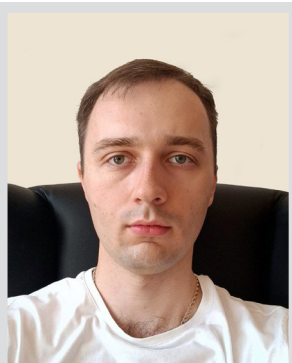


УДК 338.49

DOI: 10.24412/1998-5533-2025-3-462-467

**Обеспечение экономической безопасности цифровых экосистем
с позиции управления данными*****Томуров П.Д.**

Аспирант кафедры бухгалтерского учета,
налогов и экономической безопасности
Поволжского государственного технологического университета
(Марий Эл)

Кудрявцев К.А.

Доктор экономических наук, профессор кафедры бухгалтерского
учета, налогов и экономической безопасности
Поволжского государственного технологического университета,
ведущий научный сотрудник Марийского государственного университета



Актуальность темы исследования определяется необходимостью совершенствования алгоритма доступа к данным для эффективного управления ими и, как следствие, обеспечения экономической безопасности цифровых экосистем. В этой связи цель исследования состоит в обеспечении экономической безопасности цифровых экосистем посредством совершенствования управления данными и интерпретации задачи производственного планирования с учетом усовершенствованного алгоритма доступа к данным. Для достижения указанной цели была исследована сущность понятия «цифровая экосистема», а также изучены теоретические подходы к управлению данными на основе их индексирования. Определена возможность использования модели задачи производственного планирования для отражения связи усовершенствованного алгоритма с экономической эффективностью при ограниченных ресурсах и повышением экономической безопасности цифровых экосистем.

Научная новизна работы состоит в определении цифровой угрозы экономической безопасности, связанной с потерей смысловой целостности данных, устранением указанной угрозы, а также с интерпретацией модели задачи производственного планирования под цифровые экосистемы. Проведенное совершенствование алгоритма поиска искомого узла дерева для эффективного управления данными обуславливает практическую значимость работы. По итогам исследования предложен подход к совершенствованию алгоритма кодирования и декодирования данных для достоверного их восстановления и противодействия определенной цифровой угрозе экономической безопасности экосистем. Показана связь усовершенствованного алгоритма с моделью задачи производственного планирования для определения доходов от выполнения цифровых операций при ограниченных ресурсах.

Ключевые слова: цифровая экосистема, экономическая безопасность цифровых экосистем, управление данными, информационный обмен, индексация данных

* Исследование выполнено при финансовой поддержке Российского научного фонда в рамках научного проекта № 24-28-00062 «Экономическая безопасность субъектов системы тарифного регулирования товарных рынков базовых отраслей: тепловой энергии, водоснабжения и водоотведения».

Для цитирования: Томуров П.Д., Кудрявцев К.А. Обеспечение экономической безопасности цифровых экосистем с позиции управления данными // Вестник экономики, права и социологии. 2025. № 3. С. 462–467. DOI: 10.24412/1998-5533-2025-3-462-467.

Переход к цифровой экономике, характеризующейся интеграцией цифровых экосистем в бизнес-процессы, требует новых подходов к обеспечению экономической безопасности. Цифровые экосистемы как сложные сети взаимодействующих сервисов становятся ключевыми инфраструктурными элементами, однако влияние их на безопасность, в том числе и экономическую, остается малоизученной областью, особенно в аспекте работы с данными, что нельзя сказать об уровне исследования вопроса с позиции защиты от кибератак. Кибератаки являются серьезной угрозой для предприятий [1], компании несут финансовые потери, например: по данным лаборатории Касперского, в 2021 г. «одна кибератака обошлась крупному российскому бизнесу в 695 тыс. долларов, малому и среднему бизнесу – в 32 тыс. долларов» [2]. Другой важной, но малоизученной областью обеспечения экономической безопасности является качество управления данными и возникающие в связи с ним угрозы. По данным исследований разработчика сервисов электронной коммерции АЭРО, в России 72 % компаний фиксируют финансовые потери из-за проблем с ошибками в данных и в целом из-за невозможности формирования качественных данных [3]. В этой связи обеспечение экономической безопасности цифровых экосистем определяется по следующим факторам: устойчивость к кибератакам, эффективность обработки данных, конфиденциальность и целостность данных. Особую значимость приобретают решения, способные противодействовать угрозам скорости доступа к информации. Для реализации данных факторов необходимы меры, обеспечивающие унификацию данных и механизмы, ускоряющие поиск данных внутри цифровой экосистемы.

Таким образом, целью данной статьи является повышение эффективности управления данными в цифровых экосистемах на основе совершенствования алгоритма индексации за счёт модификации механизма поиска данных в хранилище (индексе) для достижения более быстрого доступа к данным и интерпретация задачи производственного планирования применительно к цифровым экосистемам для обеспечения их экономической безопасности.

Интерпретация результатов. В начале исследования нам необходимо определиться с понятием «цифровая экосистема». Согласно Большой Российской Энциклопедии, она определяется как «совокупность элементов среды, обеспечивающих на базе информационных технологий новые способы хозяйствования, включая электронное взаимодействие субъектов, единое цифровое пространство и цифровую культуру»

[4]. Указ Президента РФ от 09.05.2017 г. № 203 трактует цифровую экосистему как «партнёрство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан» [5]. В решении Высшего Евразийского экономического совета от 11.10.2017 г. № 12 цифровая экосистема определяется как «открытая устойчивая система, включающая субъекты цифровой экосистемы (физических, юридических, виртуальных и пр.), а также связи и отношения этих субъектов в цифровой форме на основе сервисов цифровой платформы» [6]. В этой связи в данном исследовании под *цифровой экосистемой* будем понимать комплексную структуру, объединяющую информационные системы, технологические платформы, продукты и сервисы в единую сеть взаимодействующих элементов.

Экономическая безопасность цифровой экосистемы представляет собой «состояние защищенности ключевых экономических процессов и интересов цифровой экосистемы (независимо от ее типа) от внутренних и внешних угроз, обеспечивающее ее устойчивое функционирование и развитие в условиях цифровой трансформации» [7, с. 76]. Выполнение обозначенных в приведенном понятии условий определяется следующими факторами: устойчивость к кибератакам, эффективность обработки данных, конфиденциальность и целостность данных.

Для решения задач обеспечения экономической безопасности цифровых экосистем предлагается комплексный подход, интегрирующий организационные и технологические меры, направленные на:

- «внедрение единого формата данных для пересылки пакетов внутри цифровой экосистемы;
- внедрение механизма индексации данных для ускорения поиска информации внутри баз данных экосистемы по клиентским запросам» [7, с. 76].

Данный подход обеспечивает как защищенность данных, так и эффективность их обработки в рамках экосистемы.

Процессы цифровой трансформации, сопровождающиеся автоматизацией бизнес-процедур, неизбежно генерируют экспоненциальный рост объемов создаваемой и обрабатываемой информации. Управление данными определяется как системный процесс обеспечения их доступности, неизменности и защищенности через внедрение стандартов и контрольных политик [8].

Фундаментальной предпосылкой для управления на основе данных является наличие релевант-

ной, качественной информации в требуемых объемах, что обуславливает необходимость построения комплексной системы администрирования информационными ресурсами [9]. Эффективный обмен данными требует унификации структуры информации, форматов ее представления и принципов функционирования среды взаимодействия на уровне предприятия и его систем. Структура и иерархия обменных данных должны отражать отраслевую, технологическую и организационную специфику, требуемый уровень детализации и степень интеграции в инфраструктуру [10]. Существенную роль играет разработка и использование метаданных – структурированной информации, описывающей ключевые электронные ресурсы, что значительно облегчает их идентификацию, интерпретацию и администрирование.

При разработке системы управления данными ключевыми проблемными областями являются:

- унификация данных: необходимость обеспечения семантической и форматной согласованности;
- безопасность обработки данных: защита больших объемов информации от угроз;
- оперативность доступа: гарантирование своевременного получения релевантных данных для принятия решений.

Использование механизма индексации способствует ускорению обработки запросов и анализу больших массивов данных в цифровых экосистемах, а также минимизации задержек при информационном обмене.

Индексация данных – это «технология, повышающая скорость и эффективность запросов к базе данных» [7, с. 77]. Она обеспечивает повышение скорости поиска данных, снижение нагрузки на вычислительные ресурсы и рост производительности запросов. Значимость индексации данных возрастает для оперативного отслеживания угроз, анализа факторов риска и принятия управленческих решений в режиме реального времени. В контексте цифровых экосистем предпочтительным является применение древовидных индексных структур, обладающих преимуществами в виде масштабируемости и адаптивности к распределенным архитектурам. Соответствующие алгоритмы демонстрируют эффективность как в централизованных, так и децентрализованных средах, где узлы дерева соответствуют физическим серверам экосистемы, обеспечивая отказоустойчивость и производительность. Это напрямую поддерживает критерии масштабируемости и эффективности обработки данных, являющиеся неотъемлемыми условиями обеспечения экономической безопасности.

Алгоритмы кодирования и декодирования обеспечивают двунаправленное преобразование между структурированными блоками данных и байтовыми потоками, гарантируя совместимость сервисов циф-

ровой экосистемы. Рассмотрим данные алгоритмы на примере формата *TLV* [11]. Согласно этим алгоритмам, пакеты данных обладают вложенной структурой, содержащей информацию о наименовании файла, метаданные и хеш-значение для верификации их целостности при получении.

Алгоритм кодирования принимает на вход иерархический блок данных. Первоначально идентификатор блока конвертируется в байтовый дескриптор, который однозначно определяет его семантику. Затем вычисляется длина значения блока – размер его байтового представления. При наличии вложенных элементов процедура рекурсивно применяется к каждому из них. Значение блока сериализуется в байтовый массив с сохранением внутренней структуры. Итоговый результат формируется как конкатенация трех компонентов: байтов идентификатора, байтов длины и байтов значения. Для составных блоков процесс повторяется, формируя многоуровневую вложенность с сохранением автономной целостности каждого компонента.

Алгоритм декодирования выполняет обратное преобразование. На вход подается байтовый поток и вспомогательная метаинформация, описывающая архитектуру блоков. Алгоритм последовательно извлекает сегменты потока: идентификатор декодируется в семантический тег, длина определяет границы значения. Если значение содержит вложенные блоки, процедура рекурсивно повторяется. Критическим этапом является верификация цифрового отпечатка: сравнение хеш-сумм гарантирует отсутствие искажений при передаче. Результатом работы алгоритма является полностью восстановленный структурированный блок, готовый к семантической интерпретации в целевой системе.

Программная реализация этих алгоритмов служит технологическим связующим звеном между сервисами экосистемы, обеспечивая бесшовную интеграцию без потери смысловой целостности данных.

Цифровые экосистемы, обрабатывающие значительные объемы данных, требуют высокопроизводительных механизмов индексации для оперативного выявления угроз и эффективного поиска информации. В качестве базового решения рассматривается алгоритм *CW-tree* – модификация классического В-дерева, дополненная горизонтальными связями между узлами одного уровня и поддержкой многопоточного поиска [12]. Данный алгоритм эффективен для хранения и обработки информации в многопоточных средах современных экосистем. Его архитектура базируется на группировке данных в виде набора специализированных поддеревьев (*CW-поддеревьев*). Каждое поддерево содержит уникальный набор стартовых точек поиска, включающий корневой узел и дополнительные входные вершины. Количество последних прямо пропорци-

онально числу процессорных ядер целевой платформы. Это позволяет организовать параллельную обработку запросов, где каждый вычислительный поток независимо выполняет поиск, начиная с назначенной стартовой вершины, обеспечивая одновременное сканирование верхних и периферийных уровней дерева [12].

Реализация алгоритма включает три этапа:

1. Инициализация стартовых вершин. Формирование базового В-дерева, создание горизонтальных связей между соседними узлами, определение стартовых точек.

2. Построение *CW*-поддеревьев. Заключается в формировании множества вершин и связей для каждого поддерева с последующей их композицией в единую структуру.

3. Алгоритм обхода. Реализация переходов между вершинами для поиска узла с целевым ключом по специальным правилам навигации.

В качестве примера на рисунке 1 показано *CW*-дерево с четырьмя стартовыми вершинами (16, 6, 18, 29), построенное на основе *B-tree* второй степени с высотой, равной 5.

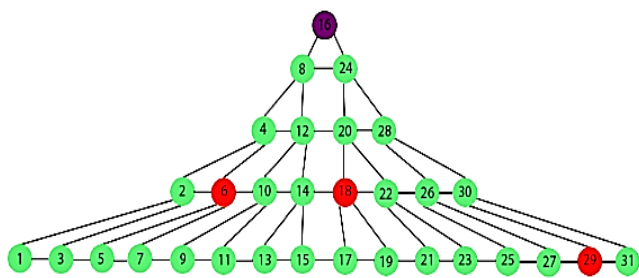


Рис. 1. *CW*-дерево [12, с. 8]

Анализ стандартной функции обхода, изложенной в исследовании В.С. Шевского [12], выявил существенный недостаток: при поиске между удаленными вершинами нижних уровней алгоритм отдает приоритет горизонтальным переходам к соседним узлам, игнорируя возможность вертикального подъема к родительским вершинам. Вместо оптимального маршрута через вышестоящие узлы алгоритм последовательно перебирает соседние вершины на том же уровне, что в контексте экономической безопасности цифровой экосистемы неприемлемо, так как это создаёт большие задержки в обнаружении различных цифровых угроз, связанных со смысловой целостностью данных.

Для устранения этого недостатка была предложена модификация алгоритма, обеспечивающая сбалансированное использование горизонтальных и вертикальных переходов. Предполагается, что каждая вершина будет хранить информацию о целесообразности перехода к родительской вершине перед проверкой дочерних и соседних вершин. Также в каждую вершину добавляется следующая информация:

- индекс корневой вершины *Root*;
- уровень дерева текущей вершины *NodeLevel*;

- степень дерева *p*;
- высота дерева *H*.

Порог подъёма вычисляется по формуле (1):

$$Limit = \begin{cases} NodeLevel, & \text{если } NodeLevel \leq [\log_p(H)] + 1 \\ NodeLevel - 1, & \text{если } NodeLevel > [\log_p(H)] + 1 \end{cases}$$

где *NodeLevel* – уровень дерева, на котором находится указатель на вершину. В переменной *p* хранится степень дерева, в *H* – высота.

$$GoUp = true, \begin{cases} \text{Если } cur > Root \text{ И } x < Root \\ \text{Если } cur < Root \text{ И } x > Root \end{cases} \quad (2)$$

Условие формулы (2) нужно для принятия окончательного решения о переходе на уровень выше в дереве. Переменная *cur* обозначает индекс текущей вершины, переменная *Root* – индекс корневой вершины.

Переход будет целесообразным при соблюдении условия:

$$NodeLevel > Limit$$

Если переход целесообразен, начинается проверка условия формулы (2). Если *GoUp* = true, переход к родительской вершине осуществляется.

Усовершенствованный алгоритм представим на рисунке 2. Этапы определения и инициализации дополнительных стартовых вершин и рёбер остаются неизменными.

Для интерпретации экономического эффекта от внедрения разработанного алгоритма древовидной индексации данных применим модель задачи производственного планирования, адаптируя ее под специфику цифровой экосистемы. В рамках данной модели максимизируется совокупный доход от выполнения цифровых операций при ограничениях на ключевые ресурсы, которые используются более эффективно, что повышает уровень экономической безопасности цифровых экосистем.

Целевая функция, которая должна принять максимальное значение:

$$F(x) = c_1 x_1 + c_2 x_2 + \dots + c_n x_n \rightarrow \max \quad (3)$$

где c_j – доход от выполнения одной операции *j*-го типа (платный аналитический запрос для внешнего клиента, экономия от предотвращения одного инцидента кибербезопасности, комиссия с одной успешно проведенной транзакции);

x_j – это количество успешно завершённых цифровых операций *j*-го типа (аналитические запросы к данным, предотвращенные инциденты кибербезопасности благодаря быстрому анализу логов, онлайн-транзакции, обработанные без ошибок и задержек, актуальные и несломанные индексы в системе);

Далее интерпретируем технологическую матрицу и ограничения, которые имеют следующий вид:

$$A = \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \leq b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \leq b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n \leq b_m \end{cases} \quad (4)$$

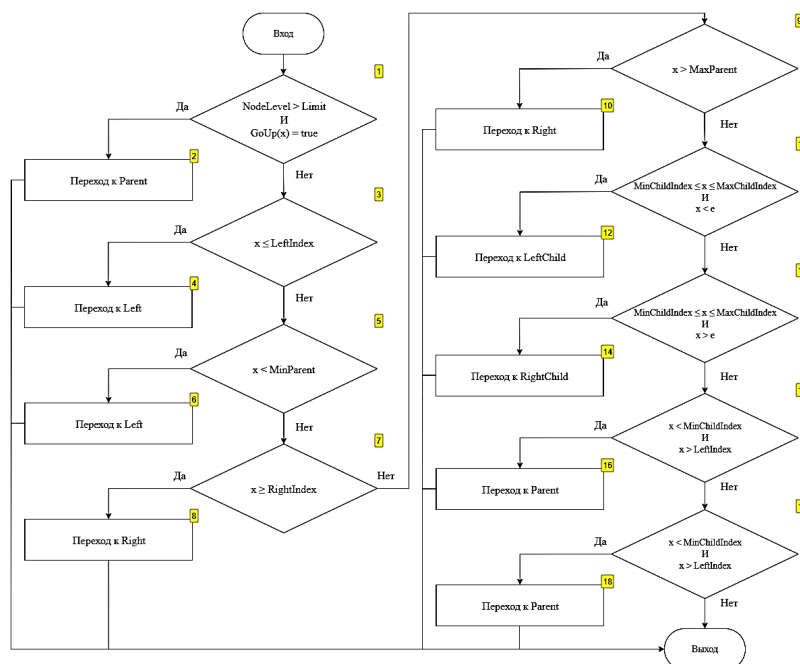


Рис. 2. Модифицированный алгоритм поиска искомого узла дерева

Источник: составлено авторами.

$$x_1 \geq 0, x_2 \geq 0, \dots, x_n \geq 0 \quad (5)$$

a_{ij} – норма расхода трудозатрат i -вида на выполнение одной операции j -го вида;

$i = 1...m$ – трудозатраты (время работы аналитика данных на поиск и агрегацию информации для одного запроса, инженера безопасности на расследование одного потенциального инцидента, системного администратора на поддержание и поиск в хранилищах данных);

b_j – трудозатраты времени на каждый вид j -ой операции;

$j = 1...n$ – индекс вида цифровой операции.

Внедрение разработанного алгоритма не изменяет внешние параметры модели c_j и b_j , но оказывает прямое воздействие на элементы технологической матрицы $A = \{a_{ij}\}$. Предложенный алгоритм (рис. 2) повышает скорость поиска и доступа к данным, что приводит к снижению трудозатрат на выполнение операций, связанных с обработкой информации.

Математически это выражается в уменьшении норм расхода трудозатрат i -вида на выполнение одной операции j -го вида:

$$a_{ij}^{(нов.)} = k_j \times a_{ij}^{(стар.)} \quad (6)$$

k_j – коэффициент эффективности ($0 < k_j < 1$) для операций j -го типа, отражающий степень снижения трудоемкости благодаря применению алгоритма.

Снижение коэффициентов a_{ij} при неизменных правых частях ограничений b_j приводит к следующим результатам:

– максимизируется значение целевой функции $F(x)$;

– увеличивается доля высокодоходных, но ранее чрезмерно трудозатратных операций (за счёт уменьшения норм расходов на операции).

Таким образом, усовершенствованный алгоритм индексации данных выступает не просто инструментом оптимизации, а фактором обеспечения экономической безопасности цифровых экосистем и противодействует цифровой угрозе экономической безопасности в виде потери цифровой целостности данных.

Экономическая безопасность цифровых экосистем в значительной степени зависит от эффективности управления данными. Обеспечение согласованности, целостности, конфиденциальности и высокой скорости доступа к данным в условиях цифровой трансформации являются необходимыми условиями для формирования устойчивой цифровой экосистемы. Для этого необходимо введение единого формата данных, внедрение механизмов, обеспечивающих бесшовный обмен между элементами цифровой

экосистемы. и механизма индексации данных для быстрого поиска информации внутри экосистемы. Объединение алгоритмов кодирования, декодирования и усовершенствованного алгоритма индексации данных обеспечивает совместимость сервисов цифровой экосистемы, улучшает информационный обмен между ними, ускоряет их работу за счёт параллельных вычислений и оптимизации логики обхода поддеревьев (поиска в индексе), обеспечивая экономическую безопасность в цифровых экосистемах с позиции управления данными.

Литература:

1. RED Security: В первом полугодии промышленность оказалась в фокусе внимания APT-группировок // RED Security. URL: <https://redsecurity.ru/news/red-security-v-pervom-polugodii-promyshlennost-okazalas-v-fokuse-vnimaniya-apt-gruppirovok> (дата обращения: 25.08.2025 г.)
2. «Лаборатория Касперского» оценила потери российского бизнеса от кибератак // Ведомости. URL: <https://www.vedomosti.ru/technology/news/2021/10/12/890858-laboratoriya-kasperskogo-otsenila-poteri-rossiiskogo-biznesa-ot-kiberatak> (дата обращения: 25.08.2025 г.)

3. Жуков В. 72 % компаний в России теряют деньги из-за отсутствия качественных данных // РБК Тренды. URL: <https://trends.rbc.ru/trends/industry/66b3beec9a79473791e60849> (дата обращения: 25.08.2025 г.)
4. Лаптев В.А. Экосистема цифровой экономики // Большая Российская Энциклопедия. URL: <https://bigenc.ru/c/ekosistema-tsifrovoi-ekonomiki-042082> (дата обращения: 26.05.2025 г.)
5. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». URL: <http://www.kremlin.ru/acts/bank/41919>
6. Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» // СПС Гарант.
7. Томуров П.Д., Кудрявцев К.А. Комплексный подход к обеспечению экономической безопасности цифровой экосистемы: стандартизация данных и эффективная индексация // Инновационное развитие экономики. 2025. Вып. № 2 (84). DOI: 10.51832/22237984_2025_2_72
8. Репичев А. И., Филатова Е.С. Определение типичных ошибок в работе команды организации при внедрении Agile // Горизонты развития проектного управления: теория и практика: Материалы II Межд. науч.-практ. конф., Москва, 04 марта 2021 г. / Редколл.: С.М. Нечаева [и др.]. М.: Гос. уни-тет управления, 2021. С. 152–154.
9. Цифровая трансформация. Основные принципы. URL: <https://roskachestvo.gov.ru/about/competence/digital/docs/standart.pdf> (дата обращения: 05.08.2025).
10. ГОСТ Р 71720-2024. Формат обмена информацией о производственной системе: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 24.10.2024 г. № 1487-ст: введен впервые: дата введения 2025-07-01 / разработан Ассоциацией «Цифровые инновации в машиностроении» и Федеральным государственным бюджетным учреждением «Российский институт стандартизации». М.: ФГБУ «Институт стандартизации», 2024.
11. Томуров П.Д., Васяева Н.С. Анализ формата TLV для структурированного представления данных // Труды Поволжского государственного технологического университета. Серия: Технологическая. 2024. Вып. 12. С. 35–39.
12. Шевский В.С. Индексирование данных на основе алгоритма CW-tree с применением параллельного чтения данных. URL: <https://moitvvt.ru/ru/journal/pdf?id=905> DOI: 10.26102/2310-6018//2021.32.1.013

Ensuring Economic Security of Digital Ecosystems from the Perspective of Data Management

Tomurov P.D., Kudryavtsev K.A.
Volga State Technological University,
Mari State University

The relevance of the research topic is determined by the need to improve the data access algorithm for effective data management and, as a result, ensuring the economic security of digital ecosystems. In this regard, the purpose of the study is to ensure the economic security of digital ecosystems by improving data management and interpreting the production planning problem taking into account the improved data access algorithm. To achieve this goal, the essence of the digital ecosystem concept was studied, as well as theoretical approaches to data management based on their indexing. The possibility of using the production planning problem model to reflect the relationship of the improved algorithm with economic efficiency with limited resources and increasing the economic security of digital ecosystems was determined. The scientific novelty of the work consists in defining a digital threat to economic security associated with the loss of semantic integrity of data, eliminating this threat, as well as interpreting the production planning problem model for digital ecosystems. The conducted improvement of the search algorithm for the desired tree node for effective data management determines the practical significance of the work. Based on the results of the study, an approach is proposed to improve the encoding and decoding algorithm for data for their reliable recovery and counteraction to a certain digital threat to the economic security of ecosystems. The improved algorithm is shown to be related to the model of the production planning problem for determining revenues from performing digital operations with limited resources.

Keywords: digital ecosystem, economic security of digital ecosystems, data management, information exchange, data indexing