Раздел 4 АВТОМАТИЗАЦИЯ, АНАЛИЗ И ОБРАБОТКА ИНФОРМАЦИИ, УПРАВЛЕНИЕ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ В СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ СИСТЕМАХ

УДК 621.3
DOI: 10.34046/aumsuomt95/22

ОПТИМИЗАЦИЯ КОМПЛЕКТА ЗИП ОБОРУДОВАНИЯ РАДИОТЕХНИЧЕСКИХ ПОСТОВ СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ СУДОВ

Н.В. Старжинская, кандидат технических наук, доцент,
А.И. Чернова, кандидат технических наук, доцент,

В работе предложены математические модели определения оптимального комплекта ЗИП берегового радиооборудования радиотехнического поста. Проведена количественная оценка необходимого количества запасных частей для различных стратегий пополнения. Полученные соотношения могут быть использованы для определения количества и оптимальной стратегии пополнения различных комплектов ЗИП берегового радиооборудования с учетом условий эксплуатации.
Ключевые слова: береговое радиооборудование, радиотехнический пост, ЗИП, надёжность, коэффициент готовности, стратегия пополнения, показатели надёжности, показатели достаточности.

The mathematic models of determining the optimal SPTA of the coastal radio equipment of radio engineering station are proposed in the article. The reliability of the coastal radio equipment of the radio engineering post as well as the SPTA quantity needed for various implementation strategies are evaluated. The obtained results may be used to determine the number of spares and the optimal strategy for replenishing different sets of radio equipment under operating conditions.
Key words: coastal radio equipment, radio engineering post, spare parts, tools and accessories (SPTA), reliability, availability factor, replenishment strategy, reliability indicator, sufficiency indicator.

Обеспечение надежности берегового радиооборудования средств контроля судозаходов, в условиях роста интенсивности судопотока через морские порты, является одной из важнейших эксплуатационных задач. Это связано с тем, что они, в свою очередь, определяют уровень безопасности мореплавания и выполнения технологических процессов работы судов на акватории морского порта. Одной из береговых систем обеспечения безопасности мореплавания на акватории порта и на подходах к нему является Система управления движением судов (СУДС). Основными задачами СУДС, согласно резолюции ИМО А.857(20), являются сбор и оценка данных, принятие решений, обработка информации и выдача её на суда, обычный контроль за судами (предоставление службой УДС данных для процесса принятия судоводительских решений на судах).

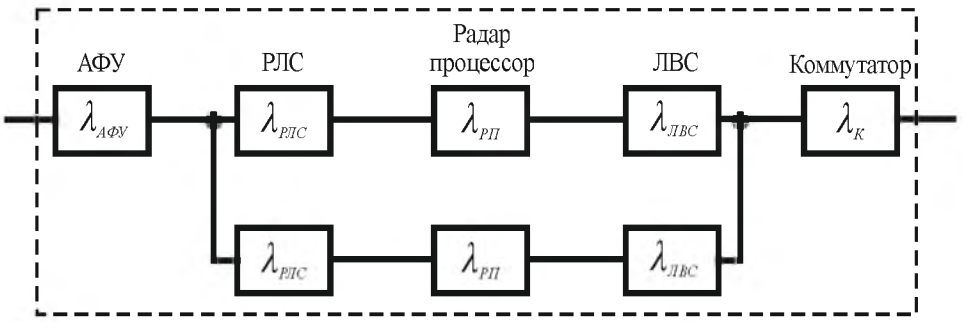
Простой или выход из строя радиоэлектронного оборудования СУДС ведёт к простою системы обеспечения безопасности в акватории порта в целом, а это недопустимо. Для обеспечения непрерывного функционирования таких систем необходимо поддерживать надёжность оборудования на требуемом уровне. Так для оборудования СУДС, согласно [1], вероятность безотказной работы должна составлять 0,9999. Для этого на радиотехнических постах (РТП) СУДС применяются различные виды резервирования радиоэлектронного оборудования. Однако при отказе основного элемента системы и включении резервного элемента, оборудование на время ремонта и замены основного элемента остается без резерва, что может привести к простою системы в случае отказа обоих элементов.

Одним из эффективных методов поддержания работоспособности радиоэлектронного оборудования в процессе эксплуатации помимо резервирования является применение запасных частей, входящих в комплект ЗИП, необходимых при проведении ремонтов и технического обслуживания (ТО). Для обеспечения требуемого

уровня надёжности радиоэлектронного оборудования РТП СУДС в процессе эксплуатации необходимо иметь такой состав ЗИП, который обеспечил бы приведенные выше требования к надёжности [2].

Рассмотрим определение комплекта ЗИП на примере радарного блока РТП «Дооб». Надежностная схема радарного блока с учетом применения резервирования, приведена на рисунке 1. Радарный блок включает два независимых радара Terma Scanter1+1 X-band с радар процессорами, которые по независимым кабельным линиям UTP (ЛВС) подключены к коммутатору. РЛС нагружены через волновод на щелевую антенну [2]

В таблице 1 приведены интенсивности отказов элементов радарного блока [2]..



РЛС Terma Scanter (1+1)

Рисунок 1 – Надежностная схема радарного блока СУДС

Таблица 1 – Интенсивности отказов элементов радарного блока

№	Наименование оборудования	Обозначения по схеме	Интенсивность отказов, 1/час	Стоимость (у.е)
1	Антенно-фидерное устройство (АФУ)	$\lambda_{АФУ}$	$1{,}87 \cdot 10^{-5}$	55000
2	БРЛС Terma Scanter	$\lambda_{РЛС}$	$1{,}41 \cdot 10^{-5}$	232000
3	Радар-процессор	$\lambda_{РП}$	$1{,}41 \cdot 10^{-5}$	90000
4	Витая пара	$\lambda_{ЛВС}$	$1 \cdot 10^{-5}$	30000
5	Коммутатор	$\lambda_{К}$	$1{,}142 \cdot 10^{-5}$	31000

Проведем расчет оптимального комплекта ЗИП для рассматриваемого блока. Согласно рис. 1 схема радиооборудования представляет собой последовательное соединение двух отдельных элементов (АФУ, коммутатор) и группы резервированных элементов (РЛС, радар-процессор, ЛВС). Группа резервированных элементов состоит из элементов, соединенных по схеме нагруженного резерва, и представляется последовательным соединением трех элементов (РЛС, радар-процессор, ЛВС) и двух резервированных групп.

В состав комплекта ЗИП последовательно включаются элементы, добавление которых приводит к максимальному приращению показателей надежности системы. После каждого шага добавления элемента необходимо оценить достаточность достигнутого значения показателей и суммарную стоимость ЗИП. Процесс формирования ЗИП завершается после того, как только будут достигнуты значения показателей надежности и стоимости, удовлетворяющие требованиям эксплуатации.

Проведем расчеты для трех стратегий пополнения ЗИП [3, 4]: периодическое пополнение, пополнение при экстренной доставке и непрерывное пополнение. Для расчетов зададим следующие временные параметры: $T_{ЗИП} = 1$ год – период пополнения ЗИП; $T_{ЭП} = 12$ часов – время экстренного пополнения ЗИП; $T_{Д\ ЗИП} = 1$ час – время доставки элемента из ЗИП; $T_{Д\ ЦБ} = 24$ часа – время доставки элемента из центральной базы.

Меняя начальные значения количества запасов в каждой группе, производим аналогичные расчеты коэффициента готовности всей системы и суммарную стоимость. Полученные данные, после каждого шага добавления элемента, сводим в таблицу 2.

1. Определение комплекта ЗИП для радарного блока СУДС при пополнении запаса с экстренными доставками

Программа расчета оптимального комплекта ЗИП для стратегии пополнения с экстренными доставками

ORIGIN:= 1

$Кгзип_{экстр} :=$

$\lambda \leftarrow \left(1.87\times 10^{-5}\ \ 1.41\cdot 10^{-5}\ \ 1.41\cdot 10^{-5}\ \ 1\cdot 10^{-5}\ \ 1.14210^{-5}\right)^{T}$

$Тзип \leftarrow 8760$

$Тэд \leftarrow 12$

$n \leftarrow 1$

$x1 \leftarrow 1$

$x2 \leftarrow 2$

$x3 \leftarrow 2$

$\omega 5 \leftarrow \dfrac{1}{\dfrac{1}{\lambda_5} + Тэд}$

$\omega 15 \leftarrow \lambda_5 + \dfrac{1}{Тэд}$

$K5экстр \leftarrow 1 - \omega 5\cdot Тэд + \dfrac{\omega 5\cdot Тэд}{\omega 15\cdot Тзип}$ — Периодическое пополнение с экстр. доставками (нерезервированный элемент, нулевой ЗИП)

$A4 \leftarrow n\cdot\lambda_4\cdot Тзип$

$\omega 14 \leftarrow \lambda_4 + \dfrac{1}{Тэд}$

$D4 \leftarrow \dfrac{Тзип}{Тэд}$

$K4экстр \leftarrow 1 - \dfrac{A4}{A4 + D4}\cdot\left(1 - \dfrac{1 - e^{-\omega 14\cdot Тзип}}{A4 + D4}\right)$ — Периодическое пополнение с экстр. доставками (резервированный элемент, нулевой ЗИП)

$A1 \leftarrow n\cdot\lambda_1\cdot Тзип$

$K1экстр \leftarrow 1 - \left[\dfrac{Тэд}{2\cdot Тзип\cdot\left(1 + \dfrac{1}{x1}\right)}\right]\cdot\left(\dfrac{2\cdot A1}{x1} - 1 + e^{\frac{-2\cdot A1}{x1}}\right)$ — Периодическое пополнение с экстр. доставками (нерезервированный элемент, ЗИП (L=1))

$A2 \leftarrow n\cdot\lambda_2\cdot Тзип$

$A3 \leftarrow n\cdot\lambda_3\cdot Тзип$

$K2экстр \leftarrow 1 - \left[\dfrac{Тэд}{2\cdot Тзип\cdot\left(1 + \dfrac{1}{x2}\right)}\right]\cdot\left(\dfrac{2\cdot A2}{x2} - 1 + e^{\frac{-2\cdot A2}{x2}}\right)$ — Периодическое пополнение с экстр. доставками (резервированный элемент, ЗИП (L=1))

$K3экстр \leftarrow 1 - \left[\dfrac{Тэд}{2\cdot Тзип\cdot\left(1 + \dfrac{1}{x3}\right)}\right]\cdot\left(\dfrac{2\cdot A3}{x3} - 1 + e^{\frac{-2\cdot A3}{x3}}\right)$

$Кгзип \leftarrow K1экстр\cdot K2экстр\cdot K3экстр\cdot K4экстр\cdot K5экстр$

$Кгзип$

$Кгзип_{экстр} = 0.9997202$

Таблица 2 – Данные, описывающие процесс формирования комплекта ЗИП для стратегии пополнения с экстренными доставками

Суммарное число элементов в ЗИП	Число типов элементов в ЗИП					Кг сист	Сзип, у.е
	λ1	λ2	λ3	λ4	λ5		
0						0,99872	0
1	1					0,99938	55000
2	1	1				0,99955	287000
3	1	1	1			0,99972	377000
4	1	1	1		1	0,99985	408000
5	2	1	1		1	0,99986	463000
6	2	1	1		2	0,999865	494000
7	2	2	1		2	0,999867	726000
8	2	2	2		2	0,999868	816000
9	3	2	2		2	0,99987	871000
10	3	2	2		3	0,99987	902000
11	3	3	2		3	0,99987	1134000
12	3	3	3		3	0,99987	1224000
13	4	3	3		3	0,99988	1279000
14	4	3	3		4	0,99988	1310000

2. Определение комплекта ЗИП для радарного блока СУДС при периодическом пополнении запаса. Проведем теперь аналогичный расчет комплекта ЗИП для радарного блока при стратегии периодического пополнения запасов. Программа расчета комплекта ЗИП выполнена в математическом редакторе MathCAD и приведена ниже.

Программа расчета оптимального комплекта ЗИП для стратегии периодического пополнения

$$\lambda := \left(1.87\times 10^{-5} \quad 1.41\cdot 10^{-5} \quad 1.41\cdot 10^{-5} \quad 1\cdot 10^{-5} \quad 1.14210^{-5}\right)^{T}$$

$$Тзип := 8760$$

$$x5 := 0 \qquad n5 := 1 \qquad A5 := n5\cdot\lambda_5\cdot Тзип$$

$$P5(t) := \sum_{i=0}^{x5} \frac{A5^{i}}{i!}\cdot e^{-A5}$$

Периодическое пополнение (нерезервированный элемент, нулевой ЗИП)

$$K5период(t) := \frac{1}{Тзип}\cdot\int_{0}^{Тзип} P5(t)\,dt$$

$$x_4 := 1 \qquad n4 := 1 \qquad A4 := n4\cdot\lambda_4\cdot Тзип$$

$$P4(t) := \sum_{i=0}^{x_4} \frac{A4^{i}}{i!}\cdot e^{-A4}$$

Периодическое пополнение (резервированный элемент, нулевой ЗИП)

$$K4период(t) := \frac{1}{Тзип}\cdot\int_{0}^{Тзип} P4(t)\,dt$$

$$x1 := 1 \qquad n1 := 1 \qquad A1 := n1\cdot\lambda_1\cdot Тзип$$

$$P1(t) := \sum_{i=0}^{x1} \frac{A1^{i}}{i!}\cdot e^{-A1}$$

Периодическое пополнение (нерезервированный элемент, ЗИП=1)

$$K1период(t) := \frac{1}{Тзип}\cdot\int_{0}^{Тзип} P1(t)\,dt$$

$$x2 := 2 \qquad n2 := 1 \qquad A2 := n2\cdot\lambda_2\cdot Тзип$$

$$P2(t) := \sum_{i=0}^{x2} \frac{A2^{i}}{i!}\cdot e^{-A2}$$

Периодическое пополнение (резервированный элемент, ЗИП (L=1))

$$K2период(t) := \frac{1}{Тзип}\cdot\int_{0}^{Тзип} P2(t)\,dt$$

$$x3 := 2 \qquad n3 := 1 \qquad A3 := n3\cdot\lambda_3\cdot Тзип$$

$$P3(t) := \sum_{i=0}^{x3} \frac{A3^{i}}{i!}\cdot e^{-A3}$$

$$K3период(t) := \frac{1}{Тзип}\cdot\int_{0}^{Тзип} P3(t)\,dt$$

$$Кгзип_{период} := K1период(Тзип)\cdot K2период(Тзип)\cdot K3период(Тзип)\cdot K4период(Тзип)\cdot K5период(Тзип)$$

$$Кгзип_{период} = 0.89016$$

Далее производим аналогичные расчеты коэффициента готовности всей системы при периодическом пополнении комплекта запасных частей, меняя значения количества запасов в каждой группе. Также находим суммарную стоимость элементов комплекта ЗИП. Результаты определения комплекта ЗИП при периодическом пополнении запаса после каждого шага добавления элементов, сводим в таблицу 3, приведенную ниже.

Таблица 3 – Данные, описывающие процесс формирования комплекта ЗИП при стратегии его периодического пополнения

Суммарное число элементов в ЗИП	**Число типов элементов в ЗИП**					**Кг сист**	**С зип**
	λ1	λ2	λ3	λ4	λ5		
0						0,75458	0
1	1					0,87819	55000
2	1	1				0,89435	287000
3	1	1	1			0,89016	377000
4	1	1	1		1	0,97922	408000
5	1	1	1	1	1	0,98266	438000
6	2	1	1	1	1	0,99399	439000
7	2	1	1	1	2	0,99852	524000
8	2	2	1	1	2	0,99879	756000
9	2	2	2	1	2	0,99907	846000
10	3	2	2	1	2	0,99969	901000
11	3	2	2	2	2	0,99979	931000
12	3	3	2	2	2	0,99980	1163000
13	**3**	**3**	**2**	**2**	**3**	**0,99995**	**1194000**
14	**3**	**3**	**3**	**2**	**3**	**0,999967**	**1284000**

3. Определение комплекта ЗИП для радарного блока СУДС при непрерывном пополнении запаса. Аналогично предыдущим расчетам произведём вычисления для определния комплекта ЗИП для радарного блока при стратегии с непрерывным пополнением запаса. Программа расчета комплекта ЗИП при непрерывном пополнении запаса выполнена в математическом редакторе MathCAD и приведена ниже.

Программа расчета оптимального комплекта ЗИП для стратегии непрерывного пополнения

ORIGIN:= 1

$\lambda := \left(1.87\times 10^{-5} \quad 1.41\cdot 10^{-5} \quad 1.41\cdot 10^{-5} \quad 1\cdot 10^{-5} \quad 1.1421\cdot 10^{-5}\right)^{T}$

Тзип := 8760 t := 8760

Тдцб := 24

x1 := 2 $\gamma 1 := \lambda_1 \cdot Тдцб$

$K1непр := 1 - \dfrac{\dfrac{\gamma 1^{x1+1}}{(x1+1)!}}{\sum_{i=0}^{x1+1} \dfrac{\gamma 1^{i}}{i!}}$

Непрерывное пополнение (нерезервированный элемент, ЗИП (L=1))

$P2c(t) := 1 - \left(1 - e^{-\lambda_2 \cdot t}\right)^{2}$

$\lambda 22(t) := \dfrac{-\left(\dfrac{d}{dt} P2c(t)\right)}{P2c(t)}$

$\lambda 22(t) = 2.936\times 10^{-6}$

x2 := 1 $\gamma 2 := \lambda 22(t) \cdot Тдцб$

$K2непр := 1 - \dfrac{\dfrac{\gamma 2^{x1+1}}{(x2+1)!}}{\sum_{i=0}^{x2+1} \dfrac{\gamma 2^{i}}{i!}}$

Непрерывное пополнение (резервированный элемент, ЗИП (L=1))

$P3c(t) := 1 - \left(1 - e^{-\lambda_3 \cdot t}\right)^{2}$

$\lambda 33(t) := \dfrac{-\left(\dfrac{d}{dt} P3c(t)\right)}{P3c(t)}$

x3 := 1 $\gamma 3 := \lambda 33(t) \cdot Тдцб$

$K3непр := 1 - \dfrac{\dfrac{\gamma 3^{x3+1}}{(x3+1)!}}{\sum_{i=0}^{x3+1} \dfrac{\gamma 3^{i}}{i!}}$

$$P4c(t) := 1 - \left(1 - e^{-\lambda_4 \cdot t}\right)^2$$

$$\lambda44(t) := \frac{-\left(\frac{d}{dt} P4c(t)\right)}{P4c(t)}$$

$\lambda44(t) = 1.548 \times 10^{-6}$

$x4 := 0 \qquad \gamma4 := \lambda44(t) \cdot Tдцб$

$$K4непр := 1 - \frac{\frac{\gamma4^{x4+1}}{(x4+1)!}}{\sum_{i=0}^{x4+1} \frac{\gamma4^i}{i!}}$$

Непрерывное пополнение (резервированный элемент, нулевой ЗИП)

$x5 := 1 \qquad \gamma5 := \lambda_5 \cdot Tдцб$

$$K5непр := 1 - \frac{\frac{\gamma5^{x5+1}}{(x5+1)!}}{\sum_{i=0}^{x5+1} \frac{\gamma5^i}{i!}}$$

Непрерывное пополнение (нерезервированный элемент, ЗИП (L=1))

$K5непр = 0.999999962$

$Kгзип := K1непр \cdot K2непр \cdot K3непр \cdot K4непр \cdot K5непр$

$Kгзип = 0.999963$

Меняя значения количества запасов в каждой группе производим расчет коэффициента готовности всей системы при непрерывном пополнении комплекта ЗИП. А также находим суммарную стоимость элементов комплекта ЗИП. Результаты определения комплекта ЗИП при непрерывном пополнении запаса после каждого шага добавления элементов, сводим в таблицу 4, приведенную ниже.

Таблица 4 – Данные, описывающие процесс формирования ЗИП для стратегии непрерывного пополнения

Суммарное число элементов в ЗИП	**Число типов элементов в ЗИП**					**Кг сист**	**С зип**
	□1	□2	□3	□4	□5		
0						0,9991	0
1	1					0,99954	55000
2	1	1				0,999618	287000
3	1	1	1			0,999689	377000
4	**1**	**1**	**1**		**1**	**0,9999627**	**408000**
5	2	1	1		1	0,9999628	463000
6	2	2	1		1	0,9999628	695000
7	2	2	2		1	0,9999628	785000
8	2	2	2		2	0,999963	816000
9	3	2	2		2	0,999963	871000
10	3	3	2		2	0,999963	1103000
11	3	3	3		2	0,999963	1193000
12	3	3	3	1	2	0,9999999	1223000

Анализ полученных выше результатов, позволяет принять решение о выборе оптимального комплекта ЗИП. Для этого построим зависимости стоимости комплектов ЗИП от суммарного числа элементов при различных стратегиях его пополнения (см. рис. 2).

Полученные с помощью проведенных расчетов результаты дают полное представление о процессе формирования комплекта ЗИП при различных стратегиях его пополнения. В частности, при периодическом пополнении ЗИП коэффициент готовности системы $K_г$ оказывается довольно низким. Коэффициент готовности нерезервированной системы с периодическим пополнением ЗИП $K_{г\ период} = 0{,}75468$, и только при числе элемен-

тов в ЗИП $N_{ЗИП}$ =13 достигает требуемого значения $K_{г\ период}$ = 0,99995. Это можно объяснить тем, что при стратегии периодического пополнения после каждого отказа система остается неработоспособной в течение всего времени до момента очередного пополнения ЗИП.

При стратегии пополнения ЗИП с экстренными доставками величина коэффициента готовности $K_{г\ экстр}$ достигает стабильного хорошего значения 0,999 (при $T_{эд}$ = 12 ч). Если время задержки при экстренной доставки увеличить, например, до 2-3 суток ($T_{эд}$ = 48÷72 ч), величина коэффициента готовности $K_{г\ экстр}$ уменьшается и изменяется в пределах от 0,9949 до 0,9995 для $T_{эд}$ = 48 ч и в пределах от 0,9924 до 0,99925 для $T_{эд}$ = 72 ч.

При использовании стратегии непрерывного пополнения комплекта ЗИП коэффициент готовности системы $K_{г\ непр}$ достигает высокого значение $K_{г\ непр}$=0,999963 при достаточно малом количестве дополнительных элементов.

Исходя из результатов расчета, приведенных в табл. 2–4 можно заметить, что распределение оптимального количества элементов в ЗИП не зависит от стратегии пополнения при числе элементов в ЗИП $N_{зип}$ < 4. При больших значениях $N_{зип}$ распределения отличаются. Это объясняется различной динамикой изменения состава ЗИП во времени в процессе эксплуатации рассматриваемой системы.

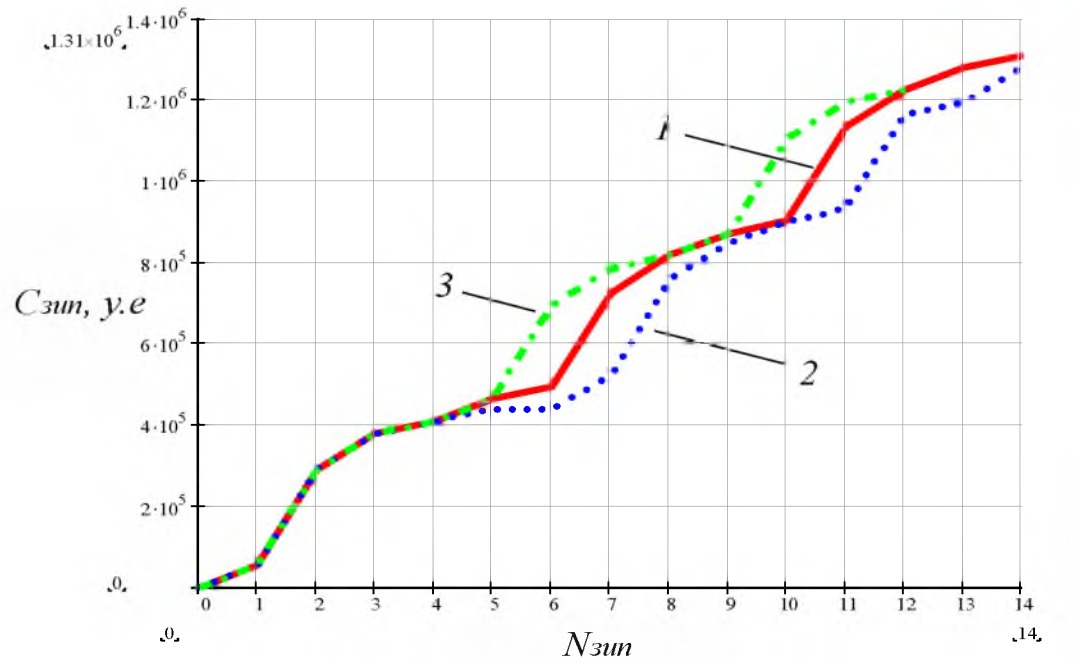


Рисунок 2 – Зависимость стоимости комплекта ЗИП от суммарного числа элементов при различных стратегиях пополнения: 1 – стратегия с экстренными доставками ЗИП; 2 – стратегия с периодическим пополнением ЗИП; 3 – стратегия непрерывного пополнения комплекта ЗИП

Приведенная в работе методика является удобным инструментом анализа возможной потребности в комплекте ЗИП при различных условиях эксплуатации рассматриваемого радиооборудования. При этом окончательное решение о необходимой комплектации ЗИП может принимать эксплуатационный персонал, учитывая реальные требования к надежности радиооборудования РТП СУДС и ограничений по стоимости.

Результаты расчетов, проведенных в работе, дают представление о процессе формирования состава ЗИП при различных стратегиях пополнения запасов. В действительности, могут применяться и другие варианты стратегий пополнения. Но, в любом случае, они них будут находиться в пределах, ограниченных крайними стратегиями – периодическое пополнение (худший случай) и непрерывное пополнение (лучший случай).

Литература

1. Приказ Минтранса РФ от 23.07.2015 № 226.
2. Чернова А.И., Старжинская Н.В. Эксплуатационная надёжность берегового радиооборудования с учётом применения ЗИП для восстановления работоспособности// Транспортное дело России. – Морские вести России.– – 2019. – № 3. – С. 129-132.
3. Черкесов, Г.Н. Оценка надежности систем с учетом ЗИП: учеб. пособие / Г. Н. Черкесов. – СПб.: БХВ-Петербург, 2012. – 480 с. – ил.
4. Черкесов, Г.Н. О критериях выбора комплектов

ЗИП / Г.Н. Черкесов // Надежность. – 2013. – №2. – С.3-33.

REFERENCES

1. Prikaz Mintransa RF ot 23.07.2015 № 226.
2. Chernova A.I., Starzhinskaya N.V. Ekspluatacionnaya nadyozhnost' beregovogo radiooborudovaniya s uchyotom primeneniya ZIP dlya vosstanovleniya rabotosposobnosti// Transportnoe delo Rossii. – Morskie vesti Rossii, Moskva. – 2019. – № 3. – S. 129-132.
3. Cherkesov, G.N. Ocenka nadezhnosti sistem s uchetom ZIP: ucheb. posobie / G. N. Cherkesov – SPb.: BHV-Peterburg, 2012. – 480 s. – il.
4. Cherkesov, G.N. O kriteriyah vybora komplektov ZIP / G.N. CHerkesov // Nadezhnost'. – 2013. – №2. – S.3–33.

УДК 681.3.001:518.5
DOI: 10.34046/aumsuomt95/23

ИСПОЛЬЗОВАНИЕ КРОНЕКЕРОВА ПРОИЗВЕДЕНИЯ МАТРИЦ ДЛЯ МОДИФИКАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Е.И. Духнич, доктор технических наук, профессор
А.Г. Чефранов, доктор технических наук, профессор

В статье рассматривается использование произведения Кронекера (КП) для повышения эффективности криптографических алгоритмов. Формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера может использоваться при разработке новых блочных криптографических алгоритмов, в которых используются матрицы со следующими свойствами: ортогональные (унитарные), обращаемые, инволютивные. Модификации шифра Хилла с ключевой матрицей размером открытого текста, $T = 2^K$ байтов, представленной как произведение Кронекера из K обратимых элементарных матриц (ОЭМ), рассматривается в ряде работ. Они имеют квадратичную вычислительную сложностиО(T^2). Мы предлагаем модификации шифра Хилла на основе КР, НКР и I-НКР, где матрица ключей квадратичного размера фактически не рассчитывается. Вместо этого ОЭМ итеративно умножаются на открытый текст за время O($T\log_2 T$) и требуют линейной сложности памяти. Оценка времени шифрования таких модифицированных алгоритмов аналогична оценке шифров AES и RC4.
Ключевые слова: произведение Кронекера, шифр Хилла, одноразовый шифр, обратимая элементарная матрица.

The article discusses the use of the Kronecker product (KP) to improve the efficiency of cryptographic algorithms. The formation of large matrices with specified properties using KP of small matrices can be used in the development of new block cryptographic algorithms that use matrices with the following properties: orthogonal (unitary), invertible, involutive. Hill cipher modifications with a plaintext key matrix, $T = 2^K$ bytes, represented as a Kronecker product of K invertible elementary matrices (IEM), are considered in a number of works. They have quadratic computational complexity O(T^2). We propose modifications of the Hill cipher based on KP where the matrix of keys of a quadratic size is not actually calculated. Instead, IEMs are iteratively multiplied by the plaintext in O ($T\log_2 T$) time and need linear memory complexity. The estimation of the encryption time for such modified algorithms is similar to the estimation of the AES and RC4 ciphers.
Keywords: Kronecker product, Hill cipher, one-time cipher, invertible elementary matrix

Введение. Кронекерово произведение (КП) матриц сходно с тензорным произведением и широко используется во многих приложениях, в том числе, при обработке сигналов и изображений [1-5]. Формирование матриц большого размера с заданными свойствами с помощью КП матриц малого размера может использоваться при разработке новых вычислительных алгоритмов. Например, известны подходы к построению матриц для обработки сигналов и блочных криптографических алгоритмов со следующими свойствами:

- ортогональные (унитарные) матрицы [2];
- обращаемые матрицы [3];
- инволютивные матрицы [4].

Имея набор матриц, необходимо многократно выполнять операцию умножения их КП на вектор. Эта операция является критическим ядром для итерационных алгоритмов, так как умножение квадратной матрицы размера $\boldsymbol{n} \times \boldsymbol{n}$на вектор имеет вычислительную сложность O(n^2), и поэтому ее необходимо эффективно ускорять.

Размер КП элементарных матриц (ЭМ) может быть значительным, например, КП десяти ЭМ с$n = 10$ равен n^{10}, соответственно, умножение на вектор имеет сложность порядка10^{20}. Известны эффективные алгоритмы выполнения умножения вектора на КП произвольных матриц, которые оптимизируют и организацию использования памяти системы. В [3] предложен эффективный алгоритм умножения КП произвольных матриц на вектор (далее, УКПВ), рассмотрена задача о выборе размера участвующих в КП матриц, минимизирующего вычислительную сложность УКПВ, и