Автоматизация и моделирование в проектировании и управлении. 2024. № 3 (25). С. 65-74.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2024. № 3 (25). P. 65-74.

Научная статья
Статья в открытом доступе
УДК 004.056
doi: 10.30987/2658-6436-2024-3-65-74.

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРОГНОЗИРОВАНИЯ ДЕФИЦИТА ВЫЧИСЛИТЕЛЬНЫХ МОЩНОСТЕЙ НА ЗНАЧИМОМ ОБЪЕКТЕ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Максим Валерьевич Ковалев[1]✉, Виталий Александрович Шкаберин[2], Михаил Юрьевич Рытов[3], Сергей Александрович Шпичак[4]
[1, 2, 3, 4] Брянский государственный технический университет, г. Брянск, Россия
[1] makskovalew@mail.ru, https://orcid.org/0009-0000-2312-2279
[2] vash@tu-bryansk.ru, https://orcid.org/0000-0002-2320-1986
[3] ozikts@yandex.ru, https://orcid.org/0000-0003-1920-4989
[4] frb113@lenta.ru, https://orcid.org/0009-0006-6263-1520

Аннотация. *Целью исследования является формализация процесса прогнозирования дефицита вычислительных мощностей на значимых объектах критической информационной инфраструктуры с помощью функциональной модели. Задача – создание корректной функциональной модели прогнозирования дефицита вычислительных мощностей. Для решения этой задачи используется программный продукт BPwin и методы функционального моделирования. Новизна работы заключается в применении аналитического выравнивания динамических рядов для прогнозирования дефицита вычислительных мощностей на значимых объектах критической информационной инфраструктуры. В результате проведенного исследования была построена функциональная модель процесса прогнозирования дефицита вычислительных мощностей на значимых объектах критической информационной инфраструктуры. Таким образом полученная функциональная модель отражает технологические особенности процесса прогнозирования дефицита вычислительных мощностей и в дальнейшем может быть автоматизирована и применима на значимых объектах критической информационной инфраструктуры.*

Ключевые слова: критическая информационная инфраструктура, прогнозирование дефицита вычислительных мощностей, информационная безопасность, функциональное моделирование, динамические ряды, аналитическое выравнивание динамического ряда

Для цитирования: Ковалев М.В., Шкаберин В.А., Рытов М.Ю., Шпичак С.А. Моделирование процесса прогнозирования дефицита вычислительных мощностей на значимом объекте критической информационной инфраструктуры // Автоматизация и моделирование в проектировании и управлении. 2024. №3 (25). С. 65-74. doi: 10.30987/2658-6436-2024-3-65-74.

Original article
Open Access Article

SIMULATING THE PROCESS OF FORECASTING THE COMPUTING POWER DEFICIT AT A SIGNIFICANT OBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

Maxim V. Kovalev[1]✉, Vitaly A. Shkaberin[2], Mikhail Yu. Rytov[3], Sergey A. Shpichak[4]
[1, 2, 3, 4] Bryansk State Technical University, Bryansk, Russia
[1] makskovalew@mail.ru, https://orcid.org/0009-0000-2312-2279
[2] vash@tu-bryansk.ru, https://orcid.org/0000-0002-2320-1986
[3] ozikts@yandex.ru, https://orcid.org/0000-0003-1920-4989
[4] frb113@lenta.ru, https://orcid.org/0009-0006-6263-1520

Abstract. *The aim of the study is to formalize the process of forecasting the computing power deficit at significant objects of critical information infrastructure using a functional model. The task is to create a correct functional model for forecasting the computing power deficit. To solve this problem, the BPwin software product and functional modelling*

methods are used. The novelty of the work lies in using the analytical alignment of dynamic series to forecast the computing power deficit at significant objects of critical information infrastructure. As the study result, the authors build a functional model of the process of forecasting the computing power deficit at significant objects of critical information infrastructure. Thus, the resulting functional model reflects the technological features of the process of forecasting the computing power deficit and can be automated and applied to significant objects of critical information infrastructure in the future.

Keywords: critical information infrastructure, forecasting the computing power deficit, information security, functional modelling, dynamic series, analytical alignment of dynamic series

For citation: Kovalev M.V., Shkaberin V.A., Rytov M.Yu., Shpichak S.A. Simulating the Process of Forecasting the Computing Power Deficit at a Significant Object of Critical Information Infrastructure. Automation and modeling in design and management, 2024, no. 3 (25). pp. 65-74. doi: 10.30987/2658-6436-2024-3-65-74.

Введение

На этапе эксплуатации системы безопасности значимого объекта критической информационной инфраструктуры может возникнуть дефицит вычислительных мощностей, когда при использовании средств защиты информации основные аппаратные средства не справляются с вычислительной нагрузкой, что приводит к замедлению, а в некоторых случаях невозможности выполнения целевого производственного процесса, или неэффективности, а в некоторых случаях невозможности функционирования средств защиты информации, или к совокупности таких последствий. Наиболее эффективным способом противодействия дефициту вычислительных мощностей является его своевременное выявление с помощью средств прогнозирования и принятие мер по его предотвращению. Прогнозирование дефицита вычислительных мощностей является сложной задачей, решению которой посвящена данная статья.

Безопасности отечественной критической информационной инфраструктуры уделяется большое внимание. Существует Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] и другие нормативные акты, в которых подробно рассмотрена процедура создания системы безопасности для значимых объектов критической информационной инфраструктуры, включающая определение категории [2] и состава мер по обеспечению безопасности [3]. Существуют методики, которые позволяют упростить процедуру категорирования [4] и автоматизировать процесс создания системы безопасности значимого объекта критической информационной инфраструктуры [5]. Однако после создания системы безопасности обязанность по поддержанию ее работоспособности ложится на специалистов по безопасности субъекта критической информационной инфраструктуры [6]. Их действия регламентируются внутренней организационно-распорядительной документацией [7]. Из установленных законом требований к системе безопасности значимого объекта критической информационной инфраструктуры можно сделать вывод о перечне организационно-распорядительной документации, необходимой на объекте. Но методы, с помощью которых специалисты по безопасности решают поставленные задачи, каждый субъект критической информационной инфраструктуры вправе определять самостоятельно [8]. Поэтому часто проблему дефицита вычислительных мощностей решают по факту его возникновения, при отсутствии понимания необходимости его предотвращения и неимением эффективных инструментов его прогнозирования. Что может привести к ущербу от нарушения целевых производственных процессов, возникновения компьютерных инцидентов, а также вследствие возникновения ответственности за неисполнение законодательных требований о защите значимого объекта критической информационной инфраструктуры [9].

Материалы, модели, эксперименты и методы

В статье был использован программный продукт BPwin для моделирования процесса прогнозирования дефицита вычислительных мощностей на значимом объекте критической информационной инфраструктуры. Использовались следующие виды моделей:

– функциональная диаграмма, построенная на основе стандарта IDEF0 для создания модели функций процесса прогнозирования дефицита вычислительных мощностей с последующей декомпозицией;

– диаграмма описания состояний перехода объектов, построенная на основе стандарта IDEF3 для описания состояний перехода объектов в процессе оценки состояния системы безопасности значимого объекта критической информационной инфраструктуры;

– диаграмма потока данных DFD, наглядно отображающая каким образом информация перемещается от задачи к задаче в рамках процесса прогнозирования дефицита вычислительных мощностей [10].

Для построения прогноза возникновения дефицита вычислительных мощностей был использован метод аналитического выравнивания динамического ряда.

Результаты

Во-первых, была построена контекстная диаграмма в нотации IDEF0, которая дает глобальное описание модели процесса прогнозирования дефицита вычислительных мощностей на значимом объекте критический информационной инфраструктуры (рис. 1).

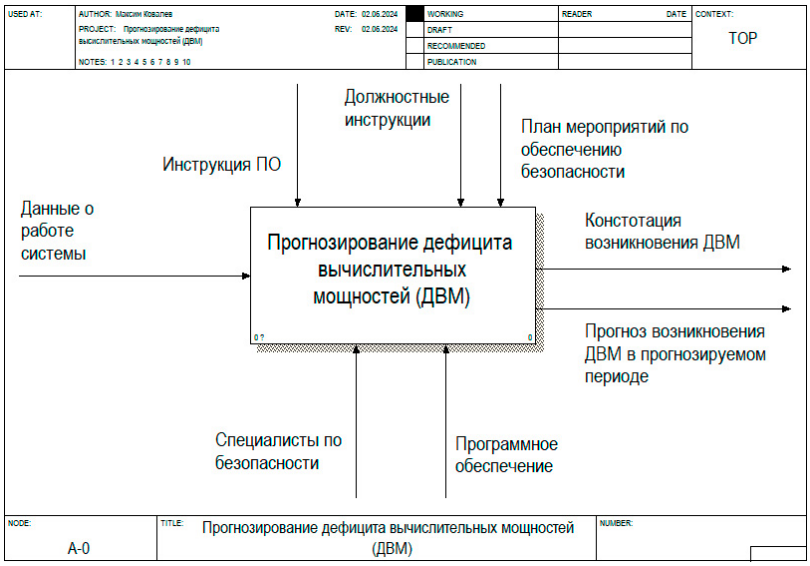

Рис. 1. Модель процесса прогнозирования дефицита вычислительных мощностей для значимого объекта критической информационной инфраструктуры в нотации IDEF0

Fig. 1. The process of forecasting the shortage of computing power for the primary object of critical information load in the IDEF0 notation

Исполнителями в процессе прогнозирования дефицита вычислительных мощностей на объекте критической информационной инфраструктуры, так же как и во всех других процессах, касающихся безопасности объекта, являются специалисты по безопасности [11]. Инструментом для выполнения прогнозирования дефицита вычислительных мощностей служит программное обеспечение, автоматизирующее описанные в данной статье процессы. Разработка такого программного обеспечения является сложной задачей, требующей отдельного детального рассмотрения. В данной статье допускаем, что такое программное обеспечение существует и выполняет свои функции в полном объеме.

В качестве источников управляющего воздействия используются:

– должностные инструкции специалистов по безопасности субъекта, которые включают в себя требования по проведению прогнозирования дефицита вычислительных мощностей на каждом значимом объекте критической информационной инфраструктуры организации и подробное руководство по осуществлению этого процесса;

– инструкция к программному обеспечению, используемому в качестве инструмента для проведения прогнозирования дефицита вычислительных мощностей;

– план мероприятий по обеспечению безопасности, в котором указаны сроки и частота проведения прогнозирования дефицита вычислительных мощностей для каждого объекта критической информационной инфраструктуры в зависимости от специфики его работы.

На вход подаются данные о работе системы за период, достаточный для проведения прогнозирования [12]. На выходе, в зависимости от результатов оценки состояния системы либо констатируется факт наступления дефицита вычислительных мощностей в текущий момент времени, что требует немедленных действий по его устранению, либо прогноз, в котором содержится информация о том, наступит ли дефицит вычислительных мощностей в прогнозируемом периоде.

Далее была проведена декомпозиция контекстной диаграммы (рис. 2).

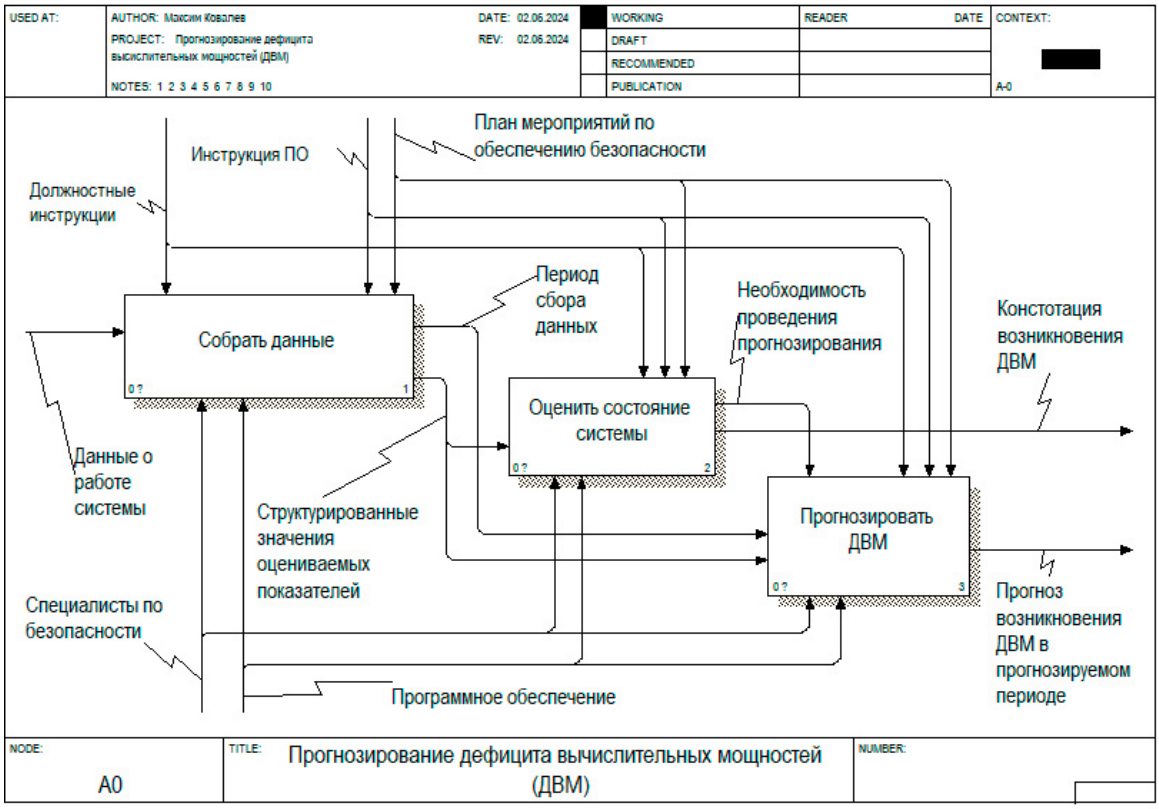

Рис. 2. Декомпозиция процесса прогнозирования дефицита вычислительных мощностей для значимого объекта критической информационной инфраструктуры в нотации IDEF0

Fig. 2. Decomposition of the process of forecasting a shortage of computing power for a significant object of critical information infrastructure in the IDEF0 notation

В результате декомпозиции основного процесса было выделено три подпроцесса: процесс сбора данных; процесс оценки текущего состояния системы; процесс непосредственно построения прогноза.

Процесс сбора данных также был декомпозирован в нотации IDEF0 (рис. 3).

В результате декомпозиции процесса сбора данных были выделены четыре подпроцесса: процесс определения набора измеряемых параметров; процесс определения графика сбора данных; процесс получения данных по графику; процесс структурирования полученных данных.

Набор измеряемых параметров в общем случае включает в себя показатели активности центрального процессора, оперативной памяти и диска каждого из основных аппаратных средств объекта критической информационной инфраструктуры. При необходимости, в случае активного использования графического процессора устройством, его показатели также могут быть включены в набор. Значение каждого из параметров может располагаться в диапазоне от 0 до 100 % и представляет собой процент задействования измеряемого ресурса в момент времени.

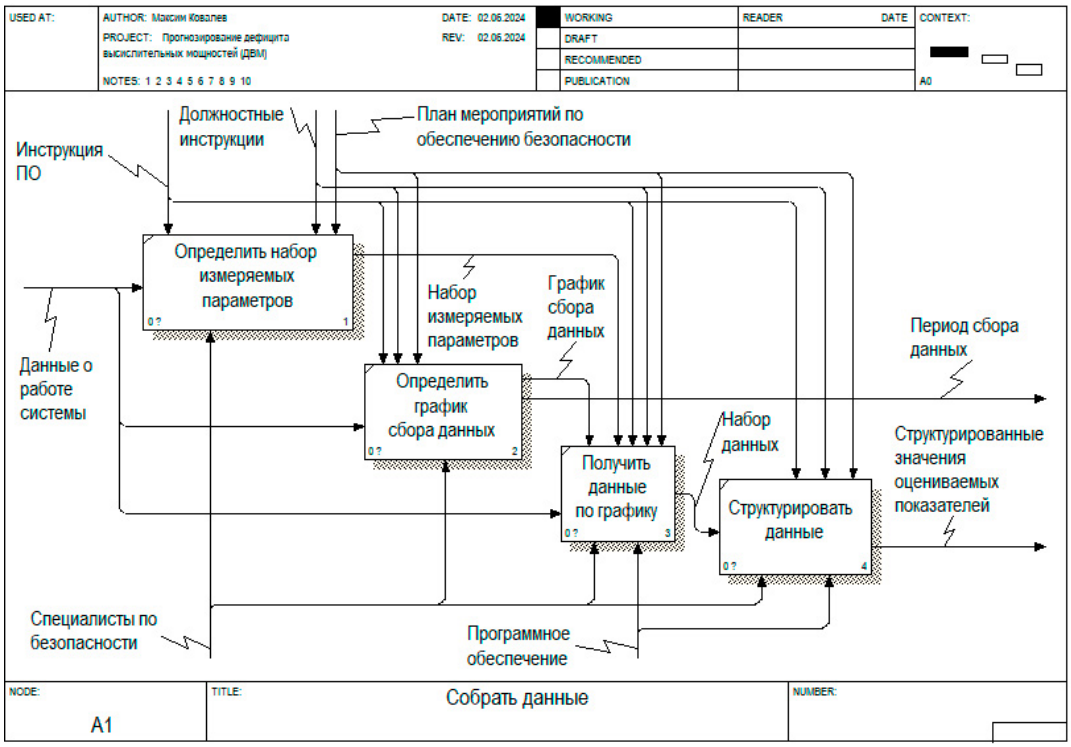

Рис. 3. Декомпозиция процесса сбора данных при прогнозировании дефицита вычислительных мощностей для значимого объекта критической информационной инфраструктуры в нотации IDEF0

Fig. 3. Decomposition of the data collection process when predicting a shortage of computing power for a significant object of critical information infrastructure in the IDEF0 notation

График сбора данных зависит от графика работы объекта критической информационной инфраструктуры [13]. Сбор данных должен проходить с одинаковыми временными интервалами между замерами и между периодами замеров. Периоды замеров также должны быть равны по времени. Период замера зависит от графика работы объекта.

$$T_{\text{сбор}} = (T_1,\ T_2, \dots, T_i);$$
$$T_i = (t_{з1},\ t_{з2}, \dots, t_{зj}),$$

где $T_{\text{сбор}}$ – период сбора данных; $T_1,\ T_2, \dots, T_i$ – периоды проведения замеров; $t_{з1}, t_{з2}, \dots$, $t_{зj}$ – времена замеров.

Получение выбранного набора данных по установленному графику должно реализовываться в автоматизированном режиме с помощью программного обеспечения и контролироваться специалистами по безопасности без их непосредственного участия в процессе сбора, а только корректироваться ими при необходимости.

Собранные данные необходимо структурировать и представить в удобном для дальнейшей обработки виде, что также должно происходить в автоматизированном режиме с помощью программного обеспечения. Данные должны представлять собой набор таблиц, для каждого периода проведения замеров T_i и каждого включенного в набор параметра, содержащих время замера и результат замера (табл. 1).

Таблица 1

Пример таблицы данных для прогнозирования дефицита вычислительных мощностей

Table 1

Example of a data table for forecasting computing power shortages

Период проведения замеров, T_i	Время замера, $t_з$	Значение параметра 1, p_1	Значение параметра 2, p_2	…	Значение параметра n, p_n
T_i	$t_{з1}$	p_{11}	p_{21}	…	p_{n1}
T_i	$t_{з2}$	p_{12}	p_{22}	…	p_{n2}
…	…	…	…	…	…
T_i	$t_{зj}$	p_{1j}	p_{2j}	…	p_{nj}

Поскольку в процессе оценки состояния системы происходит процедура выбора, этот процесс был декомпозирован в нотации IDEF3 (рис. 4).

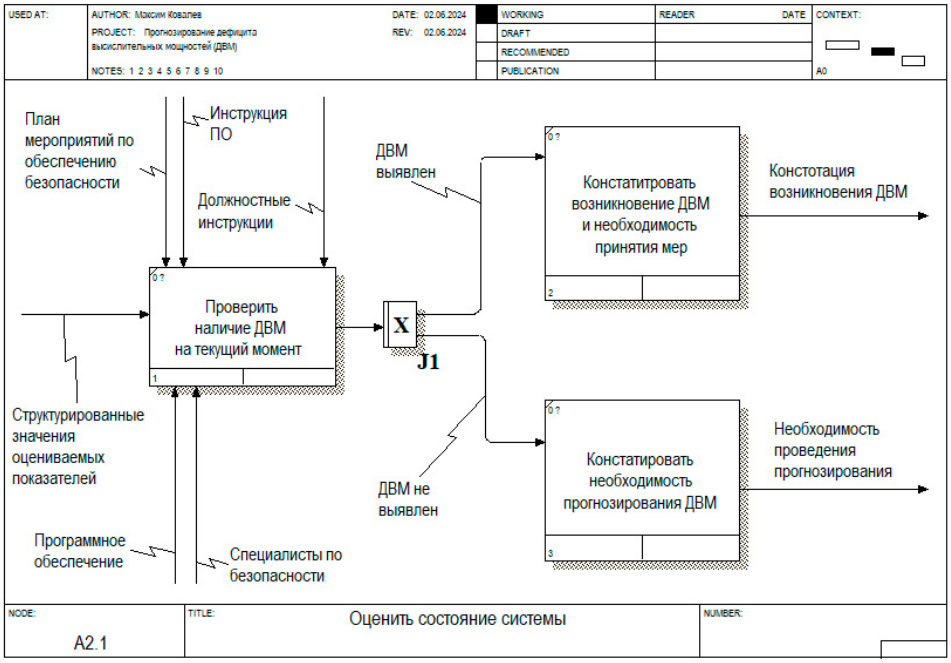

Рис. 4. Декомпозиция процесса оценки состояния системы при прогнозировании дефицита вычислительных мощностей для значимого объекта критической информационной инфраструктуры в нотации IDEF3

Fig. 4. Decomposition of the process of assessing the state of the system when predicting a shortage of computing power for a significant object of critical information infrastructure in IDEF3 notation

В результате декомпозиции процесса оценки состояния системы было выделено три подпроцесса: процесс проверки наличия дефицита вычислительных мощностей на текущий момент; процесс констатации возникновения дефицита вычислительных мощностей и необходимости принятия мер; процесс констатации необходимости прогнозирования дефицита вычислительных мощностей.

При проверке наличия дефицита вычислительных мощностей на текущий момент происходит выявление маркеров наступления дефицита вычислительны мощностей на основе структурированных значений оцениваемых показателей, полученных из предыдущего процесса. Главным маркером наступления дефицита вычислительных мощностей служит количество одновременных пиковых значений оцениваемых показателей в определенный период проведения замеров T_i [14]. Выявление других маркеров дефицита вычислительных мощностей и доказательство их эффективности является сложной задачей, требующей отдельного детального рассмотрения.

Полученное значение маркеров сравнивается с эталонными пороговыми значениями возникновения дефицита вычислительных мощностей. Такие значения могут меняться от объекта к объекту и требуют индивидуального расчета. Определение метода расчета эталонных пороговых значений возникновения дефицита вычислительных мощностей и доказательство его эффективности также является сложной задачей, требующей отдельного детального рассмотрения.

В зависимости от результатов сравнения происходит разветвление процесса. Если дефицит вычислительных мощностей обнаружен в текущем моменте времени, то его прогнозирование не требуется, остается только констатировать его наличие и принять меры для его устранения. Если дефицит вычислительных мощностей не обнаружен в текущий момент, то необходимо прогнозировать его возникновение в будущем.

Процесс непосредственного получения прогноза возникновения дефицита вычислительных мощностей на значимом объекте критической информационной

инфраструктуры должен быть автоматизирован и выполняться средствами программного обеспечения, поэтому он был декомпозирован в виде DFD диаграммы (рис. 5).

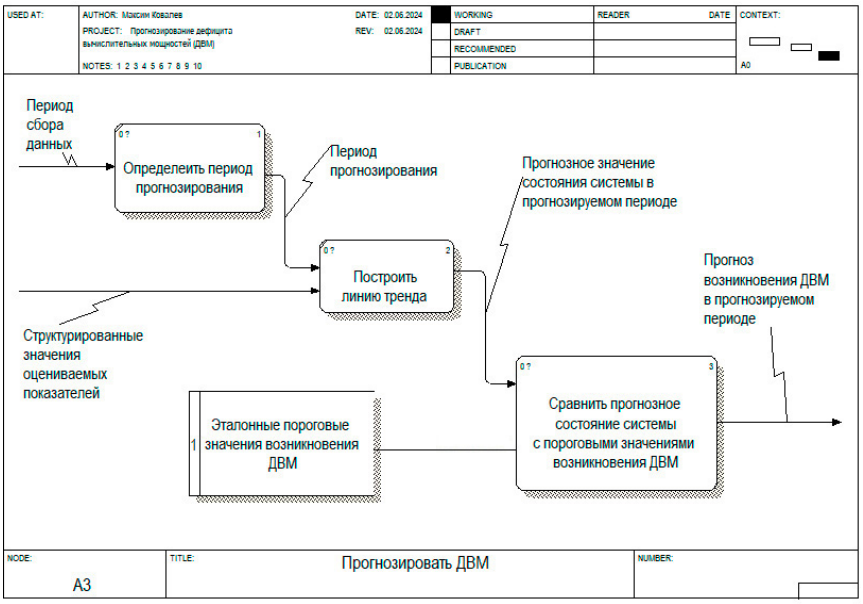

Рис. 5. Декомпозиция процесса прогнозирования при прогнозировании дефицита вычислительных мощностей для значимого объекта критической информационной инфраструктуры в нотации DFD
Fig. 5. Decomposition of the forecasting process when predicting a shortage of computing power for a significant object of critical information infrastructure in DFD notation

В результате декомпозиции процесса непосредственного получения прогноза возникновения дефицита вычислительных мощностей было выделено три подпроцесса: процесс определения периода прогнозирования; процесс построения линии тренда; процесс сравнения прогнозного значения состояния системы с эталонными пороговыми значениями возникновения дефицита вычислительных мощностей.

Определение периода прогнозирования происходит на основании периода сбора данных, так как прогноз можно сделать на период не более 25 % от имеющихся данных. Таким образом определяется максимально возможный период прогнозирования.

$$T_{\text{прогноз}} = (T_{i+1}, T_{i+2}, \dots, T_k);$$
$$k \leq 0{,}25 \cdot i;$$
$$k \in Z,$$

где $T_{\text{прогноз}}$ – период прогнозирования, $T_{i+1}, T_{i+2}, \dots; T_k$ – периоды будущих замеров.

Прогноз строится посредствам аналитического выравнивания динамического ряда. Выравнивание производится с применением уравнения прямой:

$$y_t = a_0 + a_1 t,$$

где y_t – выровненные значения уровней; a_0 – свободный член уравнения; a_1 – коэффициент регрессии; t – период времени.

Параметры уравнения (a_0, a_1) определяются путем составления и решения системы нормальных уравнений методом наименьших квадратов:

$$\sum y = n a_0 + a_1 \sum t;$$
$$\sum yt = a_0 \sum t + a_1 \sum t^2,$$

где n – число уровней ряда.

Для получения уровня линии тренда строится вспомогательная таблица (табл. 2).

Таблица 2

Вспомогательная таблица для получения уровня линии тренда

Table 2

Auxiliary table for obtaining the trend line level

Период проведения замеров, T_i	Количество одновременных пиковых значений оцениваемых показателей, y	Порядковый номер периода проведения замеров, t	yt	t^2	$y_{\text{теор.}}$
T_1	y_1	1	$y_1 \cdot 1$	1	$y_{\text{теор. 1}}$
T_2	y_2	2	$y_2 \cdot 2$	4	$y_{\text{теор. 2}}$
…	…	…	…	…	…
T_i	y_i	i	$y_i \cdot i$	i^2	$y_{\text{теор. }i}$

Прогноз строится посредством подстановки каждого порядкового номера периодов будущих замеров прогнозируемого периода $T_{\text{прогноз}}$ в полученное уравнение. Полученное значение количества одновременных пиковых значений оцениваемых показателей сравнивается с эталонными пороговыми значениями возникновения дефицита вычислительных мощностей. Если полученное значение меньше эталонного, то дефицит в рассматриваемом периоде будущих замеров не наступает. Если значение больше или равно эталонному, то это говорит о возникновении дефицита вычислительных мощностей в рассматриваемом периоде будущих замеров [15].

Заключение

С помощью средств программного продукта BPwin была построена функциональная модель процесса прогнозирования дефицита вычислительных мощностей на значимом объекте критической информационной инфраструктуры. Отдельные процессы модели были декомпозированы в нотациях IDEF0, IDEF3 и DFD. Для прогнозирования дефицита вычислительных мощностей был применен метод аналитического выравнивания динамических рядов. Также по теме исследования были выявлены сложные задачи, требующие отдельного детального рассмотрения, такие как: выявление маркеров дефицита вычислительных мощностей и доказательство их эффективности; определение метода расчета эталонных пороговых значений возникновения дефицита вычислительных мощностей; разработка программного обеспечения на основе созданной функциональной модели.

Полученная функциональная модель является основой дальнейших исследований и разработок для автоматизации процесса прогнозирования дефицита вычислительных мощностей на значимых объектах критической информационной инфраструктуры.

Список источников:

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ // СПС КонсультантПлюс.

2. Постановление Правительства РФ от 08.02.2018 N 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС КонсультантПлюс.

3. Приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической

References:

1. Federal Law No 187-FZ of June 26, 2017 “On the Security of Critical Information Infrastructure of the Russian Federation”; 2018. SPS: ConsultantPlus.

2. Resolution of the Government of the Russian Federation No 127 of February 8, 2018 “On Approval of the Rules for Categorizing Critical Information Infrastructure Objects of the Russian Federation, as well as the List of Indicators of Criteria for the Significance of Critical Information Infrastructure Objects of the Russian Federation and Their Values”; 2018. SPS: ConsultantPlus.

3. Order of the FSTEC of Russia No 239 of December 25, 2017 “On Approval of Requirements for Ensuring the Security of Significant Objects of Critical

информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс.

4. Численное исследование эффективности машинного обучения в задачах прогнозирования категории значимости объектов критической информационной инфраструктуры / М.Ю. Рытов, Ю.Ю. Громов и др. // Приборы и системы. Управление, контроль, диагностика. – 2022. – № 10. – С. 29-44.

5. Аудит и мониторинг состояния объектов информатизации в процессе проектирования комплексных систем защиты информации значимых объектов критической информационной инфраструктуры / М.Ю. Рытов, Н.О. Мусиенко и др. // Приборы и системы. Управление, контроль, диагностика. – 2022. – № 10. – С. 10-18.

6. Приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» // СПС КонсультантПлюс.

7. Постановление Правительства РФ от 15.07.2022 N 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» // СПС КонсультантПлюс.

8. Приказ ФСБ России от 19.06.2019 N 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс.

9. Давыдова Т.И., Синещук Ю.И. Политика информационной безопасности в системе мероприятий защиты информации объектов критической информационной инфраструктуры // Методология развития управления, экономики и образования. – Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2022. – С. 101-111.

10. BPwin [Электронный ресурс] // Менеджмент качества, URL: https://www.kpms.ru/Automatization/BPwin.htm.

11. Беляков М.И., Якунин В.И. Подход к моделированию целенаправленного процесса функционирования системы обеспечения информационной безопасности объекта критической информационной инфраструктуры // Методы и технические средства обеспечения безопасности информации. – 2020. – № 29. – С. 43-44.

12. Прокушев Я.Е., Пономаренко С.В., Шишов Н.В. Моделирование процессов проектирования систем защиты информации в критических информационных инфраструктурах // Computational Nanotechnology. – 2022. – Т. 9, № 2. – С. 45-55.

Information Infrastructure of the Russian Federation; 2017. SPS: ConsultantPlus.

4. Rytov MYu, Gromov YuYu, et al. Numerical Study of the Efficiency of Machine Learning in Problems of Forecasting the Significance Category of Critical Information Infrastructure Objects. Instruments and Systems: Monitoring, Control, and Diagnostics. 2022;10:29-44.

5. Rytov MYu, Musienko NO, et al. Audit and Monitoring of the State of Informatization Objects in the Process of Designing Complex Information Protection Systems for Significant Objects of Critical Information Infrastructure. Instruments and Systems: Monitoring, Control, and Diagnostics. 2022;10:10-18.

6. Order of the Federal Service for Technical and Export Control of Russia No 235 of December 21, 2017 “On Approval of the Requirements for the Creation of Security Systems for Significant Objects of the Critical Information Infrastructure of the Russian Federation and Ensuring Their Functioning”; 2017. SPS: ConsultantPlus.

7. Government Decree of Russia No. 1272 of July 15, 2022 “On Approval of a Model Regulation on the Deputy Responsible for Ensuring Information Security and a Model Regulation on a Subdivision that Ensures Information Security”; 2022. SPS: ConsultantPlus.

8. Order of the Federal Security Service of Russia No. 282 of 2019 June 19 “On Approval of the Procedure for Informing the FSB of Russia About Computer Incidents, Responding to Them, Taking Measures to Eliminate the Consequences of Computer Attacks Conducted Against Significant Objects of the Critical Information Infrastructure of the Russian Federation”; 2019. SPS: ConsultantPlus.

9. Davydova TI, Sineshchuk YuI. Information Security Policy in the System of Information Protection Measures for Critical Information Infrastructure Objects. In: Methodology for the Development of Management, Economics and Education. Penza: Privolzhsky House of Knowledge; 2022. p. 101-111.

10. BPwin. Quality Management. [Internet]. Available from: https://www.kpms.ru/Automatization/BPwin.htm

11. Belyakov M.I., Yakunin V.I. Approach to Modelling the Targeted Process of Operating the Information Security System of a Critical Information Infrastructure Facility. Methods and Technical Means of Ensuring Information Security. 2020;29:43-44.

12. Prokushev Ya.E., Ponomarenko S.V., Shishov N.V. The Modelling of Processes of Design of Information Protection Systems in Critical Information Infrastructures. Computational Nanotechnology. 2022;9(2):45-55.

13. Язов Ю.К., Соловьев С.В. Моделирование значимых объектов критической информационной инфраструктуры в интересах исследования защищенности применяемых в них информационных технологий // Безопасные информационные технологии: Сборник трудов Одиннадцатой международной научно-технической конференции, Москва, 06–07 апреля 2021 года. – Москва: Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет) (Москва), 2021. – С. 363-369.

14. Разработка экспертной системы формирования перечня угроз безопасности информации для объектов КИИ / Д. А. Заколдаев, В. Г. Швед и др. // Защита информации. Инсайд. – 2021. – № 6(102). – С. 25-29.

15. Ларичева Е.А. Применение динамических рядов для анализа и прогнозирования в логистике: Практикум. – Брянск: Брянский государственный технический университет, 2018. – 68 с.

13. Yazov YuK, Soloviev SV. Simulation of Significant Objects of Critical Information Infrastructure in the Interest of Investigating the Security of Information Technologies Used Therein. In: Proceedings of the 11th International Scientific and Technical Conference on Secure Information Technologies; 2021 Apr 06-07; Moscow: Bauman Moscow State Technical University: 2021. p. 363-369.

14. Zakoldaev DA, Shved VG, et al. Development of an Expert System for Forming a List of Information Security Threats for Objects of Critical Information Infrastructure. Information Protection. Inside. 2021;6(102):25-29.

15. Laricheva E.A. Application of Dynamic Series for Analysing and Forecasting in Logistics. Bryansk: Bryansk State Technical University; 2018.

Информация об авторах:

Ковалев Максим Валерьевич
ассистент кафедры «Системы информационной безопасности»

Шкаберин Виталий Александрович
кандидат технических наук, доцент, Первый проректор по учебной работе и цифровизации

Рытов Михаил Юрьевич
кандидат технических наук, доцент, заведующий кафедрой «Системы информационной безопасности»

Шпичак Сергей Александрович
кандидат технических наук, доцент кафедры «Системы информационной безопасности»

Information about the authors:

Kovalev Maksim Valerievich
Assistant at the Department of Information Security Systems

Shkaberin Vitaly Alexandrovich
Candidate of Technical Sciences, Associate Professor, First Vice-Rector for Academic Affairs and Digitalization

Rytov Mikhail Yurievich
Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Security Systems

Shpichak Sergey Alexandrovich
Candidate of Technical Sciences, Associate Professor at the Department of Information Security Systems

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 05.06.2024; одобрена после рецензирования 27.06.2024; принята к публикации 05.07.2024.

The article was submitted 05.06.2024; approved after reviewing 27.06.2024; accepted for publication 05.07.2024.

Рецензент – Еременко В.Т., доктор технических наук, профессор, Орловский государственный университет им. И.С. Тургенева.

Reviewer – Eremenko V.T., Doctor of Technical Sciences, Professor, Orel State University named after I.S. Turgenev.