков, Андрей Тимошенко*
Физико-технический институт НТУУ «КПИ»
**ООО «Институт компьютерных технологий»*

Аннотация: **Рассмотрены вопросы разработки аглоритма решения задачи определения множества механизмов защиты информации, обеспечивающих оптимальный уровень защищенности информации, обрабатываемой в компьютерной системе с открытой архитектурой.**
Summary: **The problems of development of the algorithm for determination a security mechanisms set that ensures an optimum level of an information security in the computer system with open architecture are considered.**
Ключевые слова: **Механизм защиты, стек протоколов, угроза информации.**

I Постановка задачи

Построение системы защиты информации (СЗИ), обрабатываемой в компьютерной системе (КС), предполагает, согласно [1], проведение анализа потенциальных угроз информации, оценки рисков, связанных с их реализацией (как функции вероятности реализации данных угроз и величины возможного ущерба). С учетом результатов проведенного анализа, должен быть проведен выбор для включения в СЗИ таких механизмов защиты, использование которых обеспечит максимальную защищенность обрабатываемой информации. При этом стоимость реализации средств защиты должна быть адекватна величине возможного ущерба. В [2] в качестве характеристики защищенности обрабатываемой в КС информации предложено использовать вероятность сохранения защищенности как функцию множества реализованных в СЗИ КС механизмов защиты $P(M)$. Там же получено следующее ее выражение для КС с открытой архитектурой и многоуровневым стеком протоколов [3]:

$$P(M)=\prod_{i=1}^{L}\left(\prod_{j=1}^{N}(1-E_{ij})+\sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1-E_{ik})\cdot\left(\sum_{k=1}^{j}M_{ik}\cdot\prod_{l=k+1}^{j}(1-M_{il})\right)\right]\right) \qquad (1)$$

где L – количество потенциальных угроз информации, обрабатываемой в КС; N – количество уровней стека протоколов КС; M_{ij} – целочисленная переменная, значение которой определяет факт наличия/отсутствия механизма защиты от i-й угрозы на протоколе j-го уровня, $M_{ij}\in\{0,1\}$; E_{ij} – показатель эффективности реализации i-й угрозы на протоколе j-го уровня, характеризующий степень риска, связанного с реализацией данной угрозы, как функцию вероятности реализации угрозы и величины возможных потерь, $E_{ij}\in[0,1]$.

Адекватность стоимости реализации средств защиты величине потенциального ущерба предполагает наличие ограничения на максимальное значение затрат на реализацию СЗИ (стоимость реализуемых в СЗИ механизмов защиты). С учетом (1), данное ограничение для КС с открытой архитектурой можно сформулировать следующим образом:

$$C(M)=\sum_{i=1}^{L}\left(\sum_{j=1}^{N}M_{ij}\cdot C_{ij}\right)\le C_o \qquad (2)$$

где $C(M)$ – стоимость реализации множества механизмов защиты $M=\{M_{ij}\}$, $i\in\{1,...,L\}$, $j\in\{1,...,N\}$; C_{ij} – стоимость реализации механизма защиты от i-й угрозы на протоколе j-го уровня; C_o – максимальное значение затрат на реализацию СЗИ.

С учетом вышесказанного, задачу математического программирования, которую необходимо решить для определения множества механизмов защиты, обеспечивающего оптимальный уровень защищенности информации, обрабатываемой в КС с открытой архитектурой, можно сформулировать следующим образом:

$$P(M) \to max \tag{3}$$

$$C(M) \le C_o \tag{4}$$

В данной статье приводятся результаты разработки алгоритма решения задачи (3), (4), учитывающего особенности использования (1) в качестве целевой функции (ЦФ), а также целочисленность компонентов вектора изменяемых параметров M_{ij} и показанное в [4] ранжирование значимостей механизмов защиты, реализованных на различных уровнях стека протоколов КС.

II Исследование целевой функции

Так как представленная в виде (1) ЦФ не является линейной относительно M_{ij}, задача поиска максимума данной функции представляет собой задачу нелинейного программирования (НЛП). При выборе метода решения задачи НЛП [5] исходят из вида ЦФ, дифференцируемости ЦФ (возможности аналитического определения частных производных ЦФ первого и более высоких порядков) и вида ограничений. Для случаев, когда вычисление частных производных ЦФ высоких порядков невозможно или затруднено, наиболее широко применяются градиентные методы. Однако, их успешное применение возможно только в случае отсутствия у ЦФ локальных экстремумов, расположенных в области допустимых решений. Для выяснения возможности использования при решении поставленной задачи градиентного метода исследуем поведение ЦФ (1) в области допустимых решений.

Функция (1) является дифференцируемой по компонентам вектора изменяемых параметров (переменным M_{ij}). Выражение для определения соответствующих частных производных имеет вид:

$$\frac{\partial P(M)}{\partial M_{ij}} = \frac{\partial P_i(M_i)}{\partial M_{ij}} \prod_{k=1}^{i-1} P_k(M_k) \prod_{k=i+1}^{N} P_k(M_k), \tag{5}$$

где

$$M_i = \{M_{ij}\}, \quad j \in \{1,...,N\},$$

$$M_k = \{M_{kj}\}, \quad k \ne i, \quad j \in \{1,...,N\},$$

$$\frac{\partial P_i(M_i)}{\partial M_{ij}} = \sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1-E_{il}) \cdot \prod_{l=1}^{j-1}(1-M_{il}) \cdot \prod_{l=j+1}^{k}(1-M_{il}) \tag{6}$$

$$P_k(M) = \prod_{l=1}^{N}(1-E_{kl}) + \sum_{l=1}^{N}\left[E_{kl} \prod_{m=1}^{l-1}(1-E_{km}) \cdot \left(\sum_{m=1}^{l} M_{km} \cdot \prod_{n=m+1}^{l}(1-M_{kn}) \right) \right] \tag{7}$$

Как известно, наличие локальных экстремумов функции определяется изменением знака частных производных. Проанализируем характер и знак частных производных ЦФ (1), заданных в виде (5), в интервале $M_{ij} \in [0,1]$, учитывая, что $E_{ij} \in [0,1]$. Поскольку (7) представляет собой выражение для оценки вероятности сохранения защищенности информации от одной, k-й угрозы, то есть, $0 \le P_k(M_k) \le 1$, и при этом, как видно из (7), $P_k(M_k)$ не зависит от M_{ij}, справедливо будет утверждать, что знак частной производной $\frac{\partial P(M)}{\partial M_{ij}}$ определяется знаком частной производной $\frac{\partial P_i(M_i)}{\partial M_{ij}}$. Учитывая, что в (6) $M_{il} \in \{0,1\}$, а $0 \le E_{ik} \le 1$ и $0 \le E_{il} \le 1$, можно утверждать, что $\frac{\partial P_i(M)}{\partial M_{ij}} \ge 0$, а, значит, в интервале $M_{ij} \in [0,1]$ при $E_{ij} \in [0,1]$ всегда выполняется условие $\frac{\partial P(M)}{\partial M_{ij}} \ge 0$. Из этого следует, что в области допустимых значений M_{ij} ЦФ, заданная в виде (1) не имеет локальных экстремумов, а, следовательно, применение градиентного метода для ее максимизации будет успешным.

III Разработка алгоритма

Известно [6], что разные варианты градиентного метода различаются способом выбора шага на каждой итерации, теми или иными способами вычисления градиентов (аппроксимация, приближенные вычисления и т. п.). Поскольку целью максимизации ЦФ (1) является поиск оптимального решения с учетом ограничений на максимальное значение затрат на реализацию СЗИ (2), предлагается при решении сформулированной задачи математического программирования в качестве направления движения из текущей допустимой точки использовать направление, соответствующее наибольшей удельной значимости по критерию затрат (определенной, как отношение прироста показателя вероятности сохранения защищенности информации к приросту стоимости). Это направление соответствует [7, 8] максимальному значению частной производной $\frac{\partial P\ (M_{ij})}{\partial C(M_{ij})}$, которое можно аппроксимировать отношением $\frac{\Delta P\ (M_{ij})}{\Delta C(M_{ij})}$, где $\Delta P\ (M_{ij})$ - приращение $P\ (M)$ при увеличении значения M_{ij} на величину шага, а $\Delta C(M_{ij})$ – приращение $C(M)$ при увеличении значения M_{ij} на величину шага. Поскольку M_{ij} может принимать только значения 0 или 1, величину шага предлагается выбрать равной 1.

На начальном шаге процесса вычислений допустимое решение имеет компоненты $M_{ij} = 0$, $i \in I = \{1,..., L\}$, $j \in J = \{1,..., N\}$, т. е. отсутствуют механизмы защиты от всех угроз на всех уровнях стека протоколов. На первом шаге среди всех угроз информации $i \in I$ и для всех уровней стека протоколов $j \in J_i^{(0)}$, $J_i^{(0)} = J_{M_i}$, где J_{M_i} – множество номеров уровней стека протоколов, на которых применим выбранный механизм защиты от i-угрозы (определяется характеристиками конкретного механизма [9–15]), отыскивается угроза информации $n \in I$ и уровень стека протоколов $m \in J_n^{(0)}$, такие, что реализация механизма защиты от данной угрозы на данном уровне стека протоколов (т. е., присвоение $M_{nm}^{(1)} = M_{nm}^{(0)} + 1$) приводит к наибольшему относительному приросту показателя вероятности сохранения защищенности информации, т. е. наибольшему приросту на единицу стоимости. С учетом того, что в КС с открытой архитектурой [4] имеется ранжирование значимостей механизмов защиты, реализованных на различных уровнях стека протоколов, а это означает, что механизм, реализованный на уровне m, обеспечивает защиту от угроз на уровнях стека протоколов, больших m, компоненты M_{ij} для $i = n, j \in \{m+1,..., \sup J_n^{(0)}\}$ принимаются равными 0 и исключаются из дальнейшего рассмотрения, т. е. $J_i^{(1)} = J_i^{(0)}, i \in I, i \neq n$, $J_n^{(1)} = J_n^{(0)} \setminus \{m,..., \sup J_n^{(0)}\}$.

На втором шаге отыскивается следующая угроза и для нее уровень стека протоколов, реализация механизма защиты которой на данном уровне стека протоколов приводит к наибольшему приросту показателя вероятности сохранения защищенности информации по отношению к стоимости. Этой новой угрозой может быть та же угроза, что и на первом шаге.

Пусть на s-м шаге процесса вычислений достигнуто допустимое решение $M^{(s)}$. Вероятность сохранения защищенности информации определяется как $P(M^{(s)}) = \prod_{i=1}^{L} P_i(M^{(s)})$,

а стоимость реализации выбранных механизмов защиты – $C(M^{(s)}) = \sum_{i=1}^{L}\left(\sum_{j=1}^{N} M_{ij}^{(s)} \cdot C_{ij}\right)$.

На $s+1$ шаге для выбора направления, в котором функция вероятности возрастает максимально, определяем $\gamma^{(s+1)} = \max_{i \in I, j \in J_i^{(s)}} \tilde{\gamma}_{ji}^{(s)}(M^{(s)})$, где

$$\tilde{\gamma}_{ji}^{(s)}(M^{(s)}) = \frac{P(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1) - P(M^{(s)})}{C(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1) - C(M^{(s)})}$$

$$P(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1) = \frac{P(M^{(s)}) P_i(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1)}{P_i(M^{(s)})}.$$

В данном выражении

$$C(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1) = C_{ij} + \sum_{i=1}^{L}\left(\sum_{j=1}^{N} M_{ij}^{(s)} \cdot C_{ij}\right) = C_{ij} + C(M^{(s)})$$

Тогда

$$\tilde{\gamma}_{ji}^{(s)}(M_{ij}^{(s)}) = P(M^{(s)})\frac{P_i(M^{(s)} \setminus M_{ij}^{(s)}, M_{ij}^{(s)} + 1) - P_i(M^{(s)})}{C_{ij} \cdot P_i(M^{(s)})} =$$

$$= P(M^{(s)})\frac{\sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1 - E_{il}) \cdot \prod_{m=1}^{j-1}(1 - M_{im}^{(s)}) \cdot \prod_{n=j+1}^{k}(1 - M_{in}^{(s)})}{C_{ij} \cdot \left(\prod_{j=1}^{N}(1 - E_{ij}) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1 - E_{ik}) \cdot \left(\sum_{k=1}^{j} M_{ik}^{(s)} \cdot \prod_{l=k+1}^{j}(1 - M_{il}^{(s)})\right)\right]\right)}$$

Таким образом

$$\gamma^{(s+1)} = \max_{i \in I, j \in J_i^{(s)}} \tilde{\gamma}_{ji}^{(s)}(M_{ij}^{(s)}) = \max_{i \in I, j \in J_i^{(s)}} P(M^{(s)})\frac{\sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1 - E_{il}) \cdot \prod_{m=1}^{j-1}(1 - M_{im}^{(s)}) \cdot \prod_{n=j+1}^{k}(1 - M_{in}^{(s)})}{C_{ij} \cdot \left(\prod_{j=1}^{N}(1 - E_{ij}) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1 - E_{ik}) \cdot \left(\sum_{k=1}^{j} M_{ik}^{(s)} \cdot \prod_{l=k+1}^{j}(1 - M_{il}^{(s)})\right)\right]\right)} =$$

$$= P(M^{(s)}) \max_{i \in I, j \in J_i^{(s)}} \frac{\sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1 - E_{il}) \cdot \prod_{m=1}^{j-1}(1 - M_{im}^{(s)}) \cdot \prod_{n=j+1}^{k}(1 - M_{in}^{(s)})}{C_{ij} \cdot \left(\prod_{j=1}^{N}(1 - E_{ij}) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1 - E_{ik}) \cdot \left(\sum_{k=1}^{j} M_{ik}^{(s)} \cdot \prod_{l=k+1}^{j}(1 - M_{il}^{(s)})\right)\right]\right)} = P(M^{(s)}) \max_{i \in I, j \in J_i^{(s)}} \gamma_{ji}^{(s)}$$

где

$$\gamma_{ji}^{(s)} = \frac{\sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1 - E_{il}) \cdot \prod_{m=1}^{j-1}(1 - M_{im}^{(s)}) \cdot \prod_{n=j+1}^{k}(1 - M_{in}^{(s)})}{C_{ij} \cdot \left(\prod_{j=1}^{N}(1 - E_{ij}) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1 - E_{ik}) \cdot \left(\sum_{k=1}^{j} M_{ik}^{(s)} \cdot \prod_{l=k+1}^{j}(1 - M_{il}^{(s)})\right)\right]\right)}.$$

Поскольку $P(M^{(s)})$ входит сомножителем во все величины $\tilde{\gamma}_{ji}^{(s)}(M_{ij}^{(s)})$ и не влияет на выбор направления движения, то можно упростить вычисления. Для этого на шаге $s+1$ необходимо двигаться в направлении $\gamma^{(s+1)} = \max_{i \in I, j \in J_i^{(s)}} \gamma_{ji}^{(s)}(M_{ij}^{(s)})$. Это позволит существенно уменьшить объем вычислений, необходимый для определения очередного направления движения.

Поиск оптимального решения должен завершаться либо при невозможности выполнения на $s+1$ шаге ограничения $C(M^{(s+1)}) \le C_o$, либо в случае, когда из рассмотрения исключены все M_{ij}, $i \in I$, $j \in I$, т. е. $J_i^{(s)} = \varnothing$, $i \in I$.

Таким образом, предлагаемый алгоритм решения поставленной задачи состоит в следующем.

Шаг 0. Полагаем $s = 0$, $I = \{1,...,L\}$, $J = \{1,...,N\}$, $M_{ij} = 0$, $i \in I$, $j \in I$. На основании характеристик выбранных механизмов определяем множество номеров уровней стека протоколов, на которых они применимы J_{M_i}, $i \in I$, задаем $J_i^{(s)} = J_{M_i}$, $i \in I$, и переходим к шагу 1.

Шаг 1. Если

$J_i^{(s)} = \varnothing$, $i \in I$, то заканчиваем вычисления, $M^{(s)}$ – оптимальное решение.

Шаг 2. Вычисляем

$$\gamma_{ji}^{(s)} = \frac{\sum_{k=j}^{N} E_{ik} \cdot \prod_{l=1}^{k-1}(1-E_{il}) \cdot \prod_{m=1}^{j-1}(1-M_{im}^{(s)}) \cdot \prod_{n=j+1}^{k}(1-M_{in}^{(s)})}{C_{ij} \cdot \left(\prod_{j=1}^{N}(1-E_{ij}) + \sum_{j=1}^{N}\left[E_{ij} \prod_{k=1}^{j-1}(1-E_{ik}) \cdot \left(\sum_{k=1}^{j} M_{ik}^{(s)} \cdot \prod_{l=k+1}^{j}(1-M_{il}^{(s)}) \right) \right] \right)}, i \in I, j \in J^{(s)}$$

и определяем

$$\gamma^{(s+1)} = \gamma_{mn}^{(s)}(M_{mn}^{(s)}) = \max_{i \in I, j \in J_i^{(s)}} \gamma_{ji}^{(s)}(M_{ij}^{(s)}).$$

Шаг 3. Полагаем

$$M_{nm}^{(s+1)} = M_{nm}^{(s)} + 1$$
$$M_{ij}^{(s+1)} = M_{ij}^{(s)}, i \in I, i \neq n, j \in J$$
$$M_{nj}^{(s+1)} = M_{nj}^{(s)}, j \in \{1,...,m-1\}$$
$$M_{nj}^{(s+1)} = 0, j \in \{m+1,...,sup\, J_n^{(s)}\}$$
$$J_i^{(s+1)} = J_i^{(s)}, i \in I, i \neq n,$$
$$J_n^{(s+1)} = J_n^{(s)} \setminus \{m,...,sup\, J_n^{(s)}\}$$

и переходим к шагу 4.

Шаг 4. Если

$C(M^{(s)}) \leq C_o \leq C(M^{(s+1)})$, то заканчиваем вычисления, $M^{(s)}$ – оптимальное решение. В противном шаге полагаем $s = s+1$ и переходим к шагу 1.

Полученное в результате выполнения данной процедуры значение $M^{(s)}$ определяет множество механизмов защиты, которое необходимо реализовать в СЗИ КС для обеспечения максимальной вероятности сохранения защищенности информации от множества выявленных угроз с показателями эффективности $E = \{E_{ij}\}, i \in I, j \in J$ при выполнении заданных в виде (2) ограничений на общую стоимость средств защиты.

В разработанном алгоритме, за счет учета вида ЦФ (1) и ограничений (2) удалось существенно уменьшить объем вычислений, необходимых для определения значений γ_{ij}. Кроме этого, за счет учета на шаге 3 алгоритма ранжирования значимостей механизмов защиты информации, реализованных на различных уровнях стека протоколов КС, удалось избежать дублирования механизмами защиты, реализованными на более высоких уровнях стека протоколов, механизмов, реализованных на более низких уровнях (с исключением соответствующих затрат на реализацию механизмов защиты).

IV Результаты численного исследования разработанного алгоритма

Для проверки сходимости предложенного алгоритма была разработана его программная реализация и проведено численное исследование на различных тестовых примерах. Исходные данные тестовых примеров (таблица 1) выбирались таким образом, чтобы можно было убедиться в сходимости алгоритма при различных закономерностях изменения эффективностей реализации угроз информации E_{ij}, при различных закономерностях распределения угроз информации и применимости механизмов защиты по уровням стека протоколов, а также при различных закономерностях изменения стоимостей реализации механизмов защиты информации C_{ij}. Результаты численного исследования предложенного алгоритма для исходных данных примеров 1–4 приведены на рис. 1 – 3.

Как видно на рис. 1 на каждом очередном шаге алгоритма независимо от варианта исходных данных достигается большее значение функции вероятности сохранения защищенности информации $P(M)$, причем достигается это за счет использования новых механизмов защиты. Одновременно растет суммарная стоимость $C(M)$, что видно из рис. 2. Однако, при этом аппроксимированное значение градиента $\Delta P(M) / \Delta C(M)$ уменьшается, стремясь к нулю, что подтверждает факт приближения к экстремуму (максимуму) $P(M)$.

Таблица 1 – Исходные данные для численного исследования разработанного алгоритма

№ примера	Распределение угроз информации по уровням стека протоколов	Показатели эффективности реализации угроз информации	Применимость механизмов защиты на различных уровнях стека протоколов	Стоимость реализации механизмов защиты	Предельная стоимость реализации СЗИ
1	Случайным образом, каждая угроза может быть реализована на одном уровне стека протоколов	Одинаковы и не зависят от уровня стека протоколов	Применимы только на тех уровнях стека протоколов, на которых реализуются угрозы	Обратно пропорциональ на уровню стека протоколов	50% от общей стоимости потенциально применимых механизмов защиты
2	Случайным образом, каждая угроза может быть реализована на одном уровне стека протоколов	Пропорциональ ны квадрату номера уровня стека протоколов	Применимы только на тех уровнях стека протоколов, на которых реализуются угрозы	Обратно пропорциональ на уровню стека протоколов	50% от общей стоимости потенциально применимых механизмов защиты
3	Случайным образом, каждая угроза может быть реализована на одном уровне стека протоколов	Пропорциональ ны квадрату номера уровня стека протоколов	Применимы на всех уровнях стека протоколов	Обратно пропорциональ на уровню стека протоколов	10% от общей стоимости потенциально применимых механизмов защиты
4	Случайным образом, каждая угроза может быть реализована на трех уровнях стека протоколов	Пропорциональ ны квадрату номера уровня стека протоколов	Применимы только на тех уровнях стека протоколов, на которых реализуются угрозы	Обратно пропорциональ на уровню стека протоколов	30% от общей стоимости потенциально применимых механизмов защиты

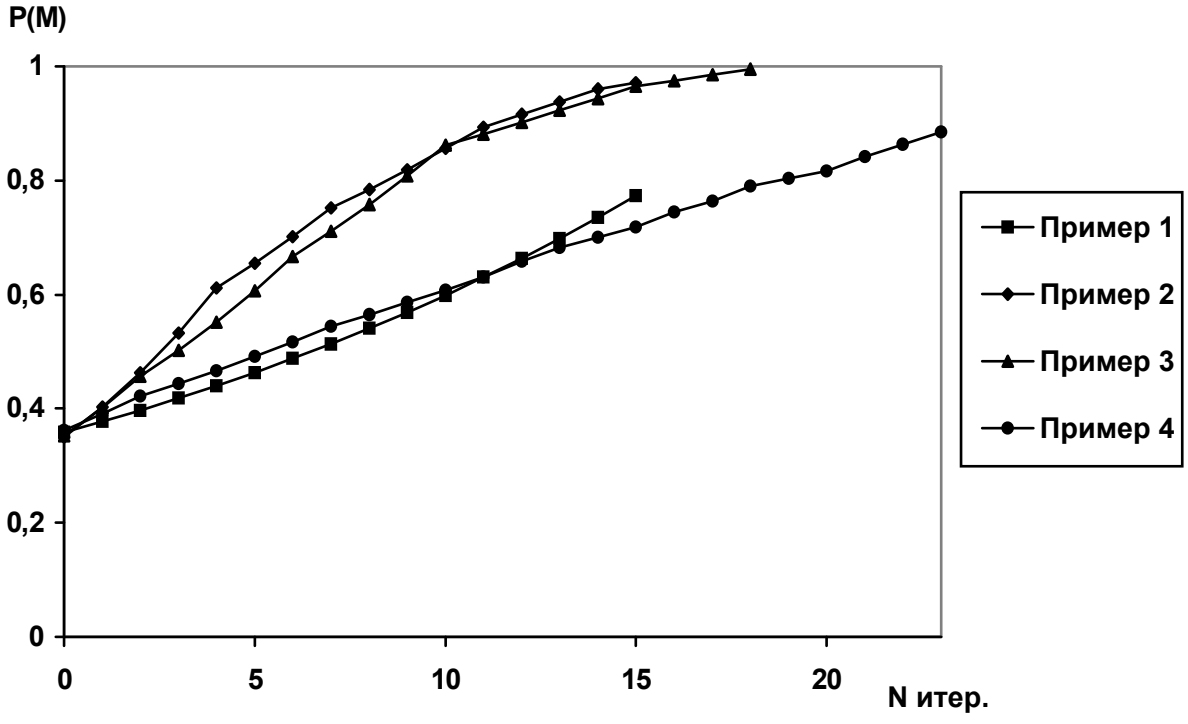

Рисунок 1 – Изменение значения *P(M)* **в ходе градиентной процедуры**

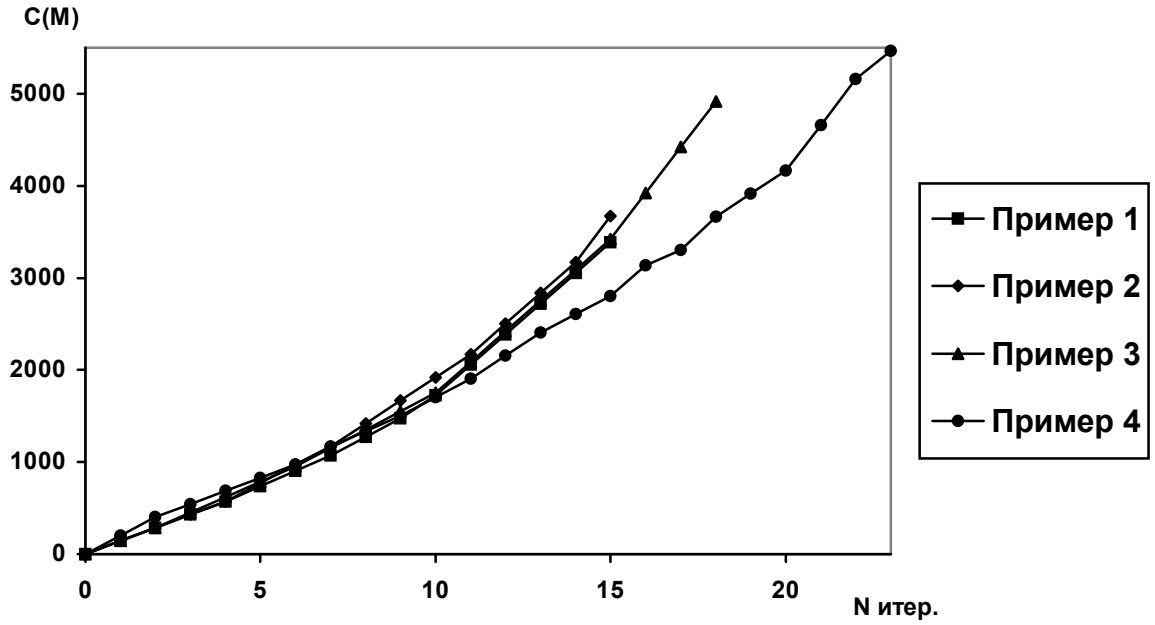

Рисунок 2 – Изменение значения $C(M)$ в ходе градиентной процедуры

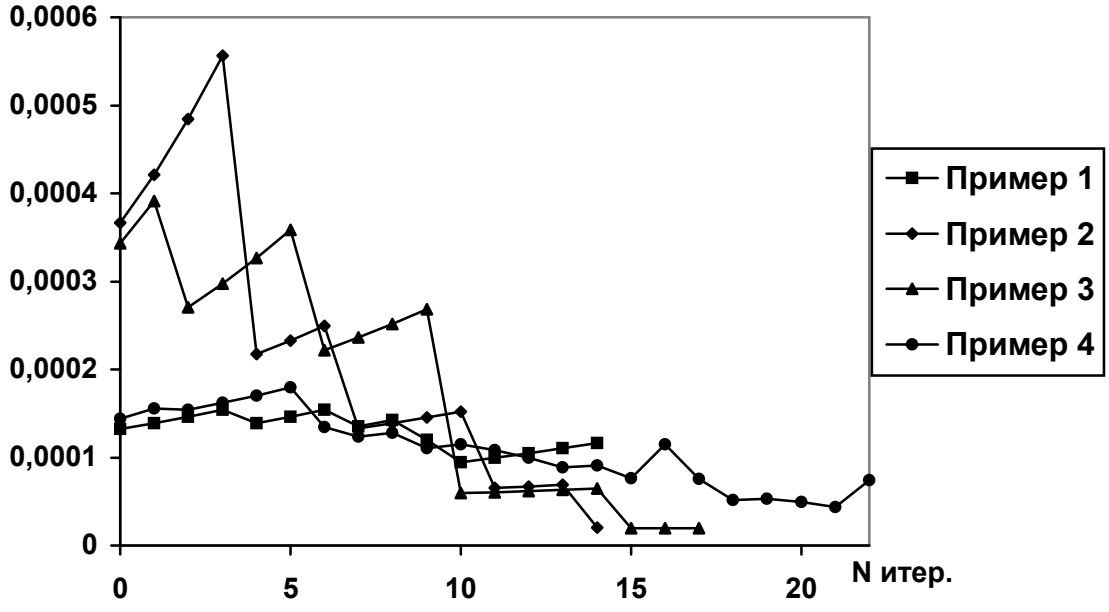

Рисунок 3 – Изменение значения $\Delta P(M)/\Delta C(M)$ в ходе градиентной процедуры

Выводы

На основании приведенных результатов можно утверждать, что разработанный алгоритм определения множества механизмов защиты, обеспечивающих оптимальный уровень защищенности информации, обрабатываемой в КС с открытой архитектурой, от множества угроз информации, заданных

эффективностями их реализации, с учетом ограничений на суммарную стоимость реализации механизмов защиты, обладает устойчивой сходимостью и может быть применен для решения поставленной задачи.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. Новиков А., Тимошенко А. Построение логико-вероятностной модели защищенной компьютерной системы. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.– 2001.– Вип. 3. – с. 101–105. 3. ISO/IEC 7498-1: 1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. 4. О. М. Новіков, А. О. Тимошенко. Логіко-функціональні моделі безпеки інформації в інформаційно-обчислювальних системах з відкритою архітектурою. – Наукові вісті Національного технічного університета України "Київський політехнічний інститут".– 2002.– № 2. 5. Реклейтис Г., Рейвиндран А., Рэгсдел К. Оптимизация в технике: Кн.1. Пер. с англ. – М.: Мир, 1986. 6. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. – М.: Наука. Главная редакция физико-математической литературы, 1984. 7. М. С. Финкельштейн. Надежность и живучесть радиоэлектронных устройств. – М.: Отраслевая система НТИ, 1990. 8. Волкович В. Л., Волошин А. Ф., Заславский В. А., Ушаков И. А. Модели и методы оптимизации надежности сложных систем. – Киев: Наукова думка, 1993. 9. ISO/IEC 7498-2:1989, Information processing systems – Open Systems Interconnection - Basic Reference Model – Part 2: Security Architecture. 10. ISO/IEC 10181-1: 1996, Information technology – Security frameworks for open systems: Overview. 11. ISO/IEC 10181-2: 1996, Information technology – Security frameworks for open systems: Authentication framework. 12. ISO/IEC 10181-3: 1996, Information technology – Security frameworks for open systems: Access control framework. 13. ISO/IEC 10181-4: 1996, Information technology – Security frameworks for open systems: Non repudation framework. 14. ISO/IEC 10181-5: 1996, Information technology – Security frameworks for open systems: Confidentiality framework. 15. ISO/IEC 10181-6: 1996, Information technology – Security frameworks for open systems: Integrity framework.

УДК 681.3.067:681.3.016

ЗОЛОТОЕ СЕЧЕНИЕ В ШИФРОВАНИИ ДАННЫХ

Виктор Мясоедов
Научно-технический комплекс "Импульс", г. Киев

Аннотация: **Безопасность информационных технологий начинается с защиты данных в коммуникациях независимо от открытости используемого канала. Безопасность данных в открытых каналов предполагает абсолютную стойкость шифрующего алгоритма. Здесь описан простой и эффективный алгоритм, удовлетворяющий всем необходимым требованиям, обеспечивающий практически неограниченную длину шифрующей последовательности.**
Summary: **Information technologies security begins with data proof in communications regardless open or close channel of communication used. Data security in open channels requires that coding algorithm should be absolutely non-vulnerable. Here is described the simplest and the most effective algorithm with required property, which provides all necessary demands to coding algorithms, and unbounded code key length as well.**
Ключевые слова: **Принцип Кирхгофа, периодичность, невырожденность, нефальсифицируемость, непрогнозируемость, тотальность, золотое сечение, числа Фибоначчи, административный стандарт, интегрированные интеллектуальные системы.**

I Введение

В обзоре алгоритмов шифрования для передачи данных в открытых сетях [1] перечислены формальные и существенные положения шифрования, пригодные для написания "know how". Вместе с тем, в число положений включено требование, не оправданное ни теоретически, ни практически. Речь идёт о реализуемости "know how" [2], выходящего за пределы условия разрешимости уравнения шифрования относительно ключа при известных открытых и зашифрованных данных.

Предметом рассмотрения является генератор Фибоначчи псевдослучайных последовательностей {t}: $u_1=v_1$, $u_2=v_2$; $t=u_1+u_2$, $u_2=u_1$, $u_1=t$, где v_1, v_2 – численно независимые начальные значения ключа, например, математические константы π и e. На деле используются двоичные представления этих констант определённой длины и длинное двоичное сложение. Последний бит переполнения при двоичном сложении игнорируется. Выходным значением генератора является старший байт числа t, применяемый для шифрования/дешифрования байта данных командой "исключающее ИЛИ". Реально используемые начальные