М. В. Тимонин

ПРОБЛЕМА ОПТИМИЗАЦИИ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ПРИ ПЛАНИРОВАНИИ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ.

1. Актуальность решения задачи

Несмотря на разнообразие методов распределения ресурсов, существующих в различных областях, исследование этого вопроса в области ИБ находится в начальной стадии. В литературе предлагаются лишь способы выбора общего размера бюджета защитных мероприятий, основанные на анализе вероятностей угроз [1] или теории игр [2]. Вопросы же распределения бюджета ИБ решаются, как правило, эмпирически или на основе базовых методов экономического анализа. Так, согласно опросу, результаты которого приведены в работе [3], основным инструментом для принятия решений по размеру инвестиций в большинстве организаций является оценка чистого дисконтированного дохода (ЧДД, NPV). Вторым по популярности методом является простое ранжирование преимуществ (под которыми обычно понимается снижение риска), получаемых от внедрения того или иного средства или проекта. В литературе, как русскоязычной, так и зарубежной, предлагаются также и другие подходы. В основном они базируются на методике AHP (analytic hierarchy process) [4]. Рассматриваются как общие вопросы оптимизации инвестиций [5, 6, 7], так и более специфические, например методы выбора коммерческих средств защитного ПО [8]. Некоторые авторы применяют методы многокритериального анализа [9], иногда дополняя его средствами теории игр [10]. Наконец, предлагаются и решения, основанные на теории надежности [11]. Главными проблемами, которые можно выделить в имеющихся подходах, являются следующие.

1. Игнорирование взаимодействия компонентов защиты. Так, вложение в некоторые части системы может привести к улучшению и в других областях. С другой стороны, разделение средств между компонентами, обладающими сходным набором функций, является зачастую нерациональным.

2. Отсутствие унифицированного подхода к оптимизации вложений на всех уровнях — фирмы, отдела и отдельного проекта.

3. Слабые средства анализа чувствительности модели, не позволяющие получить объективные суждения о наиболее востребованных инвестициях при принятии решений.

4. Необходимость большого числа данных для моделей вероятностей всех угроз, оценок потенциального ущерба и уровня атакующего. Как правило, в практических применениях доступные данные неполны и неточны.

5. Слабые средства моделирования, не позволяющие выражать весь спектр логических связей — причинно-следственных, необходимости, достаточности и т. д.

На основе предлагаемого в данной статье подхода делается попытка решить перечисленные проблемы. Так, взаимодействие компонентов в рамках модели описывается с помощью средств теории нечеткой меры. Существует возможность указать характер взаимодействия для любой группы элементов, а также смоделировать требования достаточности или необходимости какого-либо компонента. Подробно вопрос моделирования системы ИБ с помощью средств данной теории рассматривается в статье [12]. Подход нетребователен к количеству данных, необходимых для функционирования модели, и позволяет начать работу уже с малым количеством информации. Возможно использование качественных критериев, таких как, например, ранг компонента в группе. При этом числовую оценку его важности приводить необязательно, хотя, будучи доступной, такая оценка позволит увеличить точность получаемых результатов. Наконец, характер используемой методики позволяет решать многокритериальные задачи планирования как на уровне организации, так и на уровне отдельных проектов, а при желании интегрировать эти вопросы в единую модель. Подробное описание примера, демонстрирующего процесс практического применения модели, приводится во второй части данной статьи, публикуемой отдельно. Здесь же мы остановимся на математической сути вопроса.

2. Теоретические основы предлагаемого подхода

Введем два основных понятия

Определение 1. *Пусть задано конечное множество X и множество его подмножеств* 2^X. *Емкостью будем называть функцию множества* $\upsilon: 2^X \to \mathbf{R}$ *такую что:*

1. $\upsilon(\varnothing) = 0$
2. $A \subseteq B \Rightarrow \nu(A) \leq \nu(B)\ \forall A, B \in 2^X$

В данной статье, также везде подразумевается, что используемая емкость нормализована, то есть $\nu\ (X) = 1$.

Определение 2. *На конечном множестве X, интегралом Шоке дискретной функции* $f: X \to \mathbf{R}$ *со множеством значений* $\{x_1, \dots, x_n\}$ *относительно емкости* $\upsilon: 2^X \to \mathbf{R}$ *называется*

$C_\upsilon\{x_1, \dots, x_n\} = \Sigma_{i=1}^{n} (x_{(i)} - x_{(i-1)})\, \upsilon\ (x \mid f\ (x) \geq x_{(i)})$ Где $x_{(1)}, \dots, x_{(n)}$ перестановка элементов $x_1, \dots, x_n$, такая что $x_{(1)} \leq x_{(2)} \leq \dots \leq x_{(n)}$, а $x_{(1)} = 0$.

В статье[12] автором была предложена модель оценки риска ИБ, основанная на агрегации данных с помощью интеграла Шоке. Модель представляет собой древовидную структуру, пример которой представлен на рисунке 1. Общая идея состоит в построении таксономии защитных мероприятий, входящих в систему ИБ предприятия.

В данной статье представлено расширение данного подхода для решения задач оптимального распределения ресурсов. Для этого необходимо параметризовать модель с помощью вектора вложений $z = \{z_1, \dots, z_n\}$. Концевые вершины графа содержат управляемые элементы, каковыми могут служить как технические, так и организационные меры. Для таких вершин вводятся функции полезности $f_i\ (z_i)$ связывающие уровень защищенности компонента системы защиты с количеством полученных им средств z_i. В вершинах, имеющих дочерние вершины, функции полезности определяются опосредованно.

$f_A\ (L) = C_\upsilon\ (f_1(z_1),\ \dots, f_n\ (z_n))$

где функции $f_i\ (z_i)$ относятся к вершинам, являющимся дочерними для вершины A, $C_H\ (f_1(z_1), \dots\ f_n\ (z_n))$, - интеграл Шоке, взятый по отношению к мере υ, описывающей характер связи дочерних вершин с родительской, а $L = \Sigma\ z_i$ - общий объем вложений, полученных родительской вершиной. Функции $f_i\ (z_i)$ полагаются гладкими и вогнутыми, что является приближением, которое позволяет проводить анализ системы средствами математического программирования и широко встречается в литературе (см., например, [1]). Вогнутость обусловлена снижающейся маргинальной полезностью инвестиций, что в контексте ИБ выглядит вполне закономерным предположением [1]. Продолжая построение модели указанным образом, в итоге получаем функцию полезности корневой вершины, являющуюся индексом защищенности системы. Становится возможным сформулировать оптимизационную задачу, целевая функция которой представляет собой «вложенные» друг в друга интегралы Шоке для различных вершин. В литературе такая конструкция называется мношаговым интегралом Шоке [13].

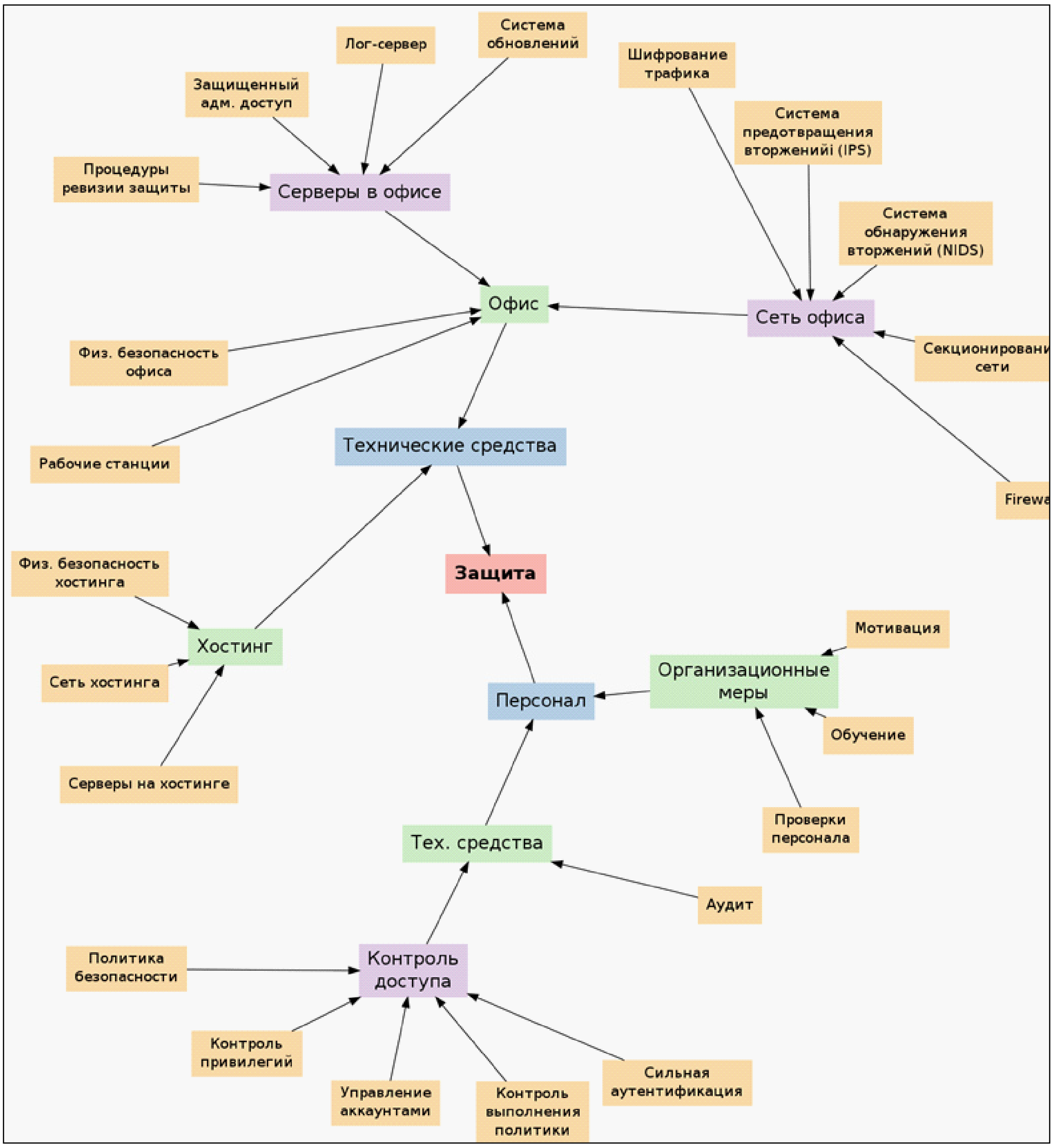

Рис. 1. Таксономия защитных средств

3. Методы оптимизации

В данной статье ввиду ограниченного объема публикации рассматривается лишь процесс оптимизации одиночной ветви. Целевая функция, таким образом, имеет вид:

$$\begin{aligned} & C_{\upsilon}(f_1(z_1),\ldots,f_n(z_n)) \uparrow max \\ & \Sigma z_i = L \\ & z \geq 0 \end{aligned} \quad , \qquad (1)$$

где z — вектор вложений, $f_i(z_i)$ — функции полезности, связывающие уровень защищенности компонента системы защиты с количеством полученных им средств, C_{υ} — интеграл Шоке по отношению к мере υ — вектора, описывающего связь корневой вершины ветви с дочерними, а L — общий бюджет инвестиций. Методы, применяемые для проведения оптимизации в предлагаемой модели, различаются в зависимости от характера связей между вершинами графа, то есть от характера емкости υ. Имеет место следующая теорема.

Теорема 1 [14]. *Функция $\upsilon:2^X\to\mathbf{R}$ является субмодулярной (супермодулярной) тогда и только тогда, когда ее интеграл Шоке является выпуклым (соответственно вогнутым) на $\mathbf{R}$.*

Дополним данную теорему, расширив ее на случай, когда значения интегрируемой функции параметрически зависят от переменной z.

Следствие 1. *Интеграл Шоке $C_\upsilon(f_1(z_1),\ldots,f_n(z_n))$ относительно емкости $\upsilon:2^X\to\mathbf{R}$ является выпуклым (вогнутым) на $\mathbf{R}^n$ при всех возможных выпуклых(вогнутых) $f_i(z_i)$ тогда и только тогда, когда емкость $\upsilon:2^X\to\mathbf{R}$ является субмодулярной (супермодулярной), а функции $f_i(z_i)$ являются выпуклыми (вогнутыми).*

Доказательство. Интеграл Шоке $C_\upsilon(f_1,\ldots,f_n)$ является неубывающей функцией по всем аргументам f_i. Сочетая это с предыдущей теоремой и правилами сохранения выпуклости для векторной композиции функций, получаем искомый результат.

Таким образом, в задаче можно выделить два случая — выпуклый и невыпуклый.

3.1. Выпуклый случай

В случае супермодулярной емкости υ и вогнутых функций $f_i(z_i)$ интеграл Шоке будет представлять собой выпуклую, хотя и недифференцируемую функцию, а значит, может быть оптимизирован методами выпуклого программирования. Численные эксперименты, демонстрирующие быстродействие модели, приводятся во второй части статьи. Одним из методов решения такой задачи может послужить метод проекции субградиента(см., например, [15]). Будем различать два типа точек z^k. Если на очередном шаге k алгоритм попадает в точку «излома» $f_i(z_i^k)=f_j(z_j^k)$, для некоторых $i, j=1,\ldots,n$, то супердифференциал $\partial\ C_\upsilon(f_1(z_1),\ \ldots,\ f_n(z_n))$ будет ограничен векторами $\{\rho_1^i\frac{\partial f_1}{\partial z_1},\ \ldots,\ \rho_n^i\frac{\partial f_n}{\partial z_n}\}$, ввиду существования нескольких перестановок $f_{(1)}(z_{(1)})\le\cdots\le f_{(n)}(z_{(n)})$. В этом случае в качестве суперградиента возможно выбрать любой из них. Коэффициенты $\rho_1^i,\ldots,\rho_n^i$ вычисляются с помощью определения интеграла Шоке $\rho_i=\upsilon\ (f_{(i)}(z_{(i)}))-\upsilon\ (f_{(i+1)}(z_{(i+1)}))$. В точках, отличных от точек «излома», то есть точек, в которых $f_i(z_i^k)=f_j(z_j^k)$ для некоторых $i, j=1,\ \ldots,\ n$, целевая функция $C_\upsilon(f_1(z_1),\ \ldots,f_n(z_n))$ является дифференцируемой в обычном смысле. В этом случае, градиент вычисляется следующим образом:

$$\nabla C\upsilon(f_1(z_1),\ \ldots,\ fn(zn))=\{\rho_1\frac{\partial f_1}{\partial z_1},\ \ldots,\ \rho_n\frac{\partial f_n}{\partial z_n}\}$$

3.2. Невыпуклый случай

Для невыпуклого случая автором была предложена модификация метода ветвей и границ, опирающаяся на свойства емкости. Задача преобразуется в множество выпуклых задач, решение которых производится методами, описанным в предыдущем параграфе. Преобразование производится путем нахождения минимального дизъюнктивного разложения емкости Н. Имеет место следующая теорема.

Теорема 2. *Интеграл Шоке функции, значения которой являются выпуклыми функциями параметра z_i , является выпуклой функцией на каждой области, определенной перестановкой $f_{(1)}(z_{(1)})\le\cdots\le f_{(n)}(z_{(n)})$.*

Доказательство. Достаточно заметить, что на каждой области интеграл Шоке представляет собой неотрицательную сумму значений интегрируемой функции. $C_\upsilon(f_1(z_1),\ldots,f_n(z_n))=\Sigma_{i=1}^n f_{(i)}(z_{(i)})(\upsilon\ (A_{(i)})-\upsilon\ (A_{(i+1)}))$, а ввиду монотонности меры υ все разности $(\upsilon\ (A_{(i)})-\upsilon\ (A_{(i+1)}))$ будут неотрицательны.

Перестановки $f_{(1)}(z_{(1)})\le\cdots\le f_{(n)}(z_{(n)})$ образуют разбиение допустимого множества задачи (1), пересекаясь только в граничных точках. Таким образом, простейшим методом глобального решения задачи максимизации будет решение $n!$ вогнутых задач, то есть перебор по всем перестановкам $f_{(1)}(z_{(1)})\le\cdots\le f_{(n)}(z_{(n)})$. К сожалению, такой подход обладает сложностями вычислительного характера. Ситуацию, впрочем, можно улучшить, если заметить, что области, соответствующие перестановкам, могут объединяться в вогнутые «кластеры». Размеры и положение этих кластеров определяются характером емкости Н. Критическими случаями являются единственный кластер при двухмонотонной емкости, то есть случай выпуклой задачи, и полное отсутствие кластеров (то есть $n!$ кластеров мощности 1). Максимум для всей группы областей, входящих в кластер, может быть эффективно найден средствами выпуклой оптимизации. Такой подход позволяет существенно снизить количество перебираемых вариантов.

Процесс поиска вогнутых областей можно сформулировать в виде следующей задачи. Необходимо найти разбиение допустимой области определения функции $C_v(f_1(z_1),\ldots,f_n(z_n))$ на подобласти, такие, чтобы функция была вогнутой на каждой из них, а количество подобластей в разбиении было бы минимальным. Можно говорить, что для решения задачи необходимо представить интеграл Шоке в дизъюнктивной форме с дополнительным требованием минимальности числа дизъюнктов. Последнее требование обеспечит оптимальность схемы ветвления.

3.2.1. Минимальное дизъюнктивное представление емкости

Допустимая область в задаче с n переменными представляет собой $(n-1)$-симплекс. Гиперповерхности $f_i(z_i) = f_j(z_j)$, $i, j = 1,\ldots,n$ разбивают симплекс на $n!$ частей, которые биективно (взаимно однозначно) соответствуют перестановкам $f_{(1)}(z_{(1)}) \leq\cdots\leq f_{(n)}(z_{(n)})$. Кроме того, известно, что элементы множества 2^x образуют решетку (т. е. любое двухэлементное множество имеет точную верхнюю и нижнюю грани) относительно операции включения. Тогда множество максимальных цепей $\varnothing \subset K_1 \subset\cdots\subset K_n = X$ (т. е. линейно упорядоченных подмножеств, к которым нельзя добавить ни один элемент без потери свойства упорядоченности) будет биективно соответствовать множеству перестановок $f_{(1)}(z_{(1)}) \leq\cdots\leq f_{(n)}(z_{(n)})$.

Емкость можно представить в виде дизъюнкции $n!$ тотально монотонных мер [16]. В конечномерном случае данные меры являются мерами необходимости, т. е. мерами, вся масса которых сосредоточена на элементах максимальной цепи. Иными словами, для некоторой максимальной цепи $\varnothing \subset K_1 \subset\cdots\subset K_n = X$ обращение Мебиуса емкости β будет иметь значения, отличные от нуля, только для элементов, входящих в эту цепь:

$$m(K_i) = v(K_i) - v(K_{i-1})$$
$$m(A) = 0,\ A \notin K \quad .$$

Достаточно очевидно, что $\beta(A) = v(A)$, $\forall A \in K$. Заметим также следующий факт. Пусть K_1 и K_2 — цепи, соответствующие областям A_1 и A_2, а β_1 и β_2 — сфокусированные на этих цепях меры необходимости. Тогда мера, соответствующая области $A_1 \cup A_2$ равняется

$$\beta_{12}(A) = \beta_1(A) \vee \beta_2(A)$$

Отметим, что мера β_{12} может быть не тотально монотонной. В случае, если это свойство сохраняется, мы можем расценивать эту емкость как меру доверия (теория Демпстера-Шафера). Будем обозначать множество цепей как **C**. Проблему можно переформулировать как задачу нахождения минимального разбиения множества **C**, такого, что емкости β_{ρ_i}, соответствующие подмножествам $\rho_i \subset C, \cup_i \rho_i = C$, тотально монотонны.

Алгоритм построения минимального представления включает в себя следующие этапы.

1. Разбиение допустимой области на подмножества такие, что интеграл Шоке является вогнутым на каждом из них.

2. Нахождение мер доверия, соответствующих подмножествам, найденным в пункте 1.

3. Слияние излишне разделенных подмножеств и соответствующих мер доверия.

Для получения разбиения допустимой области мы будем использовать свойство, более сильное, чем супермодулярность, а именно тотальную монотонность. Важным для емкости, обладающим таким свойством, является то, что ее обращение Мебиуса содержит только положительные коэффициенты. Таким образом, первым этапом представления емкости в требуемом виде является избавление от всех негативных коэффициентов ее обращения Мебиуса. Разложение проводится следующим образом. Для каждого члена $f_a(z_a)$ слагаемого вида m_i $(f_i\ (z_i) \wedge \ldots \wedge f_j\ (z_j))$, где $m_i < 0$, разделяем допустимую область на части, соответствующие равенствам вида $f_k(z_k) = \wedge\ (f_i\ (z_i),\ \ldots,\ f_k(z_k),\ \ldots,\ f_j\ (z_j))$. К примеру,

$$m_1 f_1(z_1) + m_2 f_2(z_2) - m_{12}(f_1(z_1) \wedge f_2(z_2)) \Rightarrow \begin{cases} m_1 f_1(z_1) + m_2 f_2(z_2) - m_{12}(f_1(z_1) \\ m_1 f_1(z_1) + m_2 f_2(z_2) - m_{12}(f_2(z_2). \end{cases}$$

Аналогичные изменения производятся и в других слагаемых. Например, если бы в представлении присутствовал член вида $m_{123}(f_1(z_1) \wedge f_2\ (z_2) \wedge f_3\ (z_3))$, после указанного выше разложения он превратился бы в $m_{123}(f_1(z_1) \wedge f_3\ (z_3))$ и $m_{123}(f_2\ (z_2) \wedge f_3\ (z_3))$. Получив указанным способом разложение допустимой области, переходим к образованию мер доверия, которые составят дизъюнктивное представление изначальной меры υ. Для этого, обладая для каждого полученного в разбиении подмножества набором неравенств вида $f_i(z_i) \le f_j(z_j)$, определим 2 множества. L_i содержит переменные, стоящие слева в неравенстве $i, i = 1,\ldots,\rho$, а R_i содержит переменные, стоящие справа. Коэффициенты емкости определяются итеративно, начиная с единичных элементов 2^x (которые соответствуют элементам на нижнем уровне графа).

$$Bel_s(A) = \begin{cases} \bigvee\limits_{B \subseteq A} \upsilon(B), & \exists i{:} f_i(z_i) \in R_j,\ f_i(z_i) \notin L_j,\ j = 1,\ \ldots,\ \rho \\ \mathrm{v}(A), & \text{в другом случае} \end{cases}$$

Ввиду наличия в представлении интеграла Шоке коэффициентов, содержащих малое число элементов, которые делят допустимую область на крупные части, на начальных этапах может произойти нежелательное разделение области, на которой интеграл является вогнутым. Это не влияет на верность получаемого результата, однако применительно к задаче оптимизации желательно обладать минимальным числом членов в дизъюнктивном представлении. Таким образом, необходимо произвести следующий шаг — слияние областей. Слияние производится с помощью непосредственного объединения полученных мер доверия с последующей проверкой на монотонность. Практические эксперименты показывают, что число излишне разделенных областей, как правило, невелико.

3.2.2. Глобальный поиск и локальный поиск

С помощью полученного в предыдущем параграфе разложения глобальный поиск производится путем решения набора задач вида (1), где емкость υ заменяется полученными тотально монотонными мерами. Эти задачи могут решаться параллельно для повышения быстродействия процесса. В случае, когда дизъюнктивное разложение содержит очень большое число элементов, возможно применение локального поиска. Известно, что интеграл Шоке по отношению к любой емкости представим в DC(difference of convex) виде $\int f d\upsilon = \int f d\upsilon^+ - \int f d\upsilon^-$, где емкости υ^+ и υ^- получаются из обращения Мебиуса m изначальной емкости: $m^+(A) = max(0, m(A))$, $m^- = min\ (0, m(A))$. Локальный поиск производится с помощью замены в целевой функции второго слагаемого на его линейное приближение. В очередной точке z^k получаем

$$\int f\ (z)\ d\upsilon \approx \int f\ (z) d\upsilon^+ - \int f\ (z^k)\ d\upsilon - \langle \nabla \int f(zk) d\upsilon^-, z - z^k \rangle$$

Метод вычисления градиента приводится выше. Результат возможно улучшить, запуская локальный поиск из различных начальных точек.

4. Заключение

В данной статье рассматривались математические аспекты задачи оптимизации распределения ресурсов при планировании стратегии информационной безопасности. Предложен подход к параметризации модели системы ИБ, основанной на теории нечеткой меры, рассмотрены вопросы выпуклой и невыпуклой оптимизации. Для последней предложены алгоритм дизъюнктивного разложения произвольной емкости и основанный на нем метод ветвей и границ. Практическое применение рассмотрено во второй части статьи.

(*Продолжение статьи — в будущих номерах журнала*)

СПИСОК ЛИТЕРАТУРЫ:

1. *Gordon L. A., Loeb M. P.* The economics of information security investment // ACM Transactions on Information and System Security (TISSEC). 2002. 5 (4). P. 438–457.
2. *Cavusoglu H., Raghunathan S., Yue W. T.* Decision-theoretic and game-theoretic approaches to IT security investment // Journal of Management Information Systems. 2008. 25 (2). P. 281–304.
3. *Gordon L. A., Loeb M. P.* Budgeting process for information security expenditures // Communications of the ACM. 2006. 49 (1). P. 121–125.
4. *Saaty T. L.* How to make a decision: the analytic hierarchy process // European Journal of Operational Research. 1990. 48 (1). P. 9–26.
5. *Кащенко А. Г.* Распределение ресурсов на обеспечение информационной безопасности вычислительной сети предприятия // Информация и безопасность. 2009. 13 (2). С. 209–214.
6. *Bodin L. D., Gordon L. A., Loeb M. P.* Evaluating information security investments using the analytic hierarchy process // Communications of the ACM. 2005. 48 (2). P. 78–83.
7. *Bodin L. D., Gordon L. A., Loeb M. P.* Information security and risk management // Communications of the ACM. 2008. 51 (4). P. 64–68.
8. *Chen Y., Boehm B., Sheppard L.* Measuring security investment benefit for off the shelf software systems — a stakeholder value driven approach // Online Proceedings of Sixth Workshop on the Economics of Information Security (WEIS 2007). June, 2007. Citeseer. P. 25–27.
9. *Butler S. A.* Security attribute evaluation method: a cost-benefit approach // Proceedings of the 24th International Conference on Software Engineering. 2002. ACM. P. 232–240.
10. *Калашников А. В.* Арбитражная модель ресурсного обеспечения информационной безопасности организационных систем // Управление большими системами: сборник трудов. 2006. 14. С. 92–106.
11. *Azaiez M. N., Bier V. M.* Optimal resource allocation for security in reliability systems // European Journal of Operational Research. 2007. 181 (2). P. 773–786.
12. *Тимонин М. В., Лаврентьев В. С.* Использование теории нечеткой меры для агрегации составляющих риска информационной безопасности // Безопасность информационных технологий. 2009. № 4. С. 31–35.
13. *Narukawa Y., Torra V.* Twofold integral and Multi-step Choquet integral // KYBERNETIKA-PRAHA. 2004. 40 (1). P. 39–50.
14. *Lovasz L.* and others. Submodular functions and convexity // Mathematical programming: the state of the art. 1983. P. 235–257.
15. *Поляк Б. Т.* Введение в оптимизацию. М.: Наука. Гл. ред. физ.-мат. лит., 1983.
16. *Bruning M., Denneberg D.* Max-min (σ-) additive representation of monotone measures // Statistical Papers. 2002. 43 (1). P. 23–35.