

УДК 004.056+519.854

## **Модификация метода вектора спада для оптимизационно-имитационного подхода к задачам проектирования систем защиты информации**

Быков А. Ю.<sup>1,\*</sup>, Артамонова А. Ю.<sup>1</sup>

[abykov@bmstu.ru](mailto:abykov@bmstu.ru)

<sup>1</sup>МГТУ им. Н.Э. Баумана, Москва, Россия

---

В статье рассмотрен метод для решения задачи выбора средств защиты информации, который может быть применен в рамках оптимизационно-имитационного подхода. При данном подходе задача выбора средств защиты сформулирована как задача дискретного программирования с линейным показателем качества, определяющим стоимость выбранных средств, и неявными ограничениями, суть которых заключается в проверке допустимости возможного решения с помощью экспериментов на реализации имитационной модели системы защиты информации. Предложенный метод является модификацией метода вектора спада, учитывает особенности задачи и требует максимум  $m+1$  шагов, где  $m$  – размерность неизвестного вектора булевых переменных, задающего множество выбранных средств. Приведено доказательство этого утверждения. Представлен результат решения задачи для заданных исходных данных.

**Ключевые слова:** оптимизационно-имитационный подход, средство защиты информации, дискретное программирование, метод вектора спада

---

### **Введение**

При проектировании систем защиты информации приходится решать задачи выбора в различных поставках, например, задачу выбора средств защиты информации (СЗИ) с целью обеспечения заданных требований по безопасности информации [1, 2]. Задачи выбора часто формулируются в оптимизационной постановке, когда необходимо оптимизировать значение некоторого показателя качества при заданных ограничениях (задачи математического программирования).

В качестве показателей качества при выборе СЗИ могут быть использованы следующие показатели: стоимость выбранных средств защиты; оценка риска через возможный ущерб при нарушении требований безопасности; оценка используемых вычислительных ресурсов защищаемой системы; показатели надежности системы защиты и др. В различных постановках задач некоторые показатели задают целевую функцию, а другие вводятся в ограничения. Проблема заключается в том, что только небольшое число

показателей могут быть записаны в виде явной аналитической модели. Например, с помощью линейной формы можно представить показатель, определяющий стоимость выбранных СЗИ:

$$C(\vec{X}) = \sum_{j \in M} c_j x_j \rightarrow \min_{\vec{X} \in \Delta^{\text{доп}}}, \quad (1)$$

где  $M$  – множество индексов СЗИ;  $c_j, j \in M$  – стоимость  $j$ -го средства защиты;  $x_j \in \{0, 1\}, \forall j \in M$  – булева переменная, равная 1, если  $j$ -ое СЗИ выбрано, 0 – в противном случае, переменные образуют вектор  $\vec{X}$ ;  $\Delta^{\text{доп}}$  – множество допустимых альтернатив.

В классических задачах математического программирования  $\Delta^{\text{доп}}$  задается системой равенств и (или) неравенств. В некоторых задачах выбора СЗИ множество  $\Delta^{\text{доп}}$  определяется ограничениями, например, на возможный ущерб или на выполнение заданных требований по обеспечению защищенности при использовании СЗИ, заданных виде неравенств [1, 2]. При этом некоторые параметры неравенств, такие как вероятности предотвращения угрозы средством защиты, задаются очень грубо и оценочно и предполагают наличие некоторой статистики, которой может и не быть. В [3] предложено нечеткое описание подобных параметров и представлена постановка задачи нечеткого математического программирования. В [4] подобные оптимизационные задачи рассмотрены в рамках игрового подхода (в моделях присутствует решение стороны противника). В любом случае для задания значений некоторых параметров, которые являются исходными данными для оптимизационных задач, используется субъективная и часто неполная информация.

Альтернативой в этих случаях является применение имитационного моделирования. Подобный подход, в котором при решении оптимизационных задач используется имитационное моделирование, получил название – оптимизационно-имитационный подход (ОИП). Одной из первых работ, в которой сформулирован термин ОИП, являлась [5]. В [5] предлагается в рамках ОИП рассматривать следующие задачи:

- целевая функция задана явно, ограничения проверяются на имитационной модели (ИМ);
- целевая функция задана имитационной моделью (значения показателя для решения можно получить, проведя эксперименты на ИМ), ограничения заданы явно (системой равенств или неравенств);
- целевая функция и ограничения задаются ИМ.

ОИП рассматривался во многих работах при проектировании систем различного целевого назначения [5-9]. Применительно к задачам защиты информации он применялся при выборе помехоустойчивых кодов [10]. За пределами России ОИП также использовался в различных предметных областях. В [11] рассмотрена задача планирования работы гидроэлектростанций (ГЭС). Задача ставилась как задача целочисленного нелинейного программирования, в которой переменными были выходная мощность и число включенных блоков в каждой ГЭС в каждый час работы времени. Цель

состояла в максимизации эффективности ГЭС при одновременном снижении затрат запуска / останова. Часть ограничений в модели проверялась на ИМ.

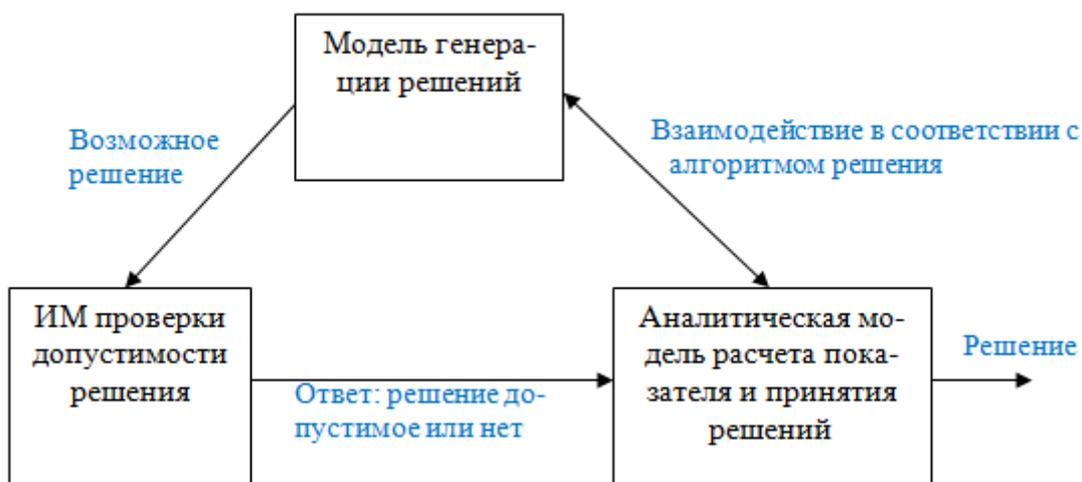
В [12] производится оптимизация работы холодильной установки, хотя и используется термин оптимизационно-имитационный подход, но имитация проводится на реальной установке для получения исходных данных для эвристической оптимизационной модели.

В [13] рассмотрены сравнительные достоинства и недостатки оптимизационных и имитационных методов и использование электронных таблиц в системах управления поставками. В [14] рассмотрено совместное применение инструментальных средств оптимизации и имитационного моделирования Matlab и Stateflow для проектирования стека протокола для беспроводных сенсорных сетей с целью оптимизации энергии, предложены разные модели (оптимизационные и имитационные) на различных сетевых уровнях протоколов – от физического до прикладного. В [15] рассмотрен комбинированный подход, основанный на генерации знаний в динамическом производственном планировании и проверке полученных решений на имитационных моделях. В [16] рассмотрены модели планирования работы систем поставок продукции клиентам на различных уровнях принятия решений от стратегического до тактического. Предложены разные модели на различных уровнях - “методология с четырьмя шагами” (сетевая оптимизация, сетевое моделирование, стратегическая оптимизация и проект для оценки устойчивости). Рассмотрено комбинирование оптимизационных и имитационных моделей на различных уровнях.

Рассмотрим пример использования оптимизационно-имитационного подхода к одной задаче, решаемой при проектировании систем защиты информации.

## **1. Постановка задачи и подходы к решению**

Остановимся на задаче выбора СЗИ, в которой целевая функция задана явно, а ограничения проверяются на ИМ, на примере задачи минимизации стоимости выбранных СЗИ с целевой функцией (1). На реализации ИМ для любого булевого вектора  $\vec{X}$  (возможного решения) проверяется его допустимость. Общая схема решения задачи на моделях, когда показатель задан явно, а ограничения проверяются на имитационной модели, представлена на рис. 1. Реализация имитационной модели должна в ходе имитационных экспериментов проверять допустимость возможного решения, поступающего на вход этой модели.



**Рис. 1.** Общая схема решения при задании ограничений имитационной моделью

Задача с показателем качества (1) является задачей булевого программирования с неявными ограничениями. Задача булевого программирования в общем случае считается *NP*-полной задачей, с учетом того, что проверка допустимости любого решения требует проведения имитационных экспериментов, которые могут иметь высокую вычислительную трудоемкость, применение точных методов является практически невозможным из-за высокой вычислительной трудоемкости задачи.

Для решения подобных задач могут быть использованы приближенные методы, например, метод вектора спада, основанный на метризации дискретного пространства и введении понятия окрестности точки в дискретном пространстве. Этот метод был использован в [17] для решения задачи выбора СЗИ в случае явного заданного нелинейного ограничения, определяющего максимально возможный ущерб от непредотвращенных угроз безопасности. В [18] доказана теорема о верхней оценке числа шагов алгоритма метода вектора спада для задач с линейным показателем качества и ограничениями любого вида. Метод обеспечивает получение локального оптимума за полиномиальное время. Тем не менее, напрямую для задач с неявными ограничениями с учетом возможной высокой вычислительной трудоемкости реализации имитационной модели этот метод применять не всегда удобно. Некоторые вопросы вычислительной сложности в системах защиты рассмотрены в [19-23].

## 2. Алгоритм метода

Рассмотрим для решения задачи с показателем качества (1) с неявными ограничениями, проверяемыми на ИМ, модифицированный метод вектора спада с радиусом окрестности 1 по метрике Хэмминга. Метод позволяет получать локальный минимум и учитывает специфику конкретной задачи. Метод требует максимум  $m+1$  шагов

(где  $m$  – размерность вектора  $\vec{X}$ ), на каждом из которых выполняются эксперименты с ИМ. Опишем разработанный алгоритм.

Компоненты вектора  $\vec{X}$  нумеруются в порядке невозрастания коэффициентов целевой функции  $c_j, j \in M$ .

**Шаг 0.** Задаем начальное значение вектора  $\vec{X}^{(0)} = \|1, 1, \dots, 1\|^m$ , состоящее из всех 1 (самое неоптимальное решение по показателю (1)), проверяем допустимость решения на ИМ, если оно недопустимо, алгоритм прекращает работу, допустимых решений не существует. Если решение допустимо, то запоминаем это решение как рекордное.

**Шаг  $i$ -ый ( $i=1, 2, \dots, m$ ).** Полагаем  $x_i = 0$ , получаем новое возможное решение  $\vec{X}^{(i)}$ , проверяем допустимость этого решения на ИМ, если решение допустимо, то его запоминаем как рекордное, если недопустимо, то возвращаем старое значение  $x_i = 1$ , переходим к следующему шагу.

После работы алгоритма локальным минимумом будет полученное рекордное решение.

Приведен доказательство того, что алгоритм дает локальный минимум за  $(m+1)$  шагов (если решение существует).

На множестве альтернатив (всех возможных векторов  $\vec{X}$ ) введем бинарное отношение доминирования (его можно назвать «доминирование по единицам»):  $d = \langle B_m, D \rangle$ , где  $B_m$  – множество всех двоичных векторов длины  $m$ ,  $D$  – график отношения. График отношения задается следующим множеством пар векторов:

$$D = \{(\vec{X}^{(i)}, \vec{X}^{(j)}) \mid \vec{X}^{(i)}, \vec{X}^{(j)} \in B_m, \forall k \in M, x_k^{(i)} \geq x_k^{(j)}, \exists l \in M, x_l^{(i)} > x_l^{(j)}\},$$

где  $x_k^{(i)}$  – обозначение  $k$ -ой компоненты вектора  $\vec{X}^{(i)}$ .

Таким образом, вектор  $\vec{X}^{(j)}$  можно получить из вектора  $\vec{X}^{(i)}$ , если в векторе  $\vec{X}^{(i)}$  некоторые единицы (хотя бы одну) заменить нулями. Содержательно это означает, что множество СЗИ, соответствующее вектору  $\vec{X}^{(j)}$ , можно получить исключением некоторых СЗИ из множества СЗИ, соответствующего вектору  $\vec{X}^{(i)}$ .

Очевидно, что  $C(\vec{X}^{(i)}) \geq C(\vec{X}^{(j)})$ .

Сформулируем одну лемму и 2 утверждения.

**Лемма.** Если  $\vec{X}^{(i)} D \vec{X}^{(j)}$  и вектор  $\vec{X}^{(i)}$ , задающий некоторое множество СЗИ, является недопустимым с точки зрения выполнения требований безопасности, то вектор  $\vec{X}^{(j)}$  также является недопустимым с точки зрения выполнения этих требований.

Содержательно это означает следующее: если некоторое множество СЗИ не обеспечивает выполнение заданных требований безопасности, то при исключении из этого множество отдельных средств (или средства), оставшиеся средства также не обеспечивают выполнение требований безопасности.

**Утверждение 1.** Для получения локального минимума в окрестности с радиусом 1 для некоторого допустимого вектора  $\vec{X}^{(i)}$  необходимо инвертировать элемент этого

вектора со значением, равным 1, и с максимальным коэффициентом целевой функции, полученный вектор при этом должен быть допустим.

Данное утверждение очевидно и не требует доказательства, содержательно это означает, что из множества СЗИ необходимо исключить средство с самой дорогой стоимостью, причем так, чтобы оставшиеся средства обеспечивали выполнение заданных требований по безопасности.

Для обеспечения этого условия все элементы вектора  $\vec{X}$  пронумерованы в порядке невозрастания коэффициентов целевой функции  $c_j, j \in M$ . В алгоритме последовательно, начиная с начала вектора, меняем значение очередной компоненты с 1 на 0 (исключаем очередное средство), проверяем допустимость полученного вектора, если вектор недопустим, то оставляем старое значение элемента вектора – единицу и переходим к следующему элементу вектора. Если полученное решение допустимое, то это есть локальный минимум окрестности (его считаем рекордом), переходим к следующему шагу.

**Утверждение 2.** Если была проверена  $i$ -ая компонента путем замены ее значения с 1 на 0 на  $i$ -м шаге алгоритма, при этом получили новый вектор  $\vec{X}$ . Если после замены полученный вектор допустим, то его назначаем рекордным решением, в противном случае остается старое рекордное решение. В любом случае рекордное решение на этом шаге обозначим –  $\vec{X}^{(i)}$ . Тогда на  $(i+1)$ -м шаге компоненты с индексами  $l=1, \dots, i$  (проверенные на предшествующих шагах) можно не рассматривать, а начинать инвертирование необходимо с компоненты с индексом  $i+1$ .

**Доказательство.** Будем пытаться инвертировать те компоненты с индексами  $l=1, \dots, i$ , которые равны единице, в допустимом векторе  $\vec{X}^{(i)}$  на  $(i+1)$ -м шаге. Пусть  $\vec{X}^{(\gamma)}$ ,  $\gamma \in \{1, 2, \dots, i\}$  вектор, который был получен инвертированием  $\gamma$ -ой компоненты из 1 в 0 на  $\gamma$ -м шаге, и этот вектор был недопустимым (иначе он был бы принят в качестве рекордного решения на  $\gamma$ -м шаге,  $\gamma$ -я компонента была бы равна 0).  $\vec{X}_{(\gamma)}^{(i+1)}$ , вектор, который был получен инвертированием той же  $\gamma$ -ой компоненты из 1 в 0 на  $(i+1)$ -м шаге. Тогда возможны следующие два случая:

- $\vec{X}^{(\gamma)} \not\subset \vec{X}_{(\gamma)}^{(i+1)}$ , так как на каждом из шагов алгоритма  $l=\gamma+1, \dots, i$  могло быть выполнено только одно возможное действие – компонента вектора со значением 1 превращена в компоненту со значением 0, но вектор  $\vec{X}^{(\gamma)}$  недопустим, тогда в соответствии с леммой вектор  $\vec{X}_{(\gamma)}^{(i+1)}$  тоже недопустим;

- вектора  $\vec{X}^{(\gamma)}$ ,  $\vec{X}_{(\gamma)}^{(i+1)}$  равны между собой, т.е. на каждом из шагов алгоритма  $l = \gamma + 1, \dots, i$  превращение компоненты из 1 в 0 давало недопустимый вектор, в этом случае  $\vec{X}_{(\gamma)}^{(i+1)}$  тоже недопустим.

Таким образом, не имеет смысла инвертировать из 1 в 0 уже проверенные компоненты вектора на предыдущих шагах.

### 3. Пример решения задачи

Учитывая то обстоятельство, что разработка имитационной модели, которая проверяет допустимость полученного решения, и реализация этой модели являются задачами отдельного исследования и выходит за рамки данной статьи, в качестве некоторого «имитатора» имитационной модели будем использовать ограничение на возможный ущерб. Ущерб будем считать в соответствии с подходами, представленными в [1, 4]. Описания подходов к построению имитационных моделей некоторых систем защиты приведены в [24-28].

Для оценки допустимости решения будем использовать следующее ограничение на предотвращенный ущерб:

$$U(\vec{X}) = 100 \frac{\sum_{i \in N} (u_i - u_i \max_{j \in M} \{p_{ij} x_j\})}{\sum_{i \in N} u_i} \leq U_{max}, \quad (2)$$

где  $U(\vec{X})$  – средний ущерб от угроз безопасности, выраженный в процентах от максимально возможного ущерба при отсутствии СЗИ (знаменатель дроби);  $u_i, \forall i \in N$  – средний ущерб от непредотвращенной  $i$ -ой угрозы за заданный период времени;  $N$  – множество индексов угроз безопасности;  $p_{ij} \in [0, 1], \forall i \in N, \forall j \in M$  – возможность, описываемая в рамках теории нечетких множеств, или вероятность (если есть статистика) предотвращения последствий  $i$ -ой угрозы с помощью  $j$ -го средства защиты;  $U_{max}$  – максимальное значение ущерба, выраженное в процентах от возможного ущерба без использования СЗИ.

Допустимость возможного решения (вектора  $\vec{X}$ ) будем проверять простой его подстановкой в ограничение (2). За основу примем исходные данные, представленные в [4].

В табл. 1 представлены некоторые угрозы для автоматизированной системы, возможный ущерб от этих угроз за заданный период (1 год) и стоимости проведения этих атак для нарушителя за тот же период. Данные об ущербе сильно зависят от специфики деятельности компании, в которой используется информационная система, и заданы приблизительно.

**Таблица 1.** Ущерб от непредотвращенных атак

№ п/п	Название угрозы	Ущерб от не предотвращения ( $u_i, \forall i \in N$ ), руб.
1.	Утечка конфиденциальной информации из сети по каналам связи (e-mail, web, chat/IM и т.п.)	10 000 000
2.	Прослушивание внешних каналов связи злоумышленниками	10 000 000
3.	Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим вне контролируемой зоны, осуществляемое внешними нарушителями путем пассивного прослушивания каналов связи	10 000 000
4.	Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика	1 000 000
5.	Замена, вставка, удаление или изменение данных пользователей в информационном потоке	5 000 000
6.	Перехват информации, например, пользовательских паролей, передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации	5 000 000
7.	Статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т.п.)	1 000 000
8.	Внедрение несанкционированного, непроверенного или вредоносного программного кода (вирусов, троянских программ и т.п.).	1 000 000
9.	Анализ и модификация программного обеспечения	15 000 000
10.	Логические бомбы, пересылаемые по e-mail	1 000 000
11.	Атаки на отказ в обслуживании против внешних хостов компании.	1 000 000

В табл. 2 представлены некоторые средства защиты от угроз безопасности. Данные о стоимости лицензий можно взять на сайтах многих организаций, занимающихся защитой информации. Угрозы в табл. 2 заданы своими номерами в соответствии с табл. 1. В таблице не приведены названия конкретных производителей средств защиты из-за антирекламных соображений. Представленные примерные цены задают конфигурацию средств защиты для информационной системы на основе локальной вычислительной сети с одним сервером и двадцатью рабочими местами.

**Таблица 2.** Средства защиты от угроз безопасности, стоимости их реализации и возможности предотвращения угроз на интервале времени 1 год

№	Средства защиты	Стоимости реализации ( $c_j, \forall j \in M$ ), руб	Возможности (вероятности) предотвращения угрозы ( $p_{ij}, \forall i \in N, \forall j \in M$ )										
			Номера угроз по табл. 1										
			1	2	3	4	5	6	7	8	9	10	11
1	Простой антивирус	30 000	0,00	0,00	0,00	0,00	0,60	0,60	0,00	0,90	0,98	0,98	0,00
2	Программа, предназначенная для шифрования и дешифрования данных, электронной подписи файлов	60 000	0,90	0,90	0,90	0,00	0,90	0,90	0,00	0,00	0,00	0,00	0,00
3	Средство для защиты от сетевых вторжений, вредоносных программ и спама	40 000	0,50	0,60	0,00	0,70	0,60	0,60	0,80	0,70	0,60	0,80	0,00
4	Средство обнаружения вторжений и несанкционированного доступа к информации	20 000	0,50	0,00	0,00	0,60	0,50	0,40	0,80	0,10	0,00	0,00	0,40
5	Средство, включающее межсетевой экран, антивирус и средства обнаружения вторжений	50 000	0,60	0,00	0,00	0,70	0,50	0,50	0,70	0,70	0,70	0,70	0,60
6	Комплекс шифрования	600 000	0,99	0,99	0,99	0,00	0,90	0,90	0,80	0,00	0,00	0,00	0,00
7	Средство защиты информации от несанкционированного доступа	35 200	0,00	0,00	0,00	0,00	0,50	0,60	0,00	0,80	0,80	0,00	0,00
8	Электронный замок	200 000	0,00	0,00	0,00	0,00	0,60	0,50	0,00	0,90	0,90	0,00	0,00
9	Средство защиты данных при взломе или краже дисков, а также при утере ноутбука или флеш-накопителя	28 000	0,90	0,00	0,00	0,00	0,00	0,80	0,00	0,00	0,00	0,00	0,00
10	Средство защиты от DDoS	60 000	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,90

Реализация алгоритма выбора СЗИ на основе метода вектора спада выполнена на языке Java, так как в этом случае имитатор ИМ может быть заменен на конкретную реализацию ИМ с использованием специальной библиотеки классов языка Java для имитационного моделирования [29]. Интегрирование реализации ИМ на специальном языке моделирования, например, GPSS с алгоритмом, реализованном на языке программирования общего назначения, было бы затруднительно. Кроме того,

использование библиотеки классов языка Java позволяет реализовать подобные программы в виде интернет - приложений [30-32].

Результаты работы всех 11 шагов алгоритма (так как размерность вектора  $\vec{X}$  равна 10) при задании ограничений на максимальный ущерб в 10 % от возможного ущерба без использования СЗИ представлены в табл. 3.

Таблица 3. Результаты работы алгоритма модернизированного метода вектора спада

№ решения	Стоимость решения (СЗИ)	Средний ущерб	Средний возможный ущерб в % от ущерба без СЗИ	Допустимость решения	Значения компонент вектора $\vec{X}$										
					1	1	1	1	1	1	1	1	1	1	1
1.	1123200	2320000	3,87	+	1	1	1	1	1	1	1	1	1	1	1
2.	523200	5020000	8,37	+	1	1	1	1	1	0	1	1	1	1	1
3.	323200	5020000	8,37	+	1	1	1	1	1	0	1	0	1	1	1
4.	263200	19020000	31,70	-	1	0	1	1	1	0	1	0	1	1	1
5.	263200	5320000	8,87	+	1	1	1	1	1	0	1	0	1	0	0
6.	213200	5520000	9,20	+	1	1	1	1	0	0	1	0	1	0	0
7.	173200	5620000	9,37	+	1	1	0	1	0	0	1	0	1	0	0
8.	138000	5620000	9,37	+	1	1	0	1	0	0	0	0	1	0	0
9.	108000	22100000	36,83	-	0	1	0	1	0	0	0	0	1	0	0
10.	110000	5620000	9,37	+	1	1	0	1	0	0	0	0	0	0	0
11.	90000	7420000	12,37	-	1	1	0	0	0	0	0	0	0	0	0

Допустимое решение оптимальное по цене используемых СЗИ получено на 10 шаге, общая стоимость выбранных СЗИ составила 110 000 руб. Оптимальное значение вектора –  $\vec{X} = \|1, 1, 0, 1, 0, 0, 0, 0, 0, 0\|^T$ . Это означает, что для защиты системы были выбраны средства с номерами 1, 2, 4 из табл. 2.

### Заключение

В статье предложена и протестирована модификация метода вектора спада, которая требует  $m+1$  шагов, где  $m$  – число неизвестных переменных булевого вектора. Модификация применима для задач выбора СЗИ в рамках оптимизационно-имитационного подхода, когда на каждом шаге для проверки допустимости возможного решения требуется проводить имитационное моделирование.

### Список литературы

1. Овчинников А.И., Журавлев А.М., Медведев Н.В., Быков А.Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2007. № 3. С. 115- 121.

2. Быков А.Ю., Панфилов Ф.А., Шмырев Д.В. Задача выбора средств защиты в автоматизированных системах с учетом классов защищенности от несанкционированного доступа к информации // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. Режим доступа: <http://engjournal.ru/catalog/it/hidden/85.html> (дата обращения 10.01.2015).
3. Быков А.Ю., Гуров А.В. Задача выбора средств защиты информации от атак в автоматизированных системах при нечетких параметрах функции цели // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. Режим доступа: <http://engjournal.ru/catalog/it/hidden/86.html> (дата обращения 10.01.2015).
4. Быков А.Ю., Алтухов Н.О., Сосенко А.С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. Режим доступа: <http://engbul.bmstu.ru/doc/708106.html> (дата обращения 10.01.2015).
5. Цвиркун А.Н., Акинфиев В.К., Филиппов В.А. Имитационное моделирование в задачах синтеза структуры сложных систем. Оптимизационный-имитационный подход. М.: Наука, 1985. 173 с.
6. Акинфиев В.К., Цвиркун А.Д. Управление развитием крупномасштабных систем: Оптимизационно-имитационный подход // Известия Волгоградского государственного технического университета. 2013. Т. 18, № 22 (125). С. 12-20.
7. Крылова О.В., Степин Ю.П. Модель системной динамики для оптимизационно-имитационного подхода к выбору схем доставки ресурсов // Управление качеством в нефтегазовом комплексе. 2012. Т. 3. С. 13-16.
8. Белецкая С.Ю. Принятие решений в информационно-управляющей системе предприятия на основе оптимизационно-имитационного подхода// Информация и безопасность. 2004. № 2. С. 59-62.
9. Ковалев И.В., Царев Р.Ю., Тюпкин М.В., Цветков Ю.Д. Оптимизационно-имитационный подход к синтезу автоматизированных систем управления // Программные продукты и системы. 2007. № 3. С. 31.
10. Антонова Г.М. Применение ЛПт - оптимизации в рамках оптимизационно-имитационного подхода при выборе помехоустойчивых корректирующих кодов // Автоматика и телемеханика. 1999. № 9. С.162-168.
11. Kadowaki M., Ohishi T., Martins L.S.A., Soares S. Short-term hydropower scheduling via an optimization-simulation decomposition approach // 2009 IEEE Bucharest Power Tech Conference. June 28th - July 2nd. Bucharest, Romania. IEEE Publ., 2009. P. 1-7. DOI: [10.1109/PTC.2009.5282116](https://doi.org/10.1109/PTC.2009.5282116) .
12. Vakiloroaya V., Samali B., Madadnia J., Ha Q.P. Component-wise optimization for a commercial central cooling plant // IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society. IEEE Publ., 2011. P. 2769-2774. DOI: [10.1109/IECON.2011.6119750](https://doi.org/10.1109/IECON.2011.6119750) .

13. Chwif L., Barretto M.R.P., Saliby E. Supply chain analysis: spreadsheet or simulation? // Proceedings of the Winter Simulation Conference, 2002. Vol. 1. IEEE Publ., 2002. P. 59-66. DOI: [10.1109/WSC.2002.1172869](https://doi.org/10.1109/WSC.2002.1172869) .
14. Anwar A.-K., Lavagno L. MEOW: Model-based design of an energy-optimized protocol stack for wireless sensor networks // 2010 IEEE 35th Conference on Local Computer Networks (LCN). IEEE Publ., 2010. P. 590-597. DOI: [10.1109/LCN.2010.5735778](https://doi.org/10.1109/LCN.2010.5735778) .
15. Aufenanger M., Dangelmaier W., Laroque C., Rungener N. Knowledge-based event control for flow-shops using simulation and rules // Winter Simulation Conference, 2008. IEEE Publ., 2008. P. 1952-1958. DOI: [10.1109/WSC.2008.4736288](https://doi.org/10.1109/WSC.2008.4736288) .
16. Hicks D.A. A four step methodology for using simulation and optimization technologies in strategic supply chain planning // 1999 Winter Simulation Conference Proceedings. Vol. 2. IEEE Publ., 1999. P. 1215-1220. DOI: [10.1109/WSC.1999.816843](https://doi.org/10.1109/WSC.1999.816843) .
17. Овчинников А.И., Медведев Н.В., Быков А.Ю. Применение метода вектора спада для решения задачи поиска вариантов защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2008. № 2. С. 73- 82.
18. Сергиенко И.В., Лебедева Т.Т., Рощин В.А. Приближенные методы решения дискретных задач оптимизации. Киев: Наукова думка, 1980. 276 с.
19. Ключарев П.Г. О вычислительной сложности некоторых задач на обобщенных клеточных автоматах // Безопасность информационных технологий. 2012. № 1. С. 30-32.
20. Ключарев П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. Режим доступа: <http://technomag.bmstu.ru/doc/312834.html> (дата обращения 10.01.2015).
21. Ключарев П.Г. О периоде обобщенных клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 2. Режим доступа: <http://technomag.bmstu.ru/doc/340943.html> (дата обращения 10.01.2015).
22. Ключарёв П.Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 10. С. 299-314. DOI: [1013.0624722](https://doi.org/10.1013.0624722)
23. Ключарёв П.Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. С. 214-223. DOI: [10.7463/0114.0675812](https://doi.org/10.7463/0114.0675812)
24. Котенко И.В., Коновалов А.М., Шоров А.В. Имитационное моделирование механизмов защиты от бот-сетей // Труды СПИИРАН. 2011. Вып. 4 (19). С. 7-33.

25. Маслов О.Н. Применение метода статистического имитационного моделирования для исследования случайных антенн и проектирования систем активной защиты информации // Успехи современной радиоэлектроники. Зарубежная радиоэлектроника. 2011. № 6. С. 42-55.
26. Цимбал В.А., Ковалев М.С. Моделирование многоэшелонированных систем защиты информации // Информационные технологии в проектировании и производстве. 2010. № 4. С. 42-48.
27. Бугров Ю.Г., Мирошников В.В., Кочергин Д.В. Повышение качества имитационной модели системы защиты информации // Информация и безопасность. 2008. Т. 11, № 1. С. 69-73.
28. Григорьев В.А., Карпов А.В. Имитационная модель системы защиты информации // Программные продукты и системы. 2005. № 2. С. 6.
29. Быков А.Ю., Панфилов Ф.А., Сумарокова О.О. Имитационное моделирование с применением библиотеки классов языка Java, разработанной для «облачных» сервисов // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 2. Режим доступа: <http://engjournal.ru/catalog/it/hidden/535.html> (дата обращения 10.01.2015).
30. Быков А.Ю., Кожемякина Е.В., Панфилов Ф.А. Имитационное моделирование систем массового обслуживания в клиентских приложениях при использовании технологии "облачных" вычислений // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 11. Режим доступа: <http://engjournal.ru/catalog/it/network/1001.html> (дата обращения 10.01.2015).
31. Быков А.Ю., Медведев Н.В., Панфилов Ф.А. Тестирование клиента и сервера для выбора объекта проведения экспериментов в инструментальном программном средстве имитационного моделирования на основе технологии "облачных" вычислений // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 11. Режим доступа: <http://engjournal.ru/catalog/it/network/989.html> (дата обращения 10.01.2015).
32. Быков А.Ю. Задача распределения заданий между клиентом и сервером в имитационном моделировании на основе технологии облачных вычислений и результаты экспериментов по ее решению // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. Режим доступа: <http://engbul.bmstu.ru/doc/697425.html> (дата обращения 10.01.2015).

## **A Modified Recession Vector Method Based on the Optimization-Simulation Approach to Design Problems of Information Security Systems**

A.Yu. Bykov<sup>1,\*</sup>, A.Yu. Artamonova<sup>1</sup>

\*[abykov@bmstu.ru](mailto:abykov@bmstu.ru)

<sup>1</sup>Bauman Moscow State Technical University, Moscow, Russia

---

**Keywords:** optimization-simulation approach, mean of information protection, discrete optimization, recession vector method

---

Modern practical task-solving techniques for designing information security systems in different purpose automated systems assume the solution of optimization tasks when choosing different elements of a security system. Formulations of mathematical programming tasks are rather often used, but in practical tasks it is not always analytically possible to set target function and (or) restrictions in an explicit form. Sometimes, calculation of the target function value or checking of restrictions for the possible decision can be reduced to carrying out experiments on a simulation model of system. Similar tasks are considered within optimization-simulation approach and require the ad hoc methods of optimization considering the possible high computational effort of simulation.

The article offers a modified recession vector method, which is used in tasks of discrete optimization to solve the similar problems. The method is applied when the task to be solved is to minimize the cost of selected information security tools in case of restriction on the maximum possible damage. The cost index is the linear function of the Boolean variables, which specify the selected security tools, with the restriction set as an "example simulator". Restrictions can be actually set implicitly. A validity of the possible solution is checked using a simulation model of the system.

The offered algorithm of a method considers features of an objective. The main advantage of algorithm is that it requires a maximum of  $m+1$  of steps where  $m$  is a dimensionality of the required vector of Boolean variables. The algorithm provides finding a local minimum by using the Hamming metrics in the discrete space; the radius of neighborhood is equal to 1. These statements are proved.

The paper presents solution results of choosing security tools with the specified basic data.

## References

1. Ovchinnikov A.I., Zhuravlev A.M., Medvedev N.V., Bykov A.Ju. Mathematical model of optimal selection of aids of protection against threats for safety of enterprise computer network. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie = Herald of the Bauman Moscow State Technical University. Ser. Instrument Engineering*, 2007, no. 3, pp. 115- 121. (in Russian).
2. Bykov A.Ju., Panfilov F.A., Shmyrev D.V. A Problem on Choosing Protection in Automated Systems Taking into Account the Classes of Immunity against Unauthorized Data Access. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2012, no. 1. Available at: <http://engjournal.ru/catalog/it/hidden/85.html>, accessed 10.01.2015. (in Russian).
3. Bykov A.Ju., Gurov A.V. A Problem on Choosing Protection against Attacks in Automated Systems with Fuzzy Parameters of Goal Function. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2012, no. 1. Available at: <http://engjournal.ru/catalog/it/hidden/86.html>, accessed 10.01.2015. (in Russian).
4. Bykov A.Ju., Altuhov N.O., Sosenko A.S. The problem of choosing software / hardware means in automated information systems based on the model of an antagonistic game. *Inzhenernyi vestnik MGTU im. N.E. Baumana = Engineering Herald of the Bauman MSTU*, 2014, no. 4. Available at: <http://engbul.bmstu.ru/doc/708106.html>, accessed 10.01.2015. (in Russian).
5. Cvirkun A.N., Akinfiev V.K., Filippov V.A. *Imitacionnoe modelirovanie v zadachah sinteza struktury slozhnyh sistem. Optimizacionnyj-imitacionnyj podhod* [Simulation modeling in problems of synthesis of the structure of complex systems. Optimization-simulation approach]. Moscow, Nauka Publ., 1985. 173 p. (in Russian).
6. Akinfiev V.K., Cvirkun A.D. Management development of large-scale systems: optimization-simulation approach. *Izvestija Volgogradskogo gosudarstvennogo tehničeskogo universiteta* [Proceedings of the Volgograd State Technical University], 2013, vol. 18, no. 22 (125), pp. 12-20. (in Russian).
7. Krylova O.V., Stepin Ju.P. System dynamics model for optimization-simulation approach to the choice of delivery resources. *Upravlenie kachestvom v neftegazovom komplekse* [Quality management in the oil and gas industry], 2012, vol. 3, pp. 13-16. (in Russian).
8. Beleckaja S.Ju. Decision making in the information-control system of the enterprise on the basis of optimization-simulation approach. *Informacija i bezopasnost'* [Information and Security], 2004, no. 2, pp. 59-62. (in Russian).
9. Kovalev I.V., Carev R.Ju., Tjupkin M.V., Cvetkov Ju.D. Optimization-simulation approach to the synthesis of automatic control systems. *Programmnye produkty i sistemy = Software & Systems*, 2007, no. 3. p. 31. (in Russian).

10. Antonova G.M. Choice of noise-immune correcting codes by the LP $\tau$ -optimization within the framework of the optimization-simulation approach. *Avtomatika i telemekhanika*, 1999, no. 9. pp. 162-168. (English translation: *Automation and Remote Control*, 1999, vol. 60, no. 9, pp. 1374-1352).
11. Kadowaki M., Ohishi T., Martins L.S.A., Soares S. Short-term hydropower scheduling via an optimization-simulation decomposition approach. *2009 IEEE Bucharest Power Tech Conference*, June 28th - July 2nd, Bucharest, Romania. IEEE Publ., 2009, pp. 1-7. DOI: [10.1109/PTC.2009.5282116](https://doi.org/10.1109/PTC.2009.5282116).
12. Vakiloroyaya V., Samali B., Madadnia J., Ha Q.P. Component-wise optimization for a commercial central cooling plant. *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*. IEEE Publ., 2011, pp. 2769-2774. DOI: [10.1109/IECON.2011.6119750](https://doi.org/10.1109/IECON.2011.6119750).
13. Chwif L., Barretto M.R.P., Saliby E. Supply chain analysis: spreadsheet or simulation? *Proceedings of the Winter Simulation Conference, 2002. Vol. 1*. IEEE Publ., 2002, pp. 59-66. DOI: [10.1109/WSC.2002.1172869](https://doi.org/10.1109/WSC.2002.1172869).
14. Anwar A.-K., Lavagno L. MEOW: Model-based design of an energy-optimized protocol stack for wireless sensor networks. *2010 IEEE 35th Conference on Local Computer Networks (LCN)*. IEEE Publ., 2010, pp. 590-597. DOI: [10.1109/LCN.2010.5735778](https://doi.org/10.1109/LCN.2010.5735778).
15. Aufenanger M., Dangelmaier W., Laroque C., Rungener N. Knowledge-based event control for flow-shops using simulation and rules. *Winter Simulation Conference, 2008*. IEEE Publ., 2008, pp. 1952-1958. DOI: [10.1109/WSC.2008.4736288](https://doi.org/10.1109/WSC.2008.4736288).
16. Hicks D.A. A four step methodology for using simulation and optimization technologies in strategic supply chain planning. *1999 Winter Simulation Conference Proceedings. Vol. 2*. IEEE Publ., 1999, pp. 1215-1220. DOI: [10.1109/WSC.1999.816843](https://doi.org/10.1109/WSC.1999.816843).
17. Ovchinnikov A.I., Medvedev N.V., Bykov A.Ju. Application of recession vector method to solving problem on search of variants of protection against security threats of enterprise computer network. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie = Herald of the Bauman Moscow State Technical University. Ser. Instrument Engineering*, 2008, no. 2, pp. 73-82. (in Russian).
18. Sergienko I.V., Lebedeva T.T., Roshhin V.A. *Priblizhennyye metody resheniya diskretnykh zadach optimizacii* [Approximate methods for solving discrete optimization problems]. Kiev, Naukova dumka Publ., 1980. 276 p. (in Russian).
19. Klyucharev P.G. Computational Complexity of Some Problems on Generalized Cellular Automations. *Bezopasnost' informacionnyh tehnologij*, 2012, no. 1, pp. 30-32. (in Russian).
20. Klyucharev P.G. NP-hard of step backward problem in generalized cellular automaton. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 2. Available at: <http://technomag.bmstu.ru/doc/312834.html>, accessed 10.01.2015.

21. Klyucharev P.G. On period of generalized cellular automation. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 2. Available at: <http://technomag.edu.ru/doc/340943.html>, accessed 10.01.2015. (in Russian).
22. Klyucharev P.G. Performance and effectiveness of hardware realization of stream ciphers based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2013, no. 10. DOI: [1013.0624722](https://doi.org/10.13063/1013.0624722) (in Russian).
23. Klyucharev P.G. The FPGA realization of the general cellular automata based cryptographic hash functions: Performance and effectiveness. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2014, no. 1. DOI: [10.7463/0114.0675812](https://doi.org/10.7463/0114.0675812) (in Russian).
24. Kotenko I.V., Konovalov A.M., Shorov A.V. [Simulation of protection mechanisms against botnets. *Trudy SPIIRAN = SPIIRAS Proceedings*, 2011, iss. 4 (19). pp. 7-33. (in Russian).
25. Maslov O.N. Statistic Imitation Modeling Method for Random Antennas Investigation and Active Information Security Systems Projecting Application. *Uspehi sovremennoj radioelektroniki = Achievements of Modern Radioelectronics*, 2011, no. 6. pp. 42-55. (in Russian).
26. Cimbal V.A., Kovalev M.S. Modelling of multilevel systems of protection of the information. *Informacionnye tehnologii v proektirovanii i proizvodstve = Information technology of CAD/CAM/CAE*, 2010, no. 4. pp. 42-48. (in Russian).
27. Bugrov Ju.G., Miroshnikov V.V., Kochergin D.V. Improving the quality of the simulation model of information security systems. *Informacija i bezopasnost' [Information and Security]*, 2008, vol. 11, no. 1. pp. 69-73. (in Russian).
28. Grigor'ev V.A., Karpov A.V. Imitacionnaja model' sistemy zashhity informacii. *Programmnye produkty i sistemy = Software & Systems*, 2005, no. 2. p. 6. (in Russian).
29. Bykov A.Ju., Panfilov F.A., Sumarokova O.O. Simulation with usage of the Java class library, developed for “cloud” services. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2013, no. 2. Available at: <http://engjournal.ru/catalog/it/hidden/535.html>, accessed 10.01.2015. (in Russian).
30. Bykov A.Ju., Kozhemjakina E.V., Panfilov F.A. Simulation of queuing systems in client applications using cloud computing technology. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2013, no. 11. Available at: <http://engjournal.ru/catalog/it/network/1001.html>, accessed 10.01.2015. (in Russian).
31. Bykov A.Ju., Medvedev N.V., Panfilov F.A. Testing of the client and the server for a choosing of an object for experiments in instrumental software for simulation based on “cloud” computing. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2013, no. 11. Available at: <http://engjournal.ru/catalog/it/network/989.html>, accessed 10.01.2015. (in Russian).

32. Bykov A.Ju. The problem of distribution of jobs between the client and server in the simulation based on cloud computing technology and results of experiments on its solution. *Inzhenernyi vestnik MGTU im. N.E. Baumana = Engineering Herald of the Bauman MSTU*, 2014, no. 1. Available at: <http://engbul.bmstu.ru/doc/697425.html>, accessed 10.01.2015. (in Russian).