УДК 681.3
DOI: 10.26102/2310-6018/2025.51.4.067

Моделирование процессов управления информационными массивами в киберфизических системах

Т.В. Аветисян[1]✉, С.И. Короткевич[2], М.В. Питолин[3]

[1]Воронежский институт высоких технологий, Воронеж, Российская Федерация
[2]Воронежский государственный технический университет, Воронеж, Российская Федерация
[3]Воронежский институт МВД России, Воронеж, Российская Федерация

Резюме. Киберфизические системы имеют существенное отличие от обычных встроенных систем тем, что в них применяются более развитые информационные связи среди вычислительных и физических элементов. В этой связи в них применяется архитектура, которая аналогична интернету вещей. Внутри киберфизических систем существует распределение вычислительной компоненты по всей физической системе. Она рассматривается в виде носителя и синергическим образом связана с ее информационными массивами. В работе рассматриваются несколько стратегий, позволяющих эффективно работать с информационными массивами. Первая базируется на создании копий информационных массивов, которые будут использоваться если основной массив будет разрушен. Вторая стратегия базируется на использовании предыстории для информационного массива. Третья стратегия базируется на том, что применяется смешанный подход, в котором учитываются и копии, и предыстории. Для каждой из стратегий приведена наглядная иллюстрация их работы. Показано, какое может быть среднее время доступа к компьютеру при различных стратегиях. Дана иллюстрация диаграммы эффективности применения разных стратегий. Результаты работы могут быть практически полезны при создании киберфизических систем и оптимизации их функционирования.

Ключевые слова: информационный массив, киберфизическая система, стратегии резервирования, моделирование процессов управления, время доступа.

Для цитирования: Аветисян Т.В., Короткевич С.И., Питолин М.В. Моделирование процессов управления информационными массивами в киберфизических системах. *Моделирование, оптимизация и информационные технологии.* 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2139 DOI: 10.26102/2310-6018/2025.51.4.067

Modeling of information management processes arrays in cyber-physical systems

T.V. Avetisyan[1]✉, S.I. Korotkevich[2], M.V. Pitolin[3]

[1]Voronezh Institute of High Technologies, Voronezh, the Russian Federation
[2]Voronezh State Technical University, Voronezh, the Russian Federation
[3]Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, the Russian Federation

Abstract. Cyberphysical systems differ significantly from conventional embedded systems in that they use more advanced information connections among computing and physical elements. In this regard, they use architecture that is like the Internet of Things. Within cyberphysical systems, there is a distribution of computing components throughout the physical system. It is considered as a carrier and is synergistically connected with its information arrays. The paper considers several strategies for effective work with information arrays. The first is based on creating copies of information arrays that will be used if the main array is destroyed. The second strategy is based on using the background for the information array. The third strategy is based on the fact that a mixed approach is used, which considers

both copies and backstories. A visual illustration of their operation is provided for each of the strategies. It shows what the average computer access time might be for different strategies. An illustration of a diagram of the effectiveness of using different strategies is given. The results of the work can be practically useful in creating cyber-physical systems and optimizing their functioning.

Keywords: information array, cyber-physical system, redundancy strategies, modeling of control processes, access time.

For citation: Avetisyan T.V., Korotkevich S.I., Pitolin M.V. Modeling of information management processes arrays in cyber-physical systems. *Modeling, Optimization and Information Technology.* 2025;13(4). (In Russ.). 2025;13(4). URL: https://moitvivt.ru/ru/journal/pdf?id=2139 DOI: 10.26102/2310-6018/2025.51.4.067

Введение

При использовании на практике киберфизических систем есть вероятность возникновения ситуации, когда в них разрушаются программные модули и информационные массивы. Это может привести к тому, что в выходных результатах таких систем будут ошибки [1, 2]. При этом будет увеличиваться время, которое требуется для того, чтобы решать задачу [3]. Тогда необходимо использовать подходы, базирующиеся на резервировании.

Можно отметить такие стратегии, связанные с резервированием информационных массивов внутри киберфизических систем.

I. Для информационных массивов происходит выделение копий различных блоков, в которых содержится информация. Предположим, что в киберфизической системе произойдет разрушение основного массива в результате того, что осуществлено внешнее воздействие. В таком случае его первая копия будет применяться в дальнейшем. Если внешние воздействия приведут к тому, что она будет разрушена, необходимо применять следующую копию и т. д.

II. Внутри киберфизической системы можно учитывать то, каким образом она организована, если осуществляется процесс обновления информационных массивов. В таких случаях для подлежащего рассмотрению массива с точки зрения его копий ведется анализ по его предысториям.

Предположим, что массив, который применяется в текущих условиях, будет разрушен. В таком случае реализуется процесс его восстановления. При этом учитываются данные по предыдущему массиву, а также массиву, в котором произошли изменения.

Предыдущая версия информационного массива может быть использована для того, чтобы его восстановить, если в нем произойдут процессы разрушения.

Может быть вариант, при котором используется архив информации. Происходит хранение основного массива, который связан с дубликатами, относящимися к пользователю, чтобы их непосредственным образом применять, когда это необходимо.

Тогда, чтобы организовать работу, можно опираться на такие две стратегии:

II.1. Копии информационных массивов, относящиеся к пользователям, будут получаться на основе дубликата с уровнем m. В случае разрушения дубликата информационного массива в киберфизической системе, будет его восстановление при помощи дубликата с уровнем $m-1$ или для $m+1$ на базе оригинальных данных. На следующем шаге реализуется попытка, связанная с тем, что должна быть получена еще одна копия. При этом необходимо учитывать, что нет возможностей для использования копий информационных массивов в киберфизической системе, которые были получены как дубликаты.

II.2. В ходе реализации процессов обработки данных для различных пользователей реализуется получение копий с учетом того, какой будет дубликат информационного массива с уровнем m. Любые из сохраненных копий могут быть применены для того, чтобы по дубликату осуществлять восстановление, если он разрушен.

III. Использование смешанной стратегии. В таком случае по текущему информационному массиву в киберфизической системе происходит создание его копий и реализуется хранение заданного числа предысторий. То, как используются и восстанавливаются информационные массивы, осуществляется аналогично предыдущим стратегиям. При этом вначале будут применяться копии, если будет разрушение информационного массива [4].

Целью данной работы является изучение особенностей различных стратегий для управления информационными массивами в киберфизических системах.

Материалы и методы

Когда происходит резервирование в киберфизической системе, необходимо ориентироваться на время обработки заданий. Проведем оценку характеристикам резервирования.

Стратегия I. Ее можно применять для того, чтобы вести анализ по массивам с постоянными и изменяющимися данными. На Рисунке 1 можно увидеть иллюстрацию работы системы, если применяется такая стратегия. Происходит резервирование основного массива на основе копий $F_{01}, F_{02}, \dots, F_{0k}$. Будем считать, что p является вероятностью того, что не произойдет процесс разрушения оригинала в течение единичного интервала времени, когда осуществляется его применение.

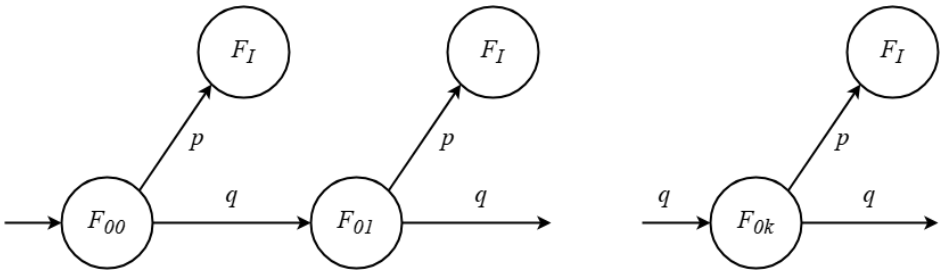

Рисунок 1 – Иллюстрация работы системы при применении стратегии I
Figure 1 – Illustration of how the system will operate when strategy I is applied

Тогда вероятность разрушения подобного массива будет определяться на основе выражения $q = 1 - p$. Исходим из работоспособности информационного массива и его копий к тому моменту, когда будет их применение. Если будет наблюдаться разрушение копии F_{01}, в рамках определенного единичного временного интервала, тогда в следующем единичном временном интервале будет применение следующей копии F_{02}. Это продолжается и для последующих копий [5, 6].

Символ I в выражениях показывает, что будет применяться стратегия резервирования I. Проведем анализ по временным характеристикам, которые относятся к стратегии I.

Пусть, если требуется сформировать k копий, требуется общее время $E[T_I{}^{(1)}] = k\tau$. При этом по одной копии будет время создания τ. Если требуется определение в ходе решения задачи среднего времени решения, когда существует k копий, с учетом успешности решения задачи, то ее результат представляется так:

$$E[T_1^{(2)}] = \theta p^{-1}[1 - q_{k+1}[1 + (k+1)p]], \quad (1)$$

при этом θ показывает время, которое требуется для того, чтобы задача была решена.

Если требуется определение в ходе решения задачи среднего времени решения, когда неважно, насколько оно успешно, то ее результат представляется так:

$$E[T_1^{(3)}] = \theta p^{-1}[1 - q_{k+1}]. \quad (2)$$

Тогда при оценке среднего планируемого времени, которое необходимо для того, чтобы иметь доступ к киберфизической системе с учетом стратегии I приходим к следующему выражению:

$$E[T_1] = E[T_1^{(1)}] + E[T_1^{(1)}]. \quad (3)$$

Стратегия II. Ее можно рассматривать с учетом того, что применяется модель, которая связана с классической задачей, в которой анализируется разрушение информационного массива. На Рисунке 2 дана иллюстрация того, как будет работать система, когда применяется стратегия II.

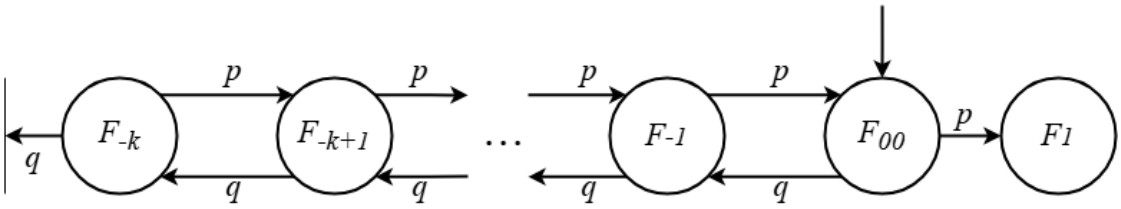

Рисунок 2 – Иллюстрация работы киберфизической системы при стратегии II
Figure 2 – Illustration of the operation of the cyber-physical system with strategy II

Например, внутри киберфизической системы для начального момента времени можно выделить k предысторий, а также массивов изменений $F_{-1}, F_{-2}, \dots, F_{-k}$ в основном массиве F_{00}. При этом обновленный массив будет формироваться в течение нескольких итераций в течение заданного фиксированного времени с учетом определенной вероятности p. В свою очередь, есть обратное действие – разрушение информационного массива. Для него вероятность разрушения равна $q = 1 - p$.

Киберфизическая система функционирует обычным [5, 6] образом пока не произойдет процесс разрушения в оригинале F_{00}, а также по k его предысториям.

В ходе осуществления процессов моделирования точка в гиперпространстве может быть сопоставлена с процессом обновления внутри киберфизической системы информационных массивов. Координаты этой точки соответствуют значениям параметров киберфизической системы в дискретный момент времени.

Обновление информационных массивов также можно связать со случайным движением точки в гиперпространстве в определенную сторону при наблюдении в дискретные моменты времени.

При анализе киберфизической системы можно исходить из того, что q_z соответствует вероятности того, что реализуется процесс разрушения в основном массиве и для его k предысторий [7]. Процессы обновлений по основному массиву имеют соответствующую вероятность p_z.

Можно показать, что при $z = 1$ будет справедливо равенство $q_1 = pq_2 + q$, при $z = k + 1$ будет справедливо $q_k + 1 = pq_k$.

Тогда для граничных условий $q_0 = 1$ и $q_{k+2} = 0$, с учетом того, что $p \neq q$, решение представляется таким образом:

$$q_z = [(q/p)^{k+2} - 1] - 1[(q/p)^{k+2} - (q/p)^z]. \quad (4)$$

Проведем анализ по временным характеристикам, которые относятся к стратегии II в ходе реализации процессов резервирования в киберфизической системе. С тем, чтобы определить среднее время функционирования киберфизической системы [8] до того, как обновляется основной массив F_{00}, а также до того, как будет разрушен основной информационный массив и k его предысторий, будем использовать метод производящих функций [7, 8].

Когда для продолжительности работы киберфизической системы можно найти величину математического ожидания с конечной величиной, то можно провести определение среднего времени для того, чтобы обновить основной информационный массив $E[T_{II}^{y}]$, среднего времени для того, чтобы успешным образом обновить основной массив и различных его предысторий $E[T_{II}^{P}]$, а также среднего независимого времени доступа к киберфизической системе $E[T_{II}]$.

Выражения для их определения – следующие:

$$\begin{gathered} E[T_{II}^{y}] = q^{-1}pC(A^{k+2} - B^{k+2})^{-2}[(k+2)(A^{k+2} + B^{k+2})(A^{k+1} - B^{k+1}) - \\ -(k+1)(A^{k+2} + B^{k+2})(A^{k+1} - B^{k-1})]\theta, \\ E[T_{II}^{P}] = (qp^{-1})^{k+1}C(D^{k+2} - E^{k+2})^{-2}[(k+2)(D^{k+2} + E^{k+2})(D-E) - \\ -(D^{k+2} - E^{k+2})(D+E)]\theta, \\ E[T_{II}] = (\frac{\theta}{q-p})(k+1-\frac{(k+2)(qp^{-1})^{k+1}}{1-(qp^{-1})^{k+2}}), \end{gathered} \quad (5)$$

при этом $A = (2q)^{-1}[1 + (1-4pq)^{0,5}], B = (2q)^{-1}[1 + (1-4pq)^{0,5}], C = (1-4pq)^{-0,5}$, $D = (2q)^{-1}[1 + (1-4pq)^{0,5}], E = (2q)^{-1}[1 + (1-4pq)^{0,5}]$.

Рассмотрим стратегию II.1. Оригинальный информационный массив характеризуется дубликатами, в которых есть m уровней. Копии, которые предназначены для пользователей, будут формироваться на основе дубликата, который относится к уровню m. Когда он будет разрушен, то происходит процесс его восстановления на основе дубликата с уровнем $m-1$. Затем опять рассматривается возможность для того, чтобы сформировать копию для пользователей [8, 9].

Надежность стратегии связана с рассмотрением вероятности того, что не будет наблюдаться разрушение в оригинальном информационном массиве, когда получены k копий:

$$p_{II-1} = \prod_{i=1}^{k}(1 - Q_i), \quad (6)$$

при этом Q_1 соответствует вероятности разрушения оригинального информационного массива, когда будут получены *i* копий от пользователей.

Если $Q_i = Q$, то $p_{II-1} = (1-Q)^k$. Вероятность того, что произойдет разрушение [9] оригинального массива в киберфизической системе, когда будет получена одна копия, определяется следующим образом:

$$Q = 1 - p(m^{m+2} - q^{m+2}) - 1(p^{m+1} - q^{m+1}). \quad (7)$$

Тогда

$$P_{II-1} = [p(p^{m+2} - q^{m+2}) - 1(p^{m+1} - q^{m+1})]k. \quad (8)$$

Проведем анализ по временным характеристикам, которые относятся к стратегии II.1.

Чтобы определить среднее время, которое требуется для того, чтобы обеспечить получение k копий пользователями, необходимо опираться на следующее выражение:

$$E[T_{II-1}^{y}] = (pq^{-1})C(A^{m+2} - B^{m+2}) - 2[(m+2)(A^{m+2} - B^{m+2}) \times \\ \times (A^{m+1} - B^{m+1}) - (m+1)(A^{m+2} - B^{m+2})(A^{m+1} - B^{m+1})\theta k, \quad (9)$$

где $A = (2q)^{-1}[1 + (1 - 4pq)^{0,5}]$, $B = (2q)^{-1}[1 - (1 - 4pq)^{0,5}]$, $C = (1 - 4pq)^{0,5}$.

Чтобы определить значение среднего времени, соответствующего разрушению оригинального информационного массива в киберфизической системе, а также всех его дубликатов, необходимо опираться на следующее выражение:

$$E[T_{II-1}^{P}] = \sum_{i=0}^{k-1}(1-Q)^{i}\ \ Q\{iE[T_{II-1}^{y}] \cdot k - 1 + E[T^{p}]\} = Q^{-1} \cdot (1 - 1 - Q)^{k} \ - \\ -kQ(1-Q)^{k+1}E[T_{II-1}^{y}] \cdot k^{-1} + E[T^{P}](1 \leftarrow Q)^{k} \ \leftarrow kQ^{k+2}), \quad (10)$$

где $E[T^{p}] = (p^{-1}q)^{m+1}C(D^{m+2} - E^{m+2})^{-2}[(m+2)(D^{m+2} + E^{m+2})(D-E) - (D^{m+2} - \\ -E^{m+2})(D-E)\theta]$, $D = (2p)^{-1}[1 + (1 - 4pq)^{0,5}]$, $E = (2q)^{-1}[1 - (1 - (4pq))^{0,5}]$.

Рассмотрим стратегию II.2. Если будет происходить разрушение дубликата информационного массива с уровнем m, то вероятность реализации его восстановления определяется следующим образом:

$$P_{II-1} = 1 - \frac{\{(qp^{-1})^{m+k+1} - (qp^{-1})^{m+1}\}}{\{(qp^{-1})^{m+k+1} - 1\}}. \quad (11)$$

Для того, чтобы по заданному числу пользователей найти среднее время поступления к ним информационных массивов в киберфизической системе, необходимо использовать выражение:

$$E[T_{II}^{y}] = (\frac{p}{q})^{k}\ C(A^{m+k+1} - B^{m+k+1})^{-2}[(m+k+1)(A^{m+k+1} + B^{m+k+1}) \times \\ \times (A^{m+1} - B^{m+1}) - (m+1)(A^{m+k+1} - B^{m+k+1})(A^{m+1} + B^{m+1})]\theta. \quad (12)$$

Рассмотрим стратегию III. Иллюстрация работы киберфизической системы в рамках указанной стратегии показана на Рисунке 3. Будет реализовываться создание копии, которая соответствует основному массиву F_{00} [10, 11]. Помимо этого, соответствующее число предысторий будет сохраняться. Подобно стратегиям I и II осуществляется решение задачи резервирования информационных массивов.

Вероятность того, что задача успешным образом решена в данной стратегии: $P_{III} = 1 - \frac{q^{x+1}(q^{y}(q-1))}{q^{y+2} - p^{y+2}}$.

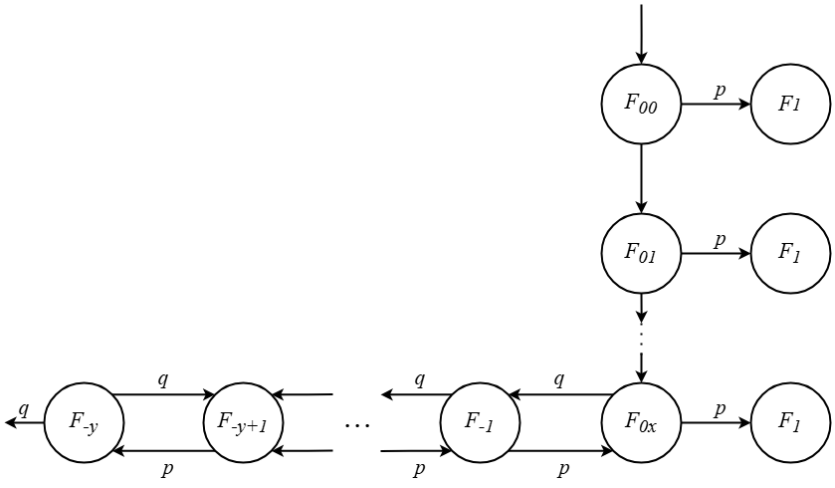

Рисунок 3 – Иллюстрация работы киберфизической системы при стратегии III
Figure 3 – Illustration of the operation of the cyber-physical system with strategy III

Если считать, что число копий массива в массиве F_{00} будет x, а число предысторий будет y, то среднее независимое время доступа к киберфизической системе $E[T_{III}]$ определяется таким образом:

$$E[T_{III}] = x\tau + \theta p(1-q^x) + (\frac{\theta q^x}{q-p})(y+1-(y+2)(1-\frac{(qp^{-1})_X^{y+1}}{1-(qp-1)^{y+2}})). \quad (13)$$

Рассмотрим возможности оценки коэффициента готовности киберфизической системы.

1. Если время работы системы будет рассматриваться как планируемое время доступа к киберфизической системе, тогда ее коэффициент готовности будет определяться таким способом:

$$A_I^{(1)} = 1-q^k,\ A_{II}^{(1)} = p,\ A_{II-1}^{(1)} = p^k, A_{II-2}^{(1)} = (p^{k+2}-q^{k+2}) - 1p^{k+2}(p-q),\ A_{II}^{(1)} = p. \quad (14)$$

При этом значение нижнего индекса, которое будет при коэффициенте готовности, относится к стратегии, применяющейся для резервирования.

Может быть случай, при котором необходимо найти вероятность того, что в анализируемой системе будет не менее, чем n копий информационного массива в киберфизической системе. При этом $A_I^{(2)} = 1-q^{k+1-n}\cdot A_{II}^{(2)}$ не имеет смысла:

$$\begin{gathered} A_{II-1}^{(2)} = \{1-[(qp^{-1})^{m+2-n} - (qp^{-1})^{m+1}][(qp^{-1})^{m+2-n}-1]-1\}^k, \\ A_{II-1}^{(2)} = \{1-[(qp^{-1})^{m+k+1-n} - (qp^{-1})^{m+1}][(qp^{-1})^{m+k+1-n}-1]\}^{-1}, \\ A_{III-2}^{(2)} = 1-q^{x+1-n}. \end{gathered} \quad (15)$$

Когда оценивается степень готовности киберфизической системы для стратегий II и III, то можно учитывать вероятность того, что система будет содержать не менее, чем n предысторий, соответствующих исправному состоянию системы. Тогда

$$A_{II,III} = p[p^{k+2-n} - q^{k+2-n}]^{-1}[p^{k-n+1} - q^{k-n+1}]. \quad (16)$$

При этом можно указать, что для $x < n$ и $y < n$ готовность, которая соответствует стратегии III, не будет иметь смысла. Это вытекает из того, что если будет сохранена хотя бы одна копия, то тогда будут сохранены все предыстории.

2. Предположим, что есть информация по плотности потока обращений к информационному массиву v. В таком случае вероятность того, что в киберфизической системе будет хотя бы один работоспособный информационный массив по всему времени работы T, определяется так:

$$\begin{gathered} A_I = (1-q^k)^{vT},\ A_{II} = p^{vT}, \\ A_{II-1} = p^{kvT}, \\ A_{II-2} = [(p^{k+2}-q^{k+2})^{-1}p^{k+1}(p-q)]^T, \\ A_{III} = (1-q^x)^{vT}. \end{gathered} \quad (17)$$

При рассмотрении коэффициента готовности [12] можно осуществить оценку вероятности того, что в киберфизической системе будут не менее, чем n копий информационного массива [13], которые работоспособны:

$$A_I = (1-q^{k+1-n})^{vT}, A_{II} = p^{vT},$$
$$A_{II-1} = \{1-[(qp^{-1})^{m+2-n} - (qp^{-1})^{m+1}][(qp^{-1})^{m+2-n}-1]^{-1}\}p^{kvT},$$
$$A_{II-2} = \{1-[(qp^{-1})^{m+k+1-n} - (qp^{-1})^{m+1}][(qp^{-1})^{m+k+1-n}-1]^{-1}\}^{vT},$$
$$A_{III} = (1-q^{x+1-n})^{vT}. \quad (18)$$

Если в качестве оценки коэффициента готовности проводить рассмотрение вероятности того, что в анализируемой киберфизической системе будет не менее, чем n предысторий, являющихся работоспособными (для стратегий II и III), то

$$A_{II} = \{p[p^{k+2-n} - q^{k+2-n}]^{-1}[p^{k+1-n} - q^{k+1-n}]\}^{vT},$$
$$A_{III} = \{1-[q^{y+2-n} - p^{y+2-n}]^{-1}[q^{k-n+1}(q-p)]\}^{vT}. \quad (19)$$

В случае, когда $y > n$, A_{III} не будет иметь смысла.

Результаты и обсуждение

Проведем сравнение стратегий резервирования для информационных массивов внутри киберфизических систем. Пусть p – это вероятность сохранения информационного массива. На Рисунке 4 продемонстрированы результаты оценки среднего времени для того, чтобы обновить основной информационный массив $E[T]$ в зависимости от p для разных стратегий. На Рисунке 5 дана демонстрация по тем областям, в которых значение p будет максимальным для соответствующей стратегии в зависимости от времени решения задачи θ.

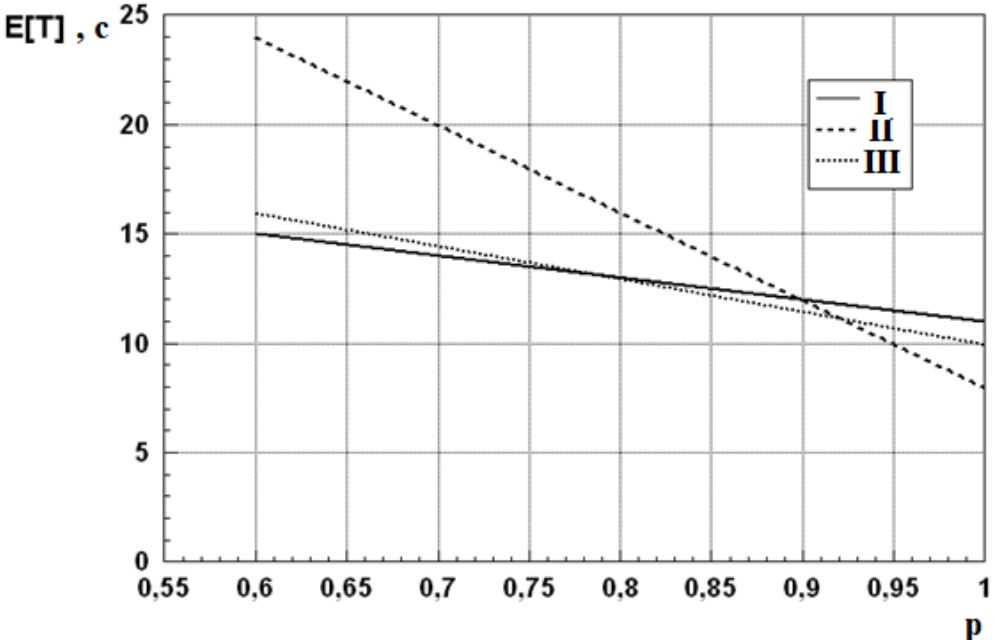

Рисунок 4 – Иллюстрация зависимости среднего времени доступа к киберфизической системе при различных стратегиях

Figure 4 – Illustration of the dependence of average access time to the cyber-physical system under different strategies

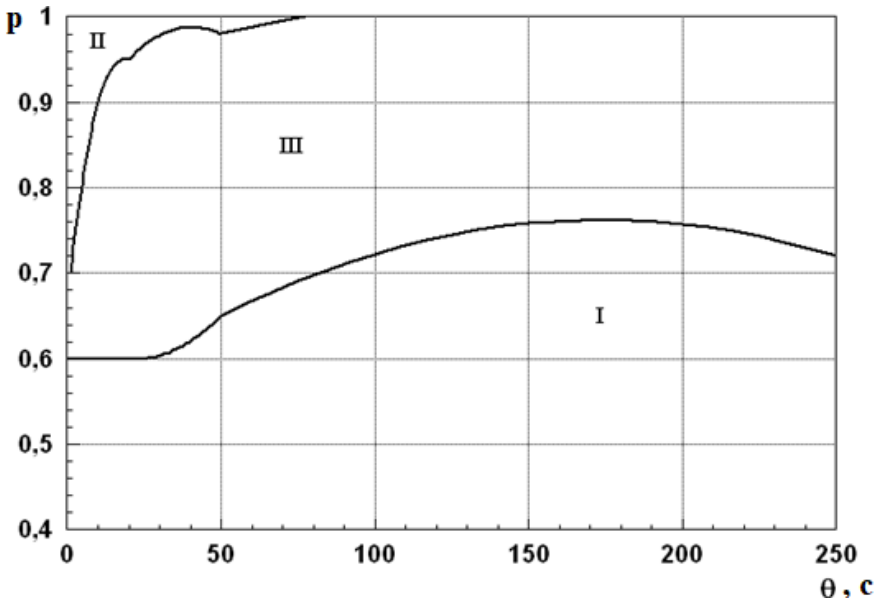

Рисунок 5 – Иллюстрация диаграммы эффективности применения разных стратегий (I, II и III)
Figure 5 – Illustration of the effectiveness diagram for the application of different strategies (I, II, III)

Заключение

В работе проведена разработка моделей функционирования информационных массивов в киберфизической системе на основе разных стратегий. Могут учитываться копии информационного массива, его предыстории, также может применяться смешанная стратегия. На основе рассмотренных подходов были получены результаты оценки характеристик по стратегиям резервирования, если рассматриваются разные параметры в киберфизической системе. Результаты работы могут быть использованы при проектировании киберфизических систем с учетом заданных требований по ресурсам.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Аветисян Т.В., Львович Я.Е., Преображенский А.П., Преображенский Ю.П. Исследование возможностей оптимизации процессов управления киберфизическими системами. *Информационные технологии и вычислительные системы*. 2023;(2):96–105. https://doi.org/10.14357/20718632230210
   Avetisyan T.V., Lvovich Ya.E., Preobrazhensky A.P., Preobrazhensky Yu.P. Investigation of the Possibilities of Optimizing the Management Processes of Cyberphysical Systems. *Journal of Information Technologies and Computing Systems*. 2023;(2):96–105. (In Russ.). https://doi.org/10.14357/20718632230210
2. Львович Я.Е., Преображенский А.П., Преображенский Ю.П. Киберфизические системы – основные направления развития. *Вестник Воронежского института высоких технологий.* 2022;16(2):90–92.
   Lvovich Ya.E., Preobrazhensky A.P., Preobrazhensky Yu.P. Cyber-Physical Systems – The Main Directions of Development. *Bulletin of the Voronezh Institute of High Technologies.* 2022;16(2):90–92. (In Russ.).
3. Липатов А.Г. Возможности использования искусственного интеллекта для управления большими информационными массивами данных Big Data. *Инновации и инвестиции.* 2023;(5):187–189.
   Lipatov A.G. Possibilities of Using Artificial Intelligence to Manage Large Information Arrays of Big Data. *Innovation and Investment.* 2023;(5):187–189. (In Russ.).

4. Литвяк Р.К. Модели оптимизации резервирования информационных массивов и программных модулей в информационных системах. В сборнике: *Информационные и измерительные системы и технологии: Сборник научных статей по материалам Международной научно-технической конференции, 01 марта 2016 года, Новочеркасск, Россия.* Новочеркасск: Лик; 2016. С. 183–190.
5. Павельев С.В. Задачи оптимального оперативного резервирования информационных массивов и программных модулей в корпоративных вычислительных сетях, построенных с использованием каналов интернета. *Проблемы управления*. 2006;(3):61–63.
Paveliev S.V. Optimal On-Line Backup of Information Arrays and Software Modules in Corporate Networks Based on Internet Channels. *Problemy upravlenia*. 2006;(3):61–63. (In Russ.).
6. Семенов В.В., Арустамов С.А. Обобщённая модель функционирования киберфизических систем, учитывающая риски нарушений информационной безопасности. *Научно-технический вестник Поволжья*. 2020;(9):67–70.
Semenov V.V., Arustamov S.A. Generalized Model for Cyber-Physical Systems Functining That Takes into Account Risks of Information Security. *Scientific and Technical Volga Region Bulletin.* 2020;(9):67–70. (In Russ.).
7. Фатин А.Д. Построение модели адаптивности киберфизических систем: функционирование и детектирование. *Вопросы кибербезопасности*. 2024;(2):36–43.
Fatin A.D. Building a Model of Adaptability of Cyberphysical Systems: Operation and Detection. *Voprosy kiberbezopasnosti.* 2024;(2):36–43. (In Russ.).
8. Кручинин Д.В. Модификация метода построения алгоритмов комбинаторной генерации на основе применения производящих функций многих переменных и приближенных вычислений. *Доклады ТУСУР*. 2022;25(1):55–60. https://doi.org/10.21293/1818-0442-2021-25-1-55-60
Kruchinin D.V. Modification of the Method for Developing Combinatorial Generation Algorithms Based on the Use of Multivariate Generating Functions and Approximations. *Proceedings of the TUSUR University.* 2022;25(1):55–60. (In Russ.). https://doi.org/10.21293/1818-0442-2021-25-1-55-60
9. Шабля Ю.В., Кручинин Д.В. Модификация метода построения алгоритмов комбинаторной генерации на основе применения теории производящих функций. *Доклады ТУСУР*. 2019;22(3):55–60. https://doi.org/10.21293/1818-0442-2019-22-3-55-60
Shablya Y.V., Kruchinin D.V. Modification of the Algorithm Development Method for Combinatorial Generation Based on the Application of the Generating Functions Theory. *Proceedings of the TUSUR University.* 2019;22(3):55–60. (In Russ.). https://doi.org/10.21293/1818-0442-2019-22-3-55-60
10. Хохлов Н.С., Канавин С.В., Гилев И.В. Модель противодействия угрозам разрушения информации в системах связи специального назначения при деструктивных воздействиях. *Вестник Воронежского института МВД России*. 2023;(1):106–117.
Khokhlov N.S., Kanavin S.V., Gilev I.V. Model of Countering Threats of Information Destruction in Communication Systems for Specia Purpose Under Destructive Impacts. *Vestnik of Voronezh Institute of the Ministry of Interior of Russia.* 2023;(1):106–117. (In Russ.).
11. Еременко И.А., Линкина А.В. Реализация цифровых трендов в контексте индустрии 4.0. *Вестник Воронежского института высоких технологий*. 2022;16(4):58–62.

Eryomenko I.A., Linkina A.V. Implementation of Digital Trends in the Context of Industry 4.0. *Bulletin of the Voronezh Institute of High Technologies.* 2022;16(4):58–62. (In Russ.).

12. Зяблов С.В., Линкина А.В. Информационные платформы как инструмент цифровой трансформации. *Вестник Воронежского института высоких технологий*. 2022;16(4):94–97.
Zyablov S.V., Linkina A.V. Information Platforms as a Tool for Digital Transformation. *Bulletin of the Voronezh Institute of High Technologies.* 2022;16(4):94–97. (In Russ.).
13. Етепнев А.С. Программный комплекс анализа, моделирования и оценки коэффициента готовности системы защиты информации от несанкционированного доступа. *Общественная безопасность, законность и правопорядок в III тысячелетии*. 2021;(7-3):55–59.
Etepnev A.S. Software Package for Analyzing, Modeling, and Evaluating the Availability Factor of an Information Security System Against Unauthorized Access. *Obshchestvennaya bezopasnost', zakonnost' i pravoporyadok v III tysyacheletii.* 2021;(7-3):55–59. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Аветисян Татьяна Владимировна, преподаватель, Воронежский институт высоких технологий, Воронеж, Российская Федерация.
e-mail: vtatyana_avetisyan@mail.ru
ORCID: 0000-0003-3559-6070

Tatiana V. Avetisyan, Lecturer, Voronezh Institute of High Technologies, Voronezh, the Russian Federation.

Короткевич Светлана Ивановна, старший преподаватель, Воронежский государственный технический университет, Воронеж, Российская Федерация.
e-mail: svelachoksveta@mail.ru

Svetlana I. Korotkevich, Senior Lecturer, Voronezh State Technical University, Voronezh, the Russian Federation.

Питолин Михаил Владимирович, кандидат технических наук, доцент, Воронежский институт МВД России, Воронеж, Российская Федерация.
e-mail: pmv_m@mail.ru

Mikhail V. Pitolin, Candidate of Engineering Sciences, Associate Professor, Voronezh Institute of the Ministry of Internal Affairs of Russia, Voronezh, the Russian Federation.

Статья поступила в редакцию 01.12.2025; одобрена после рецензирования 22.12.2025; принята к публикации 26.12.2025.

The article was submitted 01.12.2025; approved after reviewing 22.12.2025; accepted for publication 26.12.2025.