ОБ АНАЛОГИИ ЗАДАЧ ОПТИМИЗАЦИИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С НЕКОТОРЫМИ ЗАДАЧАМИ ТЕОРИИ СВЯЗИ

Грибунин В.Г.[1], Тимонов А.А.[2]

Цель статьи: *оптимизация выбора средств защиты информации в многоуровневой автоматизированной системе с учетом вышестоящих уровней, показателей качества средств защиты информации, а также общего финансового бюджета. Демонстрация аналогий решения этих задач с известными задачами из теории связи.*

Метод исследования: *оптимальный выбор средств защиты информации на основе анализа рисков и метода множителей Лагранжа. Оптимальное распределение бюджета бит на основе оптимизационного алгоритма Waterfilling. Оптимальное размещение средств защиты информации в многоуровневой автоматизированной системе на основе бисекционного поиска.*

Полученный результат: *в статье показаны аналогии между отдельными задачами теории связи и оптимальным выбором средств защиты информации. Известная задача оптимального выбора средств защиты информации решена с использованием теории искажение-скорость, известная задача оптимального распределения бюджета на их закупку решена по аналогии с задачей распределения мощности передатчиков. Впервые поставленная задача оптимального размещения средств защиты информации в многоуровневой автоматизированной системе решена по аналогии с задачей распределения общего бюджета бит между квантователями.*

Ключевые слова: *задача выбора, функция искажение-скорость, оптимизация, теория связи, множитель Лагранжа, усечение дерева.*

DOI:10.21681/2311-3456-2021-5-30-35

Введение. Подходы к оптимальному выбору средств защиты информации

Общим подходом при проектировании системы защиты информации (СЗИ) информационной системы (ИС) является реализация следующей методики [1,2]:

1. идентификация требуемых защиты активов, включающее в себя оценку потерь при нарушении их конфиденциальности, целостности, доступности;
2. моделирование угроз безопасности информации по отношению к этим активам, включающее в себя идентификацию угроз, оценку их опасности (вероятности атаки);
3. выбор механизмов защиты, парирующих идентифицированные угрозы;
4. выбор по тем или иным критериям средств защиты информации (СрЗИ), реализующих отобранные механизмы;
5. если все идентифицированные угрозы парированы СрЗИ, а планируемый на закупки бюджет не превосходит выделенного, то проектирование заканчивается. В противном случае можно пересмотреть критерии выбора СрЗИ (например, поставив во главу угла их стоимость), либо переоценить риски. В некоторых случаях «безопаснику» удается обосновать увеличение бюджета на создание СЗИ.

Таким образом при построении СЗИ обычно для каждой идентифицированной угрозы для каждого актива выбирается механизм защиты и, далее, — средство защиты информации.

При этом одной из содержательных постановок задач создания СЗИ является оптимальный в каком-либо смысле выбор СрЗИ. Этот выбор осуществляется с учетом модели нарушителя и создаваемых им угроз. Известны теоретико-игровые постановки этой задачи [4], при которых рассматриваются одношаговые игры с нулевой суммой с участием защитника и атакующего, а оптимальный выбор СрЗИ соответствует равновесию по Нэшу. В других работах оптимальный выбор СрЗИ формулируется как задача об укладке рюкзака: например, располагая некоторым общим бюджетом, необходимо выбрать СрЗИ, доставляющие наибольший эффект от их применения. Рассмотрим последнюю задачу и проведем ее аналогию с задачей из теории связи.

Оптимальный выбор средств защиты информации и теория искажение-скорость

Пусть с каждым из СрЗИ ассоциированы две величины: стоимость R и остаточный риск, который остается после их использования – D. Будем считать, что эти величины аддитивны и независимы среди всех СрЗИ.

Стоимость СрЗИ складывается из прямых затрат на их закупку, а также косвенных затрат, связанных с под-

1 Грибунин Вадим Геннадьевич, доктор технических наук, главный научный сотрудник МОУ «ИИФ», г. Москва, Россия. E-mail: wavelet2@mail.ru

2 Тимонов Андрей Александрович, сотрудник ГЦ Минобороны России, г. Москва, Россия. E-mail: a.timonov@mil.ru

держанием их функционирования на протяжении жизненного цикла. Сюда же можно отнести и вычислительные затраты программных СрЗИ.

Остаточный риск связан с тем, что СрЗИ не могут отражать угрозы с вероятностью, равной 1. Например, если исходная вероятность атаки на актив была p_a = 0.1, а вероятность парирования угрозы СрЗИ p_c = 0.95, то остаточный риск будет пропорционален величине (1 – 0.95)*0.1 = 0.005.

Вероятность парирования угрозы СрЗИ связана с такими факторами как уровень сертификации СрЗИ, уровень поддержки со стороны вендора, независимые оценки эффективности (в случае их наличия) и т.д. [5,6]

Необходимо отметить, что остаточный риск зависит не только от свойств СрЗИ, но и от величины ущерба для конкретного актива.

Со всей СЗИ в целом связаны, соответственно, R_Σ и D_Σ.

В общем случае при построении СЗИ могут решаться две оптимизационные задачи [7]:

$$\min_{\{K\}} D_\Sigma,\ R_\Sigma \le R_\Sigma^* \qquad (1)$$

и

$$\min_{\{K\}} R_\Sigma,\ D_\Sigma \le D_\Sigma^*, \qquad (2)$$

где $\{K\}$ – множество параметров, по которым можно выполнять оптимизацию (например, выбор модели СрЗИ, его конфигурации и места установки).

Проведем аналогию выражений (1) и (2) с теорией искажение-скорость, описывающей сжатие сигналов с потерями (обозначения *R* и *D* введены в настоящей статье не случайно) [8,9]. Эта теория описывает зависимость достигаемого при сжатии искажения *D* как функции от скорости *R* (понимаемой как ресурс выделенных на кодирование бит). При этом также возможны две задачи минимизации, представленные в выражениях (1) и (2).

В работе [10] показано, как от задачи условной оптимизации можно перейти к более просто решаемой задаче безусловной оптимизации. Авторы данной работы решали задачу распределения общего бюджета бит между квантователями, сжимающими с потерями различные блоки речевого сообщения. Каждый *i*-й квантователь характеризовался своей характеристикой $D_i(R_i)$. Задача заключалась в том, чтобы распределить общий бюджет R_Σ^* так, чтобы минимизировать общее искажение (выражение 1).

Задача (1) является задачей условной оптимизации. Авторами [10] была доказана теорема о том, что в предположении о гладкости и выпуклости (или вогнутости) функции $D = f(R)$ задача условной оптимизации (1) эквивалентна следующей задаче безусловной оптимизации для частного случая $R_\Sigma = R_\Sigma^*$:

$$\min_{\{K\}} J_\Sigma = \min_{\{K\}} \left(D_\Sigma + \lambda R_\Sigma\right) \qquad (3)$$

где J_Σ — функция Лагранжа, которая включает в себя скорость и искажение путем введения множителя Лагранжа $\lambda \ge 0$, который показывает взаимообмен между скоростью и искажением ($\lambda = 0$ соответствует случаю, когда скорость не учитывается, а при $\lambda = \infty$ не учитывается искажение). Известно, что λ имеет геометрический смысл: это наклон касательной к кривой скорость-искажение (рис.1).

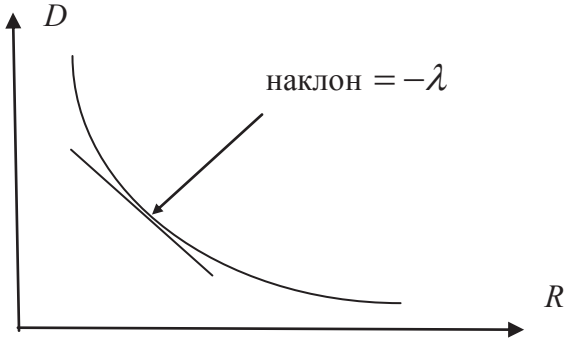

Рис.1. Кривая скорость-искажение (стоимость-остаточный риск для СрЗИ)

Можно предположить, что зависимость остаточного риска при использовании СрЗИ от его стоимости также является убывающей вогнутой функцией, как это показано на рис.1. Тогда множитель Лагранжа $\lambda \ge 0$ в (3) показывает взаимообмен между стоимостью и остаточным риском ($\lambda = 0$ соответствует случаю, когда стоимость СрЗИ не учитывается, а $\lambda = \infty$ — не учитывается остаточный риск). Известно, что λ имеет геометрический смысл: это наклон касательной к кривой стоимость-остаточный риск (рис.1).

Функция *J* определяет минимально достижимый остаточный риск для заданной стоимости или минимально достижимую стоимость для заданного остаточного риска. Отметим, что выбор каждого сочетания стоимости/риска определяет одну точку на кривой. Эти точки соответствуют разным СрЗИ или одному и тому же СрЗИ, примененному для защиты разных активов (стоимость в последнем случае будет одинаковой, а остаточный риск — разным).

Как показано на рис.1, в результате решения задачи (3) находятся точки, расположенные на выпуклой кривой функции стоимость-остаточный риск, которая получается при изменении λ от 0 до ∞. Поиск значения λ^*, оптимального для заданной стоимости, может быть выполнен многими эффективными методами, например, при помощи метода бисекционного поиска [11].

Далее, для каждого типа и местоположения СрЗИ необходимо выбрать СрЗИ с таким соотношением стоимость-эффективность (остаточный риск), которое соответствует найденному значению λ^*.

Как распределить общий финансовый бюджет между типами СрЗИ и узлами информационной системы? На этот вопрос сможет дать ответ еще один известный из теории связи алгоритм – алгоритм Waterfilling.

Оптимальное распределение бюджета на средства защиты информации и алгоритм Waterfilling

Алгоритм Waterfilling (заполнения сосудов водой) и его модификации используются в телекоммуникации

для распределения энергии передатчика по поднесущим, либо по слотам временной области [12,13].

Принцип работы алгоритма Waterfilling изображен на рис.2 [8]. В работе [8] канал с непрерывным временем и аддитивным белым гауссовским шумом (АБГШ) преобразуется к нескольким дискретным по времени каналам с АБГШ. Рассматривается пропускная способность параллельного соединения каналов. В каждом канале действует шум с дисперсией Q_i. Доказывается, что оптимальным является распределение общей энергии $R_\Sigma = \sum R_i$, дополняющее шум в каждом дискретном канале до некоторой одинаковой для всех величины B.

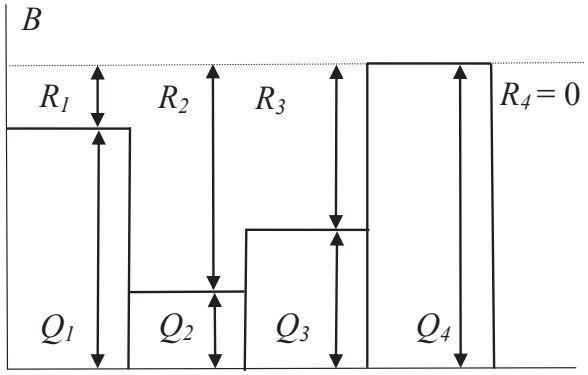

Рис.2. Иллюстрация алгоритма Waterfilling

Общая энергия представляется как объем воды, которая помещается в резервуар с неровной формой дна, определяемой дисперсией шума. Уровни, до которых поднимается вода, одинаковы (так как сосуды сообщаются).

Для перехода к задаче оптимального распределения финансового бюджета на закупку (создание) СрЗИ, заменим шум в подканалах на величину, обратную риску, а распределяемую в них энергию – на финансовые затраты. Тогда получим следующее, казалось бы, очевидное правило: следует выделять больше ресурсов на тип СрЗИ и места их размещения, в которых больше значение риска. Доказательство этого правила и необходимые выражения для каналов связи (а аналогичные им будут и для СрЗИ) приведены в [8, стр.362]

Оптимальное размещение средств защиты информации в многоуровневой системе и бисекционный поиск

Многие угрозы безопасности информации можно парировать на разных уровнях ИС, например, на уровне рабочей станции, сегмента локальной сети, границы вычислительной сети и т.д. Соответственно, существуют и СрЗИ различного уровня. Кроме того, в ряде случае целесообразно учитывать СрЗИ, которые имеются в среде функционирования конкретной ИС.

Например, рассмотрим АСУ оперативно-тактического ракетного комплекса [3]. Ракетный комплекс с точки зрения информационных технологий представляет из себя ряд вычислителей, соединенных в локальную сеть и имеющих единственную связь с «внешним миром» — с Единой системой управления тактического звена управления. С этой точки зрения она является для него средой функционирования. Далее, один из вычислителей комплекса, а именно, расположенный на пусковой машине, тоже представляет из себя локальную сеть носителя оружия, в которую включены вычислители самих ракет. Для него средой функционирования является локальная сеть ракетного комплекса. СрЗИ среды функционирования могут быть учтены как СрЗИ границы сети.

Таким образом, возникает задача размещения СрЗИ на элементах сети: поиск оптимальной расстановки СрЗИ одного типа в предположении о том, что СрЗИ на нижних уровнях могут не использоваться, в случае, если угрозы безопасности парируются СрЗИ более высокого уровня (иерархия: рабочая станция – сегмент сети – вся сеть).

Пусть имеется вычислительная сеть S, включающая в себя N сегментов $S_i, i \in \{1,\ldots,N\}$. В каждом сегменте существует M требующих защиты со стороны заданного типа СрЗИ активов (рабочих станций, серверов) $P^j_{S_i}$, $j = \{1,\ldots,M\}$.

Таким образом, для данного случая могут быть СрЗИ трех уровней: $C_S, C_{S_i}, C_{P^j_{S_i}}$.

Места расположения СрЗИ в рассматриваемой трехуровневой вычислительной сети могут быть представлены в виде дерева, где вершиной дерева является СрЗИ уровня границы сети, листьями являются СрЗИ рабочих станций (рис. 3).

Изображенное на рис.3 дерево является полным в том смысле, что оно характеризует все возможные места расположения СрЗИ.

Для каждого узла дерева, изображенного на рис. 3, можно записать задачу минимизации, аналогичную (3). При этом общий бюджет затрат, также как и остаточного риска, должен быть распределен между узлами (отдельными СрЗИ и их комбинациями) (это эквивалентно распределению общего бюджета бит между квантователями в работе [9]).

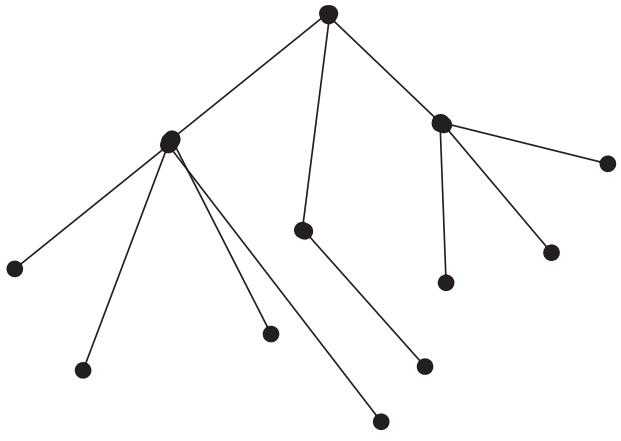

Рис. 3. Изображение мест размещения СрЗИ на уровнях вычислительной сети

На рис. 4 показано принятие решение о конфигурации дерева, представленного на рис. 3. Для каждого на-

УДК 004.491

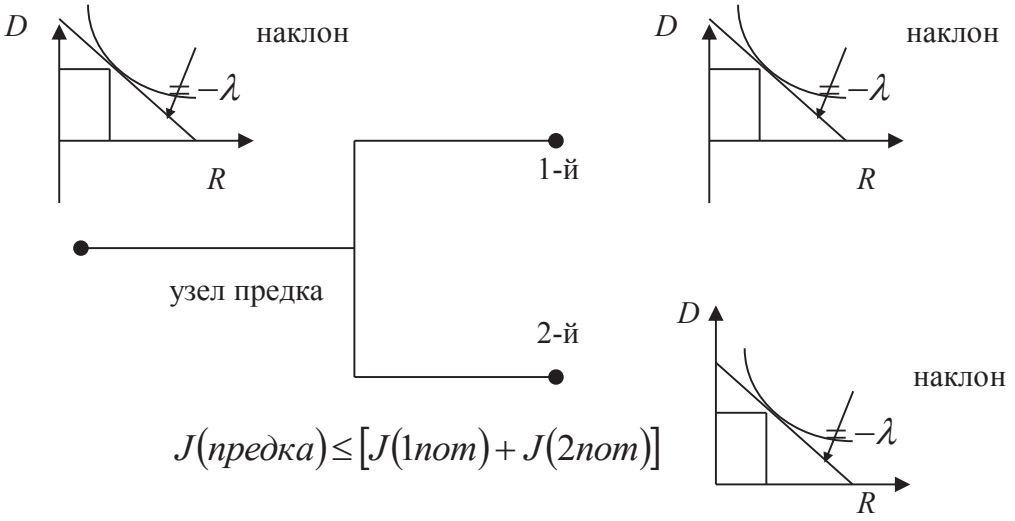

Рис. 4. Принятие решения при выборе конфигурации дерева

бора {предок-потомки} алгоритм проверяет, что выгоднее с точки зрения минимизации функции *J*: оставить потомков или заменить их на предков? Алгоритм начинает работу с листьев дерева (рис. 3) и функционирует итеративно до того, как обойдет все узлы дерева.

В результате получается некоторое усеченное дерево, характеризующее оптимальную структуру СЗИ в отношении данного типа СрЗИ.

Для нахождения оптимального значения λ^* в каждом узле может быть применен быстрый алгоритм выпуклого поиска — бисекционный метод. Алгоритм заключается в последовательном делении интервала поиска на субинтервалы до достижения сходимости. Выпуклость функции стоимость-остаточный риск гарантирует сходимость. Вначале вводится понятие смещенной стоимости Лагранжа:

$$W(\lambda) = W\left(\lambda, x^*(\lambda)\right) = \left(J^*(\lambda)\right) - \lambda R^* = \left(\min_x \left[D(x) + \lambda R(x)\right] - \lambda R^*\right) \quad (4)$$

Значение λ^*, доставляющее максимум этой функции, является оптимальным. Также оптимальной с точки зрения выбранного критерия стоимость-риск является и рабочая точка $x^*\left(\lambda^*\right)$ для данного бюджета.

Следовательно, необходимо найти точку, в которой производная от $W(\lambda)$ обращалась бы в нуль:

$$\frac{\partial W}{\partial \lambda} = \frac{\partial}{\partial \lambda}\left(\left(\sum_i \min_{x_i \in X_i}\left[D(x_i) + \lambda R(x_i)\right]\right) - \lambda R^*\right) = \sum_i R_i^*(\lambda) - R^* \quad (5)$$

где $R_i^*(\lambda)$ — стоимость, связанная с оптимальным субдеревом для СрЗИ i. В силу дискретности задачи λ является сингулярной лишь в конечном числе точек. Оптимальный наклон λ^*, максимизирующий $W(\lambda)$, соответствует сингулярному значению. Из равенства (5) следует, что для несингулярных точек $\lambda < \lambda^*$, $\sum_i R_i^*(\lambda) > R^*$, а для $\lambda > \lambda^*$, $\sum_i R_i^*(\lambda) \le R^*$. Отсюда вытекает быстрый алгоритм поиска, описываемый ниже.

Шаг 1. Выбираем значения $\lambda_l \le \lambda_h$, так чтобы

$$\sum_i R_i^*(\lambda_u) \le R^* \le \sum_i R_i^*(\lambda_l) \quad (6)$$

Шаг 2. $\lambda_{next} \leftarrow \left|\frac{\sum_i \left[D_i^*(\lambda_l) - D_i^*(\lambda_u)\right]}{\sum_i \left[R_i^*(\lambda_l) - R_i^*(\lambda_u)\right]}\right| + \varepsilon$, где ε - сколь угодно малая величина. Она необходима для того, чтобы была достигнута точка с более низкой скоростью, в том случае если λ_{next} сингулярна.

Шаг 3. Для λ_{next} выполняем первую часть алгоритма.

Если $\sum_i R_i^*(\lambda_{next}) = \sum_i R_i^*(\lambda_u)$, стоп. $\lambda^* = \lambda_u$.

Иначе если $\sum_i R_i^*(\lambda_{next}) > R^*$, то $\lambda_l \leftarrow \lambda_{next}$. Переход к шагу 2.

Иначе $\lambda_u \leftarrow \lambda_{next}$. Переход к шагу 2.

Таким образом, в настоящей статье приведены аналогии между некоторыми задачами из теории связи и задачами из теории защиты информации. При проведении аналогий были опущены некоторые математические подробности и сделаны упрощения, которые, тем не менее, могут оказаться важными с точки зрения применимости или не применимости рассмотренных подходов (например, предположение о независимости СрЗИ, исследование условий Куна-Такера и т.п.). Эти вопросы требуют дальнейших исследований.

Литература

1. В.Г. Грибунин, В.Е. Костюков, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко. Современные методы обеспечения безопасности информации в атомной энергетике / Грибунин В.Г. и др. Саров. – Изд-во РФЯЦ-ВНИИЭФ, 2014 г. 636 с.
2. Грибунин В.Г., Гришаненко Р.Л., Тимонов А.А., Смирнов Я.Д.. О проектировании системы защиты информации для информатизированных образцов вооружения // Известия института инженерной физики, №2(60), 2021 г. – С. 69-74.
3. Паршин Н.М. Перспективы развития автоматизированных систем управления ракетными войсками и артиллерией ВС РФ // Военная мысль, № 12, 2019 г. – С.76-80.
4. Лаврентьев А.В., Зязин В.П. О применении методов теории игр для решения задач компьютерной безопасности // Безопасность информационных технологий, том 20, №3, 2013 г. – С.19-24.
5. Щеглов А.Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А.Ю. Щеглов, К.А. Щеглов. – Москва: Издательство Юрайт, 2020. – 309 с.
6. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем: учебное пособие / А.Ю. Щеглов, К.А. Щеглов. – СПб: Университет ИТМО, 2015. – 93 с.
7. Горлов А.П. Способы и приемы выбора технических средств защиты информации с учетом одновременности реализации угроз. / Дисс-я на соискание ученой степени канд.техн.наук. – СПб НИУ ИТМО. — 2016. — 149 с.
8. Осокин А.Н. Теория информации: учебное пособие для прикладного бакалавриата / А.Н. Осокин, А.Н. Мальчуков. – Москва, Издательство Юрайт, 2019. – 205 с.
9. Y. Blau, T. Michaeli. Rethinking Lossy Compression: The Rate-Distortion-Perception / Tradeoff of the 36th International Conference on Machine Learning, Long Beach, California, PMLR 97, 2019.
10. Mounir Kaaniche, Aurella Fraysse, Beatrice Pesquet-Popescu, Jean-Christophe Pesquet. A convex programming bit allocation method for sparce sources. // Proc. Of the IEEE International Picture Coding Symposium. – 2012. Poland. – P.853-856..
11. Слабнов В.Д. Численные методы. — М.: Лань, 2020. — 392 с.
12. Б.Скляр. Цифровая связь: теоретические основы и практическое применение / Скляр Б., Гроза Е. [и др.] (пер. с англ.) – 2-е изд. – М.: Вильямс. – 2016. – 1099 с.
13. Bianchi G., Cuomo F., Garlist D., Tinnirello I. Capture Aware Sequential Waterffilling for LoraWAN Adaptive Data Rate. – IEEE Transactions on Wireless Communications. – V.20. – Issue 3. – March 2021. – P.2019-2033.

ON THE ANALOGY OF THE PROBLEMS OF OPTIMIZING THE CHOICE OF INFORMATION SECURITY CONTROLS WITH SOME PROBLEMS OF COMMUNICATION THEORY

Gribunin V.G.[3], Timonov A.A.[4]

Abstract

Purpose of the article: *optimization of the choice of information security tools in a multi-level automated system, taking into account higher levels, quality indicators of information security tools, as well as the general financial budget. Demonstration of analogies of solving these problems with known problems from communication theory.*

Research method: *optimal choice of information security tools based on risk analysis and the Lagrange multiplier method; Optimal bit budget allocation based on the Waterfilling optimization algorithm. Optimal placement of information security tools in a multilevel automated system based on bisectional search.*

Obtained result: *the article shows analogies between some problems of communication theory and the optimal choice of information security tools. The well-known problem of the optimal choice of information security tools is solved using the rate-distortion theory, the well-known problem of the optimal budget allocation for their purchase is solved by analogy with the problem of distributing the power of transmitters. For the first time, the problem posed for the optimal placement of information security tools in a multilevel automated system was solved by analogy with the problem of distributing the total bit budget between quantizers.*

Keywords: *problem of choice, rate-distortion function, Lagrange multiplier, tree pruning, optimization, communication theory.*

3 Vadim Gribunin, Dc.Sc., Chief Researcher of the IIF, Moscow, Russia. E-mail: wavelet2@mail. ru

4 Andrey Timonov, Russian Defense Ministry employee, Moscow, Russia. E-mail: a. timonov@mil.ru

References

1. V.G. Gribunin, V.E. Kostiukov, A.P. Marty`nov, D.B. Nicolaev, V.N. Fomchenko. Sovremenny`e metody` obespecheniia bezopasnosti informatcii v atomnoi` e`nergetike / Gribunin V.G. i dr. Sarov. – Izd-vo RFIATC-VNIIE`F, 2014 g. 636 s.
2. Gribunin V.G., Grishanenko R.L., Timonov A.A., Smirnov Ia.D.. O proektirovanii sistemy` zashchity` informatcii dlia informatizirovanny`kh obraztcov vooruzheniia // Izvestiia instituta inzhenernoi` fiziki, №2(60), 2021 g. – S. 69-74.
3. Parshin N.M. Perspektivy` razvitiia avtomatizirovanny`kh sistem upravleniia raketny`mi voi`skami i artilleriei` VS RF // Voennaia my`sl`, № 12, 2019 g. – S.76-80.
4. Lavrent`ev A.V., Ziazin V.P. O primenenii metodov teorii igr dlia resheniia zadach komp`iuternoi` bezopasnosti // Bezopasnost` informatcionny`kh tekhnologii`, tom 20, №3, 2013 g. – S.19-24.
5. Shcheglov A.Iu. Zashchita informatcii: osnovy` teorii: uchebnik dlia bakalavriata i magistratury` / A.Iu. Shcheglov, K.A. Shcheglov. – Moskva: Izdatel`stvo Iurai`t, 2020. – 309 s.
6. Shcheglov A.Iu. Matematicheskie modeli i metody` formal`nogo proektirovaniia sistem zashchity` informatcionny`kh sistem: uchebnoe posobie / A.Iu. Shcheglov, K.A. Shcheglov. – SPb: Universitet ITMO, 2015. – 93 s.
7. Gorlov A.P. Sposoby` i priemy` vy`bora tekhnicheskikh sredstv zashchity` informatcii s uchetom odnovremennosti realizatcii ugroz. / Diss-ia na soiskanie uchenoi` stepeni kand.tekhn.nauk. – SPb NIU ITMO. — 2016. — 149 s.
8. Osokin A.N. Teoriia informatcii: uchebnoe posobie dlia pricladnogo bakalavriata / A.N. Osokin, A.N. Mal`chukov. – Moskva, Izdatel`stvo Iurai`t, 2019. – 205 s.
9. Y. Blau, T. Michaeli. Rethinking Lossy Compression: The Rate-Distortion-Perception / Tradeoff of the 36th International Conference on Machine Learning, Long Beach, California, PMLR 97, 2019.
10. Mounir Kaaniche, Aurella Fraysse, Beatrice Pesquet-Popescu, Jean-Christophe Pesquet. A convex programming bit allocation method for sparce sources. // Proc. Of the IEEE International Picture Coding Symposium. – 2012. Poland. – P.853-856.
11. Slabnov V.D. Chislenny`e metody`. — M.: Lan`, 2020. — 392 s.
12. B.Scliar. Tcifrovaia sviaz`: teoreticheskie osnovy` i prakticheskoe primenenie / Scliar B., Groza E. [i dr.] (per. s angl.) – 2-e izd. – M.: Vil`iams. – 2016. – 1099 s.
13. Bianchi G., Cuomo F., Garlist D., Tinnirello I. Capture Aware Sequential Waterffilling for LoraWAN Adaptive Data Rate. – IEEE Transactions on Wireless Communications. – V.20. – Issue 3. – March 2021. – P.2019-2033.