ЗАДАЧА О ПОКРЫТИИ И МАТЕМАТИЧЕСКИЕ МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гордеев Э.Н.[1]

Задача о покрытии является существенной частью математических моделей, возникающих в проблемах информационной безопасности. Примеры использования задач дискретной оптимизации в таких математических моделях можно найти в [1]. В статье приведено два таких примера. В силу NP–трудности задачи интерес представляют оценки мощности минимального покрытия. Более адекватное использование задачи в математических моделях осуществляется путем обобщения за счет введения «веса» покрытия. В работе рассматривается известное обобщение задачи о покрытии – задача об α–глубине матриц. В реальных моделях есть определенные закономерности в расположении элементов матрицы, связанные со свойствами «покрывающих» и «покрываемых» объектов. Приведены примеры таких закономерностей, получена верхняя оценка мощности покрытия в общем случае, а также рассмотрены два класса матриц, для которых, для которых можно уточнить и упростить эту оценку. Результаты работы достаточно естественно применяются в задачах большой размерности. Однако, на сегодня точные алгоритмы позволяют решать задачу на матрицах, размер которых не превышает 40–50. Поэтому полученные в работе оценки являются полезным инструментом для проверки качества эвристических алгоритмов.

Ключевые слова*: система защиты информации, качество эвристики, α–глубина матриц, оценка мощности минимального покрытия.*

Введение

Пусть A прямоугольная матрица размеров mxn. Элементы матрицы принимают значения из множества целых чисел: 0,1,…,q-1.

Определение. α-глубиной матрицы A называется минимальное число строк этой матрицы такое, что в образованной этими строками подматрице сумма элементов каждого столбца не менее, чем α.

Обозначим эту величину через $\zeta_\alpha^q(A)$. Если A-(0,1)-матрица, то ее α-глубина обозначается через $\zeta_\alpha(A)$. В этом случае вместо *задачи об 1-глубине* употребляется термин *задача о покрытии*.

Задача является известной NP-трудной проблемой, поэтому для ее решения используются либо эвристические алгоритмы, либо методы направленного перебора. Та же сложность задачи остается, если вместо требования точности ограничиваться ε-приближенными алгоритмами. Однако в общем случае даже методы направленного перебора не позволяют решать задачи, в которых размеры матриц больше 50-60. В разных же прикладных областях при математическом моделировании проблем эта задача возникает очень часто.

Возможная интерпретация задачи в области информационной безопасности) следующая. Пусть $N = \{1,..., n\}$ – множество угроз ; $M = \{1,..., m\}$ – множество контрмер. Требуется обеспечить условия покрытия угроз:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{n1}x_m \geq 1 \\ a_{12}x_1 + \ldots + a_{n2}x_m \geq 1 \\ a_{1n}x_1 + \ldots + a_{nm}x_m \geq 1 \end{aligned},$$

где a_{ij} – коэффициенты покрытия, такие что a_{ij}=1, если i - я контрмера покрывает j - ю угрозу, a_{ij}=0, в противном случае, а x – искомый булевский вектор размерности m. На практике более естественно вводить оценки качества покрытия угрозы j контрмерой i. В этом случае матрица перестает быть булевской. Задача об α-глубине возникает, если необходимо варьировать качеством всего покрытия. Тогда требования покрытия следующие:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{n1}x_m \geq \alpha \\ a_{12}x_1 + \ldots + a_{n2}x_m \geq \alpha \\ a_{1n}x_1 + \ldots + a_{nm}x_m \geq \alpha \end{aligned}.$$

Другой пример частого возникновения задачи об α-глубине – моделирование систем физической защиты объектов. Например, размещение видеокамер на большой площади в области с препятствиями (обозреваемыми объектами) так, чтобы со всех сторон видеть все объекты. В частности, здесь большой интерес представляет этап моделирования самой области и препят-

1 Гордеев Эдуард Николаевич, доктор физико-математических наук, профессор, профессор кафедры ИУ8 МГТУ им. Н.Э. Баумана, Москва, tatmigor@gmail.com

ствий, сводящийся, как правило, к оптимизационной задаче вычислительной геометрии. (См., например, [2]).

В этом случае возникает аналогия: обозреваемый объект – угроза, обозревающий объект – контрмера (средство защиты). Вновь из содержательной постановки следует, что более естественна на практике модель, когда можно обозревать только часть объекта одной камерой; когда критичные объекты необходимо обозревать, возможно, несколькими камерами; когда общее качество системы защиты может варьироваться.

Для описания всех этих ситуаций уже не достаточно простой задачи о покрытии, а возникает задача об α-глубине.

Верхняя оценка α-глубины одного класса (0,1)-матриц

Пусть T_m^n - класс бинарных прямоугольных матриц размеров mxn, q – натуральное число, $0 \le q \le n$. Введем некоторые параметры:

1. β_i - число строк в матрице, содержащих более (i-1) единицы, i=1,…,n. $\beta(A)=(\beta_1,\beta_2,\ldots,\beta_n)$.
2. $\beta_k^1(q)$ - число единиц в k-м столбце, которые принадлежат строкам, содержащим более (q-1) единицы. $\beta^1(A,q)=(\beta_1^1(q), \beta_2^1(q), \ldots, \beta_n^1(q))$.
3. $\beta_k^0(q)$ - число нулей в k-м столбце, которые принадлежат строкам, содержащим более (q-1) единицы. $\beta^0(A,q)=(\beta_1^0(q), \beta_2^0(q), \ldots, \beta_n^0(q))$.
4. Через $\overline{P}(A)$ обозначим 3n-мерный вектор, компонентами которого являются последовательно записанные компоненты трех вышеприведенных векторов: $\overline{P}(A) = (\beta(A), \beta^1(A,q), \beta^0(A,q))$.
5. Через $T(\overline{P}(A))$ обозначим подкласс T_m^n -, содержащий матрицы с одинаковыми векторами $\overline{P}(A)$.

Определение. α-глубиной подкласса матриц $T(\overline{P}(A))$ называется максимальная α-глубина матрицы A из этого подкласса.

Обозначим ее $\zeta_\alpha(\overline{P}(A))$, а ее верхнюю оценку через $\overline{\zeta_\alpha}(\overline{P}(A))$.

Если ввести еще одну группу параметров (они нам понадобятся исключительно из технических соображений):

6. A_q – подматрица A, состоящая из строк, содержащих более (q-1) единицы, q=1,…,n. $E(A_q)$ и $Z(A_q)$ – количества единиц и нулей в этой подматрице;
7. Пусть $l_i(A)$ ($\lambda_i(A)$) число строк в ,содержащих ровно i единиц (нулей). $l(A)=(l_1(A), l_2(A),\ldots, l_n(A))$. $\lambda(A)=(\lambda_0(A), \lambda_1(A),\ldots, \lambda_{n-1}(A))$. Заметим, что $\lambda(A)=(l_n(A), l_{n-1}(A),\ldots, l_1(A))$;

то это позволит указать очевидные связи между введенными ранее параметрами виде нижеприведенных двух типов равенств (a), и b)) и одного типа неравенств – c).

Действительно, так как $E(A_q) = \sum_{j=q}^{n} j l_j(A)$ и $Z(A_q)= \sum_{j=0}^{n-q} j\lambda_j(A)$, но с другой стороны $E(A_q) = \sum_{i=1}^{k} \beta_i^1(q)$ и $Z(A_q)= \sum_{i=1}^{k} \beta_i^0(q)$, а $l_i=\beta_i-\beta_{i+1}$, $\lambda_i=l_{n-i}=\beta_{n-i}-\beta_{n-i+1}$, i=1,…,n, то отсюда и получаем ограничения:

a) $\sum_{j=q}^{n} j(\beta_j - \beta_{j-1}) = \sum_{i=1}^{n} \beta_i^1(q), 0 \le \beta_i^1(q) \le m, i = 1,\ldots,n.$

b) $\sum_{j=0}^{n-q} j(\beta_{n-j} - \beta_{n-j+1}) = \sum_{i=1}^{n} \beta_i^0(q), 0 \le \beta_i^0(q) < m, i = 1,\ldots,n.$

c) $\beta_1=m$, $0 \le \beta_i \le m$, i=2,3,…,n. $m \le \sum_{i=1}^{n} \beta_i \le mn$.

Теорема 1. Справедливо неравенство

$$\overline{\zeta_\alpha}(\overline{P}(A)) \le \min_q \min_s \{s + \frac{\alpha}{C_{\beta_q}^s} \sum_{k=1}^{n} \sum_{v=0}^{\alpha-1} C^v_{\beta_k^1(q)} C^{s-v}_{\beta_k^0(q)}\},$$

где минимумы берутся по множествам натуральных чисел из отрезков [1,m] для s и [1,n] для q, а параметры $\beta(A)$, $\beta^1(A,q)$, $\beta^0(A,q)$ удовлетворяют ограничениям a), b),c).

Доказательство. Зафиксируем q. Рассмотрим произвольную матрицу $A=(a_{ij})$ из класса $T(\overline{P}(A))$. В ней берем подматрицу Aq, в которой выбираем произвольные s строк. Для краткости эту последнюю обозначим просто A`.

Пусть теперь число H(A`) – количество столбцов в A`, каждый из которых содержит не более (α-1) единицы. Пусть $\overline{H}_A(s,q,\alpha)$ - среднее значение H(A`) на множестве всех подматриц матрицы A_q, содержащих ровно s строк. Тогда

$$\overline{H}_A(s,q,\alpha) = \frac{1}{C_{\beta_q}^s} \sum_{A` \in A_q} H(A`), \qquad (1)$$

где суммирование производится по всевозможным наборам из s строк матрицы A_q.

Из (1) вытекает, что в A_q существует подматрица $A_0`$ из s строк такая, что число столбцов в ней, содержащих менее, чем α единиц не превосходит $\overline{H}_A(s,q,\alpha)$. Отсюда следует, что

$$\overline{\zeta_\alpha}(\overline{P}(A)) \le s + \alpha \overline{H}_A(s,q,\alpha). \qquad (2)$$

Введем теперь $\tilde{N}_{\beta_q}^s$ функций вида:

$$f_k^{i_1,\ldots,i_s} = \begin{cases} 1, \sum_{t=1}^{s} a_{i_t k} < \alpha; \\ 0, \sum_{t=1}^{s} a_{i_t k} \ge \alpha. \end{cases}$$

Если подматрица $A_0^{`}$ состоит из строк: $u_{i_1}, u_{i_2}, \ldots, u_{i_s}$, тогда

$$H(A^{`})=\sum_{k=1}^{n} f_k^{i_1,,,i_s} \quad .$$

Из (2) и (5) следует

$$\overline{H}_A(s,q,\alpha)=\frac{1}{C_{\beta_q}^{s}}\sum_{k=1}^{n}\sum_{\{i_1,\ldots,i_s\}} f_k^{i_1,\ldots,i_s} \quad .$$

Внутренняя сумма в (6) равна числу выборов совокупности строк $\{u_{i_1}, u_{i_2}, \ldots, u_{i_s}\}$ таким образом, чтобы для элементов k-го столбца матрицы A выполнялось неравенство

$$\sum_{t=1}^{s} a_{i_t k} < \alpha;$$

что эквивалентно одному из следующих равенств:

$$\sum_{t=1}^{s} a_{i_t k} = v \text{, где } v=0,1,\ldots,\alpha-1. \qquad (3)$$

Но k-й столбец содержит ровно $\beta_k^1(q)$ единиц, лежащих в строках, составляющих A_q, и ровно $\beta_k^0(q)$ нулей в этих же строках. Тогда v-е равенство в (3) выполнимо $C_{\beta_k^1(q)}^{v} C_{\beta_k^0(q)}^{s-v}$ способами. Так как v строк выбирается произвольно из $\beta_k^1(q)$ строк, которые содержат в себе все единицы k-го столбца подматрицы A_q, а остальные s-v строк можно выбирать произвольно и независимо из $\beta_k^0(q)$ строк, содержащих нули этого столбца, то отсюда следует равенство:

$$\sum_{\{i_1,\ldots,i_s\}} f_k^{i_1,\ldots,i_s} = \sum_{v=0}^{\alpha-1} C_{\beta_k^1(q)}^{v} C_{\beta_k^0(q)}^{s-v} \quad .$$

Но тогда

$$\overline{H}_A(s,q,\alpha)=\frac{1}{C_{\beta_q}^{s}}\sum_{k=1}^{n}\sum_{v=0}^{\alpha-1} C_{\beta_k^1(q)}^{v} C_{\beta_k^0(q)}^{s-v}.$$

Теперь, используя (2), минимизируем по s и по q. Окончательно получаем

$$\overline{\zeta}_\alpha(\overline{P}(A)) \le \min_q \min_s \{s+\frac{\alpha}{C_{\beta_q}^{s}}\sum_{k=1}^{n}\sum_{v=0}^{\alpha-1} C_{\beta_k^1(q)}^{v} C_{\beta_k^0(q)}^{s-v}\}.$$

Теорема доказана.

Прием доказательства, который здесь используется. Является классическим. (См. [3, 100 с.]).

Частные случаи закономерностей расположения единиц матрицы

Определенные интерес представляет ситуация, когда доказанная выше теорема упрощается за счет учета закономерностей расположения единиц матрицы. При этом для оценки качества эвристик, которые могут применяться при решении задачи интересно было бы иметь не только верхнюю, но и нижнюю оценку мощности минимального покрытия. Рассмотрим здесь два таких примера.

Класс T*.

Пусть подкласс T* вышеопределенного класса матриц, задается следующими параметрами:

1. $\beta(A)=(m,\{m-n\},\ldots,\{m-n(1+1/2+\ldots+1/(i-1))\},\ldots,\{m-n(1+1/2+\ldots+1/(p-1))\},0,\ldots 0)$.
2. $\beta^1(A,1)=(p,\ldots,p)$, $\beta^1(A,2)=(p-1,\ldots,p-1),\ldots$, $\beta^1(A,i)=(p-i+1,\ldots,p-i+1),\ldots$, $\beta^1(A,p-1)=\ldots=\beta^1(A,n)=(0,\ldots,0)$.
3. $\beta^0(A,1)=(m-p,\ldots,m-p)$, ,…, $\beta^0(A,i)=(\{m-p+i-1-n(1+1/2+\ldots+1/(i-1))\},\ldots,),\ldots$, $\beta^0(A,w)=\ldots=\beta^1(A,n)=(0,\ldots,0)$.

Здесь {x}- целая часть с избытком, а в 3. w – минимальный индекс, при котором компоненты вектора обнуляются.

Этот подкласс содержит множество матриц T*(p) следующего вида. Матрица из T*(p) состоит из расположенных друг под другом p блоков: $A_1,\ldots,A_p$. В любом столбце блока A_k ровно одна единица. Во всех строках, кроме последней – k единиц. В последней от 1 до k единиц. (Так как мы ищем верхнюю оценку, то этой последней строкой тоже можно считать строку с k единицами, чтобы не загромождать выкладки).

$$A_k = \begin{matrix} 1\ldots1 & 0\ldots0 & \ldots & 0\ldots0 \\ 0\ldots0 & 1\ldots1 & 0\ldots0 & 0\ldots0 \\ \ldots & \ldots & \ldots & \ldots \\ 0\ldots0 & \ldots & 0\ldots0 & 1\ldots1 \end{matrix}$$

Очевидно, что 1-глубина блока A_k равна {n/k}.

Лемма. Минимальная 1-глубина для матриц из T* достигается матрицах из T*(p).

Теорема 2. Для класса T* выполняется неравенство

$\overline{\zeta}_\alpha(\overline{P}(A)) \le \min\{\ (m/p)\ln(np/m)$, ((m-nε(q*))/(p+1-q*)$\{1+\ln(n(p+1-q^*)/(m-n\varepsilon(q^*))\}$,

где $\varepsilon(q)=\sum_{i=1}^{q-1}\frac{1}{i}$, а q*=q*(p,m,n) – решение уравнения

q-ε(q)=p+1-m/n.

Доказательство. Из теоремы 1 следует:

$$\overline{H}_A(s,q,1)=\frac{1}{C_{\beta_q}^{s}}\sum_{k=1}^{n} C_{\beta_k^0(q)}^{s} = n\frac{C_{\varphi-h}^{s}}{C_{\varphi}^{s}} \le n(1-h/\varphi)^s,$$

где h=p-q+1, φ= m-nε(q) при q>1 и φ=m при q=1.

Отсюда следует

$$\overline{\zeta}_\alpha(T^*) \le \min_q \min_s \{s+n\exp(-sh/\varphi)\}.$$

Минимизируя эту функцию по s, получаем экстремум в точке s*=(φ/h) ln(nh/φ).

Отсюда следует

$$\overline{\zeta}_\alpha(T^*) \le \min_q (\varphi/h)\{1+\ln(nh/\varphi)\}.$$

Минимизируя эту функцию по q, при q>1 получаем уравнение, корень которого является экстремумом: nh=φ, а для случая q=1 имеем $(\varphi/h)\{1+\ln(nh/\varphi)\}=(m/p)\ln(np/m)$.

Отсюда следует

$\overline{\zeta_\alpha}(\overline{P}(A)) \le \min\{(m/p)\ln(np/m)$, ((m-nε(q*))/(p+1-q*){1+ln(n(p+1-q*)/(m-nε(q*))}.

Теорема доказана.

Класс T^0.

Рассмотрим матрицу размеров kx k(k+1)/2 следующего вида

$$A_0=\begin{vmatrix} 1 & 0 & 0 & \dots & \dots & 0 \\ 0 & 11 & 0 & \dots & \dots & 0 \\ 0 & 0 & 111 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1111 & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 0 & 1\dots1 \end{vmatrix}.$$

В ней в первой строке 1 единица, во второй – 2, …, в k-й – k единиц. Запишем теперь друг под другом (k+1)/2 таких матриц. Получим матрицу размеров nxn, где n= k(k+1)/2 x k(k+1)/2. Обозначим это множество матриц через $T^0(k)$.

Эти матрицы входят в класс T^0 с параметрами:

1. $\beta(A)=(k(k+1)/2, \{(k-1)(k+1)/2\},\dots,\{(k-i+1)(k+1)/2\},\dots, \{(k+1)/2\})$.
2. $\beta^1(A,1)=((k+1)/2,\dots,(k+1)/2)$, $\beta^1(A,2)=(0,(k+1)/2,\dots,(k+1)/2),\dots$, $\beta^1(A,i)=(0,\dots,0,(k+1)/2,\dots,(k+1)/2),\dots$, $\beta^1(A,v)=\dots=\beta^1(A,n)=(0,\dots,0)$.
3. $\beta^0(A,1)=(n-(k+1)/2,\dots,n-(k+1)/2),\dots$, $\beta^0(A,i)=(\{n-(k+1)(i-1)/2\},\dots,\{n-(k+1)(i-1)/2\},\{n-(k+1)i/2\}\dots,\{n-(k+1)i/2\}),\dots$, $\beta^0(A,k)=(\{(k+1)/2\},\dots,\{(k+1)/2\},0,\dots,0),\dots$, $\beta^0(A,w)=\dots=\beta^1(A,n)=(0,\dots,0)$.

Здесь {x}- целая часть с избытком, а в 2 и 3 v и w – минимальные индекс, при котором компоненты вектора обнуляются. В $\beta^1(A,i)$ последний 0 находится на месте с индексом i(i-1)/2, а в $\beta^0(A,i)$ на этом месте – последний элемент вида n-(k+1)(i-1)/2. В $\beta^0(A,k)$ последний ненулевой элемент находится на месте с индексом k(k-1)/2.

Лемма. Класс T^0 удовлетворят ограничениям a), b), c).

Лемма. Минимальная 1-глубина для матриц из T^0 достигается матрицах из $T^0(k)$.

Теорема. Для класса T^0 выполняется неравенство:

$\overline{\zeta_\alpha}(\overline{P}(A)) \le (k+1-q^*)\{\ln(k+q^*)/2\}+(k-q^*+1)+q^*(q^*-1)/2$,

где q*=q*(k) – решение уравнения

$$\frac{2q-1}{2}\left[1-\frac{2}{(q+k)}\right]=\ln\frac{q+k}{2}.$$

Доказательство. Из теоремы 1 следует:

$$\overline{H}_A(s,q,1)=\frac{1}{C^s_{\beta_q}}\sum_{k=1}^{n}C^s_{\beta^0_k(q)}=W(q)+V(q)\frac{C^s_{\varphi-h}}{C^s_\varphi}, \quad (4)$$

где φ=n+(k+1)(q-1)/2, h=(k+1)/2, W(q)=q(q-1)/2, V(q)=n-q(q-1)/2.

Из теоремы 1 имеем:

$$\overline{\zeta_\alpha}(\overline{P}(A)) \le \min_q \min_s\{s+\frac{\alpha}{C^s_{\beta_q}}\sum_{k=1}^{n}\sum_{v=0}^{\alpha-1}C^v_{\beta^1_k(q)}C^{s-v}_{\beta^0_k(q)}\}.$$

Рассмотрим выражение в скобках с учетом (4):

$$s+\overline{H}_A(s,q,1)\le s+W(q)+V(q)\frac{C^s_{\varphi-h}}{C^s_\varphi}\le s+W(q)+V(q)$$

$(1-h/\varphi)^s\le s+W(q)+V(q)\exp(-sh/\varphi)$.

Минимизируя эту функцию по s, получаем экстремум в точке s*=(φ/h) ln(V(q)h/φ).

Отсюда следует

$\overline{\zeta_\alpha}(T^*) \le \min_q[(\varphi/h)\ln(V(q)h/\varphi)+W(q)+\varphi/h]$.

Минимизируя эту функцию по q, при q>1 получаем уравнение для точки экстремума:

$$\frac{2q-1}{2}\left[1-\frac{2(k-q+1)}{2n+q-q}\right]=\ln\frac{n(n-q(q-1)/2)}{kn(1-(q-1)/k)}.$$

Подставляя n=k(k+1)/2, после упрощений получаем:

$$\frac{2q-1}{2}\left[1-\frac{2}{(q+k)}\right]=\ln\frac{q+k}{2},$$

корень которого q* является экстремумом.

Окончательно получаем:

$\overline{\zeta_\alpha}(\overline{P}(A)) \le (k+1-q^*)\{\ln(k+q^*)/2\}+(k-q^*+1)+q^*(q^*-1)/2$.

Теорема доказана.

Выводы

На основе полученных в работе результатов можно в какой-то степени преодолеть невозможность точного решения оптимизационной задачи, возникающей при моделировании некоторых прикладных проблем информационной безопасности.

Так как задача о покрытии NP-трудна и точно решается лишь для небольших размерностей, то вместо точного решения можно применять эвристики, для оценки качества при подборе эвристи-

ки можно сравнивать полученные нею результат с верхними и нижними оценками мощности покрытия или α-глубины.

Безусловно, данный метод корректен, если сама исходная ситуация моделируется матрицами из рассматриваемых классов. Учитывая, что строки и столбцы можно менять местами, а также факт использования эвристических методов, некоторым дополнительным эвристическим аргументом может служить «степень похожести» матрицы из модели на матрицы рассматриваемых классов. Однако, это тема отдельного разговора.

***Рецензент**: Матвеев Валерий Александрович, доктор технических наук, профессор, заведующий кафедры ИУ8 «Информационная безопасность» МГТУ им.Н.Э.Баумана, Москва, v.a.matveev@bmstu.ru*

Литература:

1. Гордеев Э.Н. Использование радиуса устойчивости задач для скрытия и проверки корректности информации // Инженерный журнал: наука и инновации. 2013. № 11 (23). С. 3.
2. Артеменко В.И., Гордеев Э.Н., Журавлев Ю.И. и др. Метод формирования оптимальных программных траекторий робота-манипулятора // Кибернетика и системный анализ. 1996. № 5. С. 84-106.
3. Леонтьев В.К. Комбинаторика и информация. Часть 1. Комбинаторный анализ. М.: МФТИ, 2015. 173 с.

COVERING PROBLEM AND MATHEMATICAL MODELLING IN INFORMATION SECURITY

***Gordeev E.N.*[2]**

The minimum covering problem is an important part of some mathematical models, arising from information security. Examples of the use of discrete optimization problems in such mathematical models can be found in [1]. In this article are given two such examples. By virtue of NP–hardness of the problem, interest objectives are bounds of the minimum value of the covering. A more appropriate use of the problem in mathematical models carried out by generalization by introducing the «weight» of the covering. The paper deals with the well–known generalization covering problem – the problem of α–depth matrices. In real models, there are certain patterns in the arrangement of elements of the matrix associated with the properties of «covering» and «covered» objects. Examples of such laws, upper bounds for coverage of power in general, as well as two classes of matrices are considered, for which you can refine and simplify this assessment. The results quite naturally apply to large–scale problems. However, today the exact algorithms allow solving the problem in the matrices, the size of which does not exceed 40–50. Therefore, obtained results are a useful tool for checking the quality of heuristic algorithms.

***Keywords**: information security, quality of heuristics, α–depth of matrices, upper bounds in the covering problem.*

References:

1. Gordeev E.N. Ispol'zovanie radiusa ustoychivosti zadach dlya skrytiya i proverki korrektnosti informatsii, Inzhenernyy zhurnal: nauka i innovatsii. 2013. No 11 (23), P. 3.
2. Artemenko V.I., Gordeev E.N., Zhuravlev Yu.I. i dr. Metod formirovaniya optimal'nykh programmnykh traektoriy robota-manipulyatora, Kibernetika i sistemnyy analiz. 1996. No 5, pp. 84-106.
3. Leont'yev V.K. Kombinatorika i informatsiya. Chast' 1. Kombinatornyy analiz. M.: MFTI, 2015. 173 P.

2 Eduard Gordeev, Dr.Sc. (Math), Professor, Professor at Bauman Moscow State Technical University, Moscow, tatmigor@gmail.com