Научная статья
УДК 004.27+004.056
DOI:10.31854/1813-324X-2022-8-3-101-116

Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий

Виталий Владимирович Грызунов[1], viv1313r@mail.ru

[1]Российский государственный гидрометеорологический университет,
Санкт-Петербург, 192007, Российская Федерация

Аннотация: *Сложность обеспечения доступности ресурсов геоинформационных систем обусловлена волатильной структурой системы, неопределенностью задач пользователя и деструктивных воздействий. В настоящей работе предлагаются методы, позволяющие вполовину снизить вероятность риска информационной безопасности, связанного с нарушением доступности ресурсов. Эффект достигается за счет: 1) сохранения требуемой вероятности достижения цели деятельности системой идентификации, не зависимо от силы деструктивных воздействий; 2) за счет агрегирования производительности отдельных физических элементов системы в виртуальные пулы; 3) за счет преобразования внутренних резервов задач пользователей в резервы производительности. Работа методов оценивалась с помощью имитационной модели, разработанной в среде MATLAB.*

Ключевые слова: *геоинформационная система, деструктивные воздействия, доступность ресурсов, идентификация, адаптивное управление*

Ссылка для цитирования: Грызунов В.В. Методы адаптивного управления доступностью ресурсов геоинформационных систем в условиях деструктивных воздействий // Труды учебных заведений связи. 2022. Т. 8. № 3. С. 101–116. DOI:10.31854/1813-324X-2022-8-3-101-116

Methods for Adaptive Resource Availability Management of Geoinformation Systems under Destructive Impacts

Vitaly Gryzunov[1], viv1313r@mail.ru

[1]Russian State Hydrometeorological University,
St. Petersburg, 192007, Russian Federation

Abstract: *The complexity of ensuring the availability of geoinformation systems resources is due to the volatile structure of the system, the uncertainty of user tasks and destructive influences. This paper proposes methods that allow to halve the probability of information security risk associated with the disruption of resource availability. The effect is achieved by: 1) preserving the required probability of achieving the activity goal of the identification system, regardless of the strength of disruptive influences; 2) by aggregating the performance of individual physical system elements into virtual pools; and 3) by converting internal user task reserves into performance reserves. The performance of the methods was evaluated using a simulation model developed in MATLAB environment.*
Keywords: *geoinformation system, destructive impacts, resource availability, identification, adaptive management*

For citation: Gryzunov V. Methods for Adaptive Resource Availability Management of Geoinformation Systems under Destructive Impacts. *Proc. of Telecom. Universities.* 2022;8(3):101–116. (in Russ.) DOI:10.31854/1813-324X-2022-8-3-101-116

Введение

Геоинформационные технологии и геоинформационные системы (ГеоИС) стали неотъемлемыми элементами всеобщей информатизации общества. Согласно [1, 2] основное предназначение ГеоИС – обеспечение управленческих решений в практической и научно-исследовательской деятельности пространственными данными (ГОСТ Р 52438-2005 Геоинформационные системы. Термины и определения). Таким образом, доступность ресурсов ГеоИС является обязательным условием своевременного принятия этих решений. А поскольку ГеоИС становятся распределенными в пространстве-времени, то и сами требуют децентрализованного управления [3].

Новые вызовы, обусловленные резко обострившейся информационной войной, активизировали межгосударственные источники деструктивных воздействий (ДВ) на информационную инфраструктуру РФ. Обеспечение доступности ресурсов ГеоИС в этих условиях является серьезно проблемой, затронутой в [4] и решаемой автором настоящей статьи.

Нарушение доступности, или отказ в обслуживании – DoS (*аббр. от англ.* Denial of Service), как правило, достигается генерацией большого количества задач и/или разрушением структуры и/или функций ГеоИС. С начала специальной военной операции на Украине статистика атак типа «отказ в обслуживании» на объекты информационной инфраструктуры РФ неутешительная – только в одном госсекторе жертвами стали 90 % организаций [*], а число лиц, причастных к нападениям, может превысить 500 000 человек. То есть, атаки также являются распределенными по источникам угроз в сетевом пространстве – DDoS (*аббр. от англ.* Distributed Denial of Service)/

Примечание. Здесь и далее по тексту [*] – ссылка на новостной сайт лаборатории Касперского.

Многофакторные и многоцелевые DDoS-атаки уже давно стали реальностью. Сейчас за базовым уровнем флуда (исчерпания ресурсов сервера или канала) может последовать вполне интеллектуальная атака на перебор паролей или использование серверных уязвимостей. И отследить такую «умную» атаку, чтобы оперативно защититься от нее или от ее последствий, может быть мало реально.

Согласно данным [*] общее количество DDoS-атак за 1 год превысило 450 % (рисунок 1), и непосредственно после начала спецоперации – 3000 % (рисунок 2). При этом средняя длительность атак составила 6716 %, а максимальная – 12090 % от зафиксированных годом ранее (рисунок 3). Следовательно, и угроза нарушения доступности ресурсов ГеоИС увеличивается в разы, а возросшая длительность атак автоматически увеличивает длительность простоя ГеоИС

Рис. 1. Статистика DDoS-атак (Q1 – первый квартал и т.д.)

Fig. 1. DDoS Attack Statistics (Q1 – First Quarter etc.)

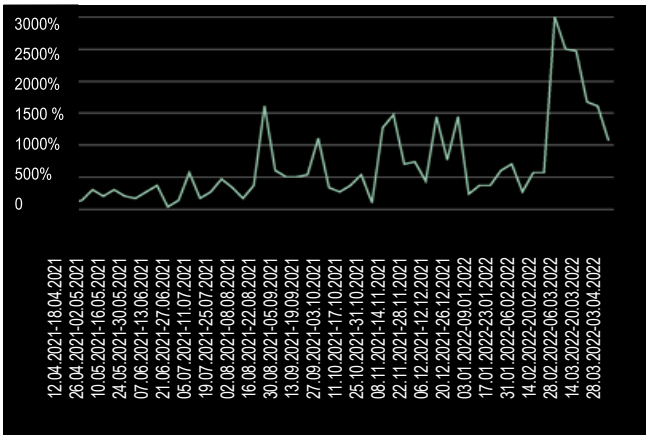


Рис. 2. Статистика еженедельного роста DDoS-атак

Fig. 2. Statistics of Weekly Growth of DDoS Attacks

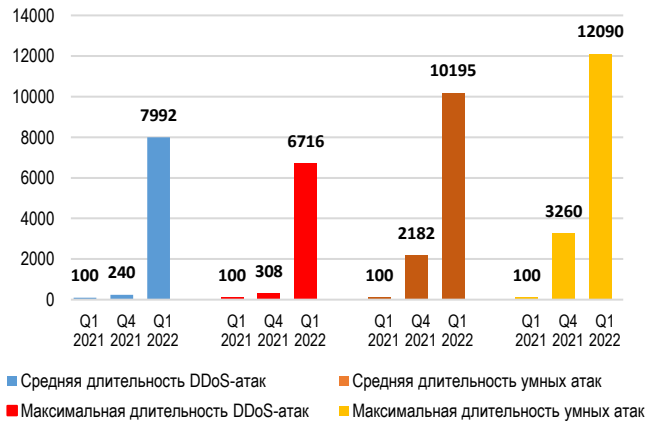


Рис. 3. Длительности DDoS-атак

Fig. 3. Durations of DDoS Attacks

Нарушение доступности особенно опасно тем, что доступность лежит в основе обеспечения других аспектов информационной безопасности (ИБ) – целостности и конфиденциальности. Сказанное формулируется в виде *необходимого и достаточного условия обеспечения ИБ*: «Чтобы обеспечить целостность, конфиденциальность и доступность

в ИС, необходимо и достаточно выделить ресурс для решения штатных задач ИС и только их».

ОГРАНИЧЕНИЕ 1

Нарушитель целостности, конфиденциальности и доступности для достижения своих целей обязательно использует ресурс ИС.

Доказательство

Необходимость. Средства, которые обеспечивают целостность, конфиденциальность и доступность в ИС, являются ее компонентами. Следовательно, для их работоспособности необходимо выделить ресурс ИС.

Достаточность. Нарушая целостность, конфиденциальность и доступность, злоумышленник обязательно использует ресурсы ИС (см. ограничение 1), то есть использует ресурсы ИС в целях, для этого не предусмотренных. Следовательно, если не выделять ресурс ИС на решение задач злоумышленника, а выделять только для штатного использования ИС, то у него не будет ресурса, чтобы нарушить целостность, конфиденциальность и доступность.

Необходимое и достаточное условие доказано. То есть чисто теоретически, если удается создать ИС, в которой каким-то способом реализовано сформулированное условие, то вопросы информационной безопасности в такой ИС не актуальны.

Сформулированное условие отлично согласуется с практикой. Действительно, все системы защиты информации – от простейшего процесса операционной системы, разграничивающего доступ к файлу на основе его атрибутов, до полноценных комплексных систем защиты информации – требуют дополнительного ресурса для своего функционирования.

С другой стороны, действия всех средств защиты информации направлены на обеспечение достаточности сформулированного условия, то есть выделение ресурса ИС только для штатного использования, например: средства аутентификации и средства криптографической защиты информации имеют цель выделить ресурс только разрешенным пользователям, межсетевые экраны и антивирусы – выделить ресурс разрешенным процессам, системы обнаружения атак – обнаружить процессы, использующие ресурсы не в соответствии с целями ИС и т. д.

Если реализуется защита от инсайдеров, это означает, что в состав ИС включается персонал. В этом случае обеспечение достаточности условия реализуется с помощью DLP-систем, работой с персоналом офицерами по безопасности, внедрением организационных мероприятий и т. д. Сказанное верно для всех уровней ИС согласно модели FIST [6].

Настоящее исследование ориентировано на уровни аппаратного и программного обеспечения модели FIST и для описания деструктивных воздействий использует подход, изложенный в [7], согласно которому, с точки зрения обеспечения доступности, не имеет значения, каким именно образом ресурс выведен из строя, а важно, как это отразится в системе. ДВ в ИС выражаются в нарушении ее структуры и/или функций на различных уровнях, например:

– на уровне программного обеспечения, приводящие к истощению адресного пространства (атаки типа Slowloris, SYN / ACK flood, DHCP starvation и т. д.);

– на уровне логической структуры (нарушение штатного режима функционирования ИС путем перегрузки созданных пулов, сбои в системе управления ими, разрушение самих пулов с помощью программных или программно-аппаратных средств и т. п.;

– ДВ уровня физической структуры: выход из зоны видимости мобильных элементов ИС, использование технических средств для несанкционированного доступа, паразитное электромагнитное излучение, потоки отказов или сбоев оборудования, хищение элементов ИС и т. п.

Согласно [7] спецификой ГеоИС, как объекта инфраструктуры, в общем виде является распределенность в пространстве-времени, включение в состав ГеоИС пассивных и активных элементов, которые самостоятельно изменяют структуру и/или функции ГеоИС. ГеоИС обрабатывает все возможные типы данных от текстовых до мультимедиа. В некоторых случаях ГеоИС требует работы в реальном времени. При этом ДВ на ГеоИС имеют неопределенность, описываемую стохастическими процессами, и неопределенность, связанную с агрессивными целенаправленными действиями, которые такими процессами описываться не могут. Опираясь на данные обстоятельства, в работе [3] показано, что в силу неопределенности структуры, функций и проч. проблема обеспечения доступности ресурсов распределенной ГеоИС в условиях ДВ должна решаться средствами теории адаптивного управления. В случае противостояния ДВ методами теории управления формируется множество целей и определяется множество ресурсов. Затем выбирается такой вариант объекта, который по критерию достижимости этих целей окажется лучше всех [8, 9], тем самым речь идет об адаптации ГеоИС к ДВ.

Цель управления (адаптации к ДВ) – достичь и/или поддержать заданное значение показателя эффективности функционирования ГеоИС [10, 11]. Этот показатель обычно формулируется как предоставление некоторого качества обслуживания (QoS, *аббр. от англ.* Quality of Service) [12]. Например, в работе [13] QoS фигурирует как функция экспонен-

циально взвешенной скользящей средней длины очереди и функция сброса. В протоколе MQTT (*аббр. от англ.* Message Queuing Telemetry Transport) QoS оценивается как вероятность прохождения пакета между двумя точками сети.

Можно сказать, что QoS в той или иной степени характеризует доступность всех типов ресурсов ГеоИС на уровне программного и аппаратного обеспечения ГеоИС согласно модели FIST: вычислителей, памяти, каналов связи, устройств ввода-вывода [7].

Анализ существующих подходов

Достижение и/или поддержание заданного QoS в качестве цели управления традиционно реализуется как адаптация программного обеспечения с использованием классических подходов [14], модельного прогнозирующего управления (MPC, *аббр. от англ.* Model Predictive Control) [15] или адаптационных структур на основе PID-регуляторов [16]. Первые два предполагают детерминированное или стохастическое описание объекта управления (ОУ) и возмущающей среды (имеется в виду ДВ), а применение последнего – линейность системы. Выше отмечалось, что специфика ГеоИС не позволяет использовать для описания стохастические и, тем более, детерминированные процессы, поскольку не известен не только механизм выбора из множества альтернатив (множества допустимых ДВ), но само множество альтернатив, из которого осуществляется выбор. Линейность ГеоИС также вызывает сомнения [3]. Все это означает, что необходимы иные подходы адаптации ГеоИС к ДВ.

Так, например, автор в [17] рассматривает интеллектуально-адаптивное управление информационной инфраструктуры предприятия. Управление реализуется в виде централизованной системы, которая за счет распознания угрозы и подключения нужного сценария обработки угрозы обеспечивает доступность ресурсов инфраструктуры, то есть требуемую производительность. Система защиты, в свою очередь, потребляет ресурс системы, следовательно, влияние ее работы на достижение всей системой целей деятельности требует дополнительного исследования.

Отдельно можно выделить работы по самоадаптации Интернета-вещей (IoT, *аббр. от англ.* Internet-of-Things), так как IoT обычно обрабатывает пространственные данные. Метод самоадаптации с акцентом на свойство безопасности рассмотрен на примере IoT, контролирующем работу сердца пациента, в работе [18]. Поскольку от работоспособности системы зависят жизни пациентов, то ее можно причислить к объектам критической информационной инфраструктуры. ДВ являются естественные сбои и отказы устройств, разряд батарей и т. д., то есть они довольно редки, и имеют стохастическую природу, что не вполне адекватно ГеоИС [19]. В работе реализовано управление по состоянию. Адаптация заключается в обнаружении неработоспособного устройства, и перевода системы в следующее состояние согласно правилам.

В [20] предлагается централизованно управляемая архитектура IoT-системы прогнозирования бдительности водителя с использованием Apache Nifi и Raspberry Pi, оптимизирующая загрузку сети. В зависимости от входных данных активируется тот или иной управляющий скрипт.

В исследовании [21] методом систематического обзора литературы (SLR, *аббр. от англ.* Systematic Literature Review) проведен анализ работ самоадаптивных архитектур IoT и сделан вывод относительно оценки управления QoS: обычно это уменьшение передачи данных, времени ожидания и потребления полосы пропускания, – то есть исследователи сосредоточены в первую очередь на оптимизации производительности каналов связи. Выявлено, что QoS изменяется вследствие следующих причин:

1) мобильность клиентов – появление и исчезновение устройств из IoT;

2) динамическая скорость передачи данных – изменение скорости в зависимости от ситуации на устройстве;

3) возникновение важного для устройства события, влекущее изменение его загрузки и/или скорости передачи данных;

4) сбои и обновления прошивки, вызывающие остановку назначенных задач и/или скорость передачи данных;

5) изменения сетевого подключения, выражающееся в изменении скорости или прекращении передачи данных;

6) кибератаки в приложениях IoT, вызывающие нарушение целостности, конфиденциальности и доступности как самих устройств, так и смежных устройств.

Согласно данному исследованию, методы адаптации заключаются в следующем:

– реконфигурация потока данных, имеющая целью сокращение нагрузки на каналы связи, то есть сокращение использования ресурса уровня аппаратного обеспечения модели FIST (устраняет причины 1, 2, 3 и 5). К этому же методу можно отнести введение приоритетов на выполнение задач и выделение ресурсов только приоритетным задачам;

– автоматическое масштабирование сервисов и приложений в центры обработки или ближайшие, с точки зрения маршрутизации, узлы ГеоИС с целью выделить дополнительный ресурс на уровне программного обеспечения модели FIST (устраняет причины 1, 2, 3);

– развертывание и обновление программного обеспечения – полуавтоматическая стратегия, це-

лью которой является сокращение времени простоя ресурсов уровня аппаратного обеспечения модели FIST, вызванного сбоями и отказами по вине аппаратного и программного обеспечения (устраняет причину 5);

– выгрузка решаемых задач при превышении загрузки процессора и/или канала связи на ближайшее устройство (устраняет причины 1–4).

При организации отказоустойчивых IoT [22] были выделены следующие механизмы адаптации:

– репликация процессов на дополнительные элементы IoT по пассивной (элементы подключаются после обнаруженного отказа) или активной (процесс выполняется одновременно с основным) схеме;

– управление сетью посредством разделения на кластеры и выделения их «головы», которая контролирует работоспособность его элементов, рассылая соответствующие запросы;

– распределенный блок восстановления, когда выделяется пара узлов, выполняющих процесс, один из узлов является основным, второй – теневым, результаты выполнения процесса обоими узлами сравниваются, на основе этого принимается решение, был отказ или нет;

– резервирование времени, в котором процесс выполняется дважды на одном и том же узле, после чего результаты сравниваются.

С учетом вышеизложенного, можно сделать следующие предварительные выводы:

– во-первых, целью адаптации является предоставление заданного QoS, то есть обеспечение требуемого уровня доступности производительностей вычислителей, памяти, каналов связи и/или устройств ввода-вывода;

– во-вторых, существующие методы адаптации не решают вопросы информационной безопасности, так как не устраняют причину 6.

Примечание. *Однако, используя обоснованное в начале статьи необходимое и достаточное условие обеспечения ИБ, можно все свести к задаче обеспечения доступности ресурсов.*

– в-третьих, обеспечение QoS зависит от качества идентификации ОУ.

В методах, приведенных выше, обеспечение требуемого уровня QoS идет по пути предоставления функционального и/или структурного резерва ГеоИС. Когда все они исчерпаны, а ДВ продолжаются, целесообразно использовать внутренние резервы [23]. В результате задачи, поставленные перед ГеоИС, решаются не в требуемый, но приемлемый срок, и не с требуемой, но допустимой точностью.

Схематично применение методов обеспечения доступности ресурсов на различных стадиях деградации ГеоИС, вызванных ДВ, можно представить, как показано на рисунке 4.

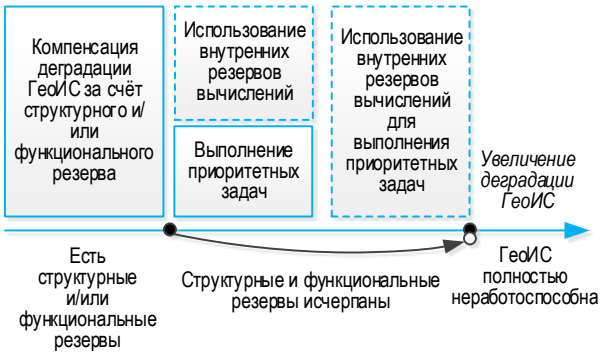


Рис. 4. Схема применения методов обеспечения доступности ресурсов ГеоИС в условиях ДВ на различных стадиях ее деградации

Fig. 4. Application of Methods to Ensure the Availability GeoIS Resources under Conditions of DV at Different Stages GeoIS Degradation

Как видно из рисунка, использование внутренних резервов может применяться совместно с выполнением приоритетных задач, что позволит увеличить возможности ГеоИС по адаптации. Количественные оценки эффективности адаптации рассчитываются для каждой ГеоИС и каждого набора задач отдельно.

Схема позволяет применять методы, использующие структурные и/или функциональные резервы ГеоИС (оптимизация процессов, планирование вычислений и т. д.). Предложим авторский метод адаптивного управления доступностью ресурсов ГеоИС, учитывающий неопределенность ее структуры и/или функций в условиях произвольного ДВ.

Абстрактная модель ГеоИС

Достаточно абстрактная модель ГеоИС содержит блоки наблюдения и управления, а также исполнительные устройства, и представлена на рисунке 5, где: Ω – доступная производительность элементов ГеоИС; K – множество решенных ГеоИС задач; K^* – множество поставленные перед ГеоИС задач;, $\Delta K = K^*/K$ – изменения в решаемых задачах, вызванные входной ситуацией; Q_{st} – множество воздействий стохастической среды; Q_{nst} – то же нестохастической среды; Q_d – то же детерминированной среды; $K^* \subset Q = Q_{st} \cup Q_{nst} \cup Q_d$ [3].

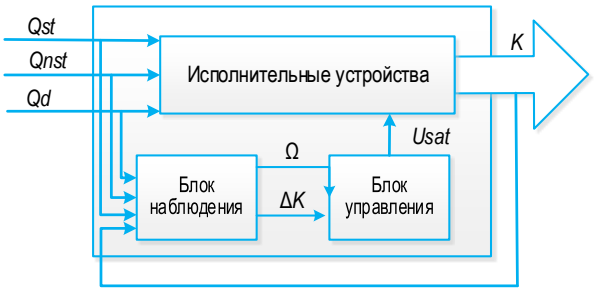


Рис. 5. Модель ГеоИС с блоками наблюдения и управления

Fig. 5. GeoIS Model with Observation and Control Unit

Задача блока наблюдения (БН) – идентифицировать ОУ, то есть предоставить актуальные данные о его текущем состоянии. Задача блока управления (БУ) – оказывать управляющие воздействия на исполнительные устройства (ИУ), миссия которых – решить задачи, поставленные пользователем. Эффективность функционирования всех блоков характеризуется соответствующими вероятностями достижения цели деятельности (ВЦД): P_{id}, P_c и P_{node}. Названные вероятности формируют ВЦД всей ГеоИС – P – и описываются деревом вероятностей (рисунок 6).

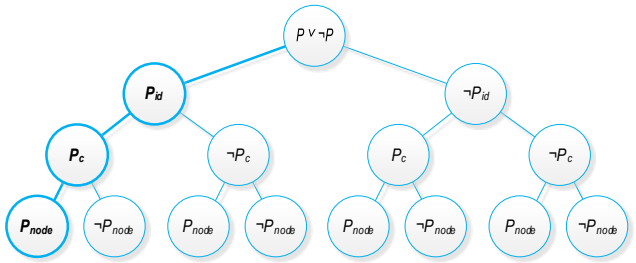


Рис. 6. Дерево ВЦД ГеоИС

Fig. 6. VDC GeoIS Tree

Допущение

Если система идентификации неверно идентифицирует ОУ, то БУ принимает решение на основе ложных (ошибочных) данных и, следовательно, его решения не адекватны ОУ. То есть можно сказать, что в случае не достижения БН своей цели деятельности обязательно происходит целевой срыв БУ. В свою очередь, если БУ выдает управляющие сигналы, неадекватные ОУ, то исполнительные устройства отработают неадекватно целям ГеоИС. Как результат – ГеоИС не достигнет цели своей деятельности.

Теоретически возможны ситуации, когда при срыве целевой деятельности одним из блоков последующие отрабатывают правильно, однако такие случаи, скорее, исключение, чем правило. И если они происходят, то ВЦД ГеоИС не уменьшается, поэтому далее считается, что искомая P является нижней границей ВЦД ГеоИС.

Согласно дереву вероятностей, общая ВЦД P рассчитывается как вероятность совместных событий:

$$P = P(P_{id}P_cP_{node}) = P(P_{node}|P_c)P(P_c|P_{id})P(P_{id}).$$

Очевидно, что величина, дополняющая P до единицы, является вероятностью реализации риска ИБ (P_{risk}), связанного с нарушением доступности ресурсов ГеоИС:

$$P_{risk} = 1 - (P_{node}|P_c)P(P_c|P_{id})P(P_{id}).$$

Данное выражение определяет шаги метода адаптации информационно-управляющих процессов ГеоИС к ДВ.

Шаги метода адаптации доступности ресурсов ГеоИС к деструктивным воздействиям

Согласно модели FIST [7] ГеоИС состоит из четырех типов ресурсов: вычислители (C), память (Sp), каналы связи (L), устройства ввода-вывода (Tr), – характеризуемых своим типом физической производительности ω (ω_C, ω_{Sp}, ω_L, ω_{Tr}) и образующих ее физическую структуру или уровень физической структуры (УФС). ДВ проявляются в падении доступной производительности ГеоИС, потому что они нарушают ее структуру и/или функции [19]. Для противостояния ДВ строится уровень логической структуры (УЛС) путем агрегирования каждого типа физических производительностей ω в пулы с соответствующими производительностями Ω (Ω_C, Ω_{Sp}, Ω_L, Ω_{Tr}). Уровень программного обеспечения (УПО) запрашивает у УЛС требуемую производительность Ω для решения множества поставленных задач K^*. УЛС, в свою очередь, выдает команды УФС на формирование пулов, обладающих требуемой производительностью заданного типа.

На вход метода подаются множества поставленных задач K^*, дестабилизирующих воздействий Ψ и элементов ГеоИС V. Цель метода – найти такие функции $f^{\text{УФС}}$, $f^{\text{УЛС}}$, $f^{\text{УПО}}$, чтобы ВЦД, как отношение количества выполненных задач K к количеству поставленных K^*, стремилась к единице [12]:

$$f^{\text{УФС}}, f^{\text{УЛС}}, f^{\text{УПО}}: P = \frac{K}{K^*} \to 1 \Rightarrow P_{risk} \to 0. \qquad (1)$$

Структура метода в нотации *IDEF*0 представлена на рисунке 7. Метод включает в себя несколько блоков (рисунок 8).

Рис. 7. Структура метода в нотации *IDEF*0

Fig. 7. Structure of the Method in IDEF0 Notation

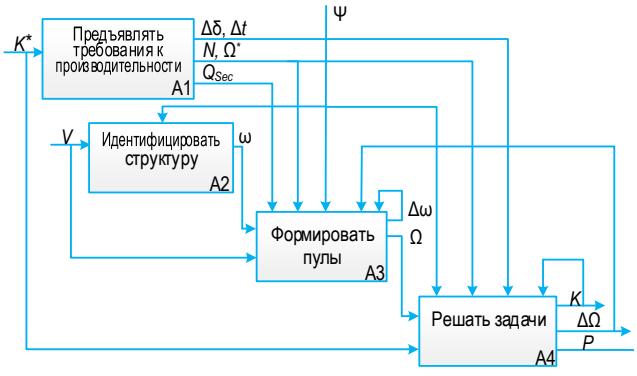


Рис. 8. Блочная структура метода в нотации *IDEF*0

Fig. 8. Structure of the Method in IDEF0 Notation

Блок $A1$ принимает задачи пользователей. Каждая поступившая задача $k \in K^*$ имеет свой приоритет и требования по обеспечению ИБ Q_{Sec}: $K^* = \bigcup_{i=1}^{M} K_i^*$ – множество задач, решаемых за время T; K_i^* – множество задач с i-м приоритетом; M – множество приоритетов.

Согласно принятому представлению в модели FIST, задача описывается в терминах требуемой производительности и допустимых погрешностей, в точности $\Delta\delta$ и времени Δt выполнения:

$$\Omega^* = \{\Omega_C^*, \Omega_L^*, \Omega_{Sp}^*, \Omega_{Tr}^*\}.$$

Предъявление требований к производительности (блок $A1$) довольно хорошо изучено. ГеоИС запрашивает ресурс для поставленных задач K^* согласно их приоритетам и выбранной стратегии: статическая, полудинамическая, динамическая [24]; децентрализованная, централизованная, иерархическая; с представлением в виде ациклического графа [25, 26], с упорядочиванием вершин и возможностью независимой работы [27], путем сетевого планирования [28]; при параллельной организации вычислений [29]; с учетом энергосбережения [30] и т. д. Требования к производительностям и допустимые погрешности в точности и времени исполнения определяет пользователь ГеоИС. Поскольку он находится на уровне персонала модели FIST, то эти требования являются требованиями метасистемы для УФС, УЛС, УПО, не подлежат модификации и принимаются «как есть». Требования по обеспечению безопасности накладывают дополнительные ограничения на запрашиваемый ресурс.

Не зависимо от поставленных задач K^*, существует процесс идентификации структуры ГеоИС (блок $A2$). Процесс предоставляет данные о доступной производительности ω физических элементов V в текущий момент времени:

$$\omega = \{\omega_C, \omega_L, \omega_{Sp}, \omega_{Tr}\}.$$

На распределение производительности в пространстве-времени влияют ДВ Ψ, выражающиеся в изменении доступной производительности Ω и/или ω из-за разрушения структуры и/или функций ГеоИС [19].

В блоке $A3$ выполняется метод D-FIST [31], который, исходя из существующих ДВ Ψ и требований к производительности Ω^* и безопасности Q_{Sec}, аккумулирует производительность физических элементов ω в пулы Ω:

$$\Omega = \{\Omega_C, \Omega_L, \Omega_{Sp}, \Omega_{Tr}\}.$$

Требования к производительности пулов корректируются на величину $\Delta\Omega$ в зависимости от ДВ на процесс решения задач в блоке $A4$. Изменение в производительности пулов $\Delta\Omega$ в свою очередь влечет за собой выдачу управляющих воздействий U на перемещение элементов V и изменение распределения производительности $\Delta\omega$ в пространстве-времени.

Решение задач (блок $A4$), подробно описанное в источнике [23], заключается в сопоставлении каждой задаче $k \in K$ требуемого ресурса $\Omega_k \in \Omega$. Если такое сопоставление невозможно, то есть существующих ресурсов недостаточно для формирования пулов с требуемой производительностью Ω^*, то допустимые погрешности задач по точности и времени преобразуются в резервы производительности $\Delta\Omega$. Данные об этой коррекции производительности пула учитываются при формировании новых пулов (блок $A3$). Исходя из соотношения решенных задач к поставленным, рассчитывается ВЦД системы P.

Таким образом, блоки $A1$ и $A4$ реализуют отображение $f^{\text{УПО}}$, блок $A2$ – отображение $f^{\text{УФС}}$, блок $A3$ – отображение $f^{\text{УЛС}}$. Идентификация ОУ в блоке $A2$ реализуется отдельным методом.

Метод идентификации объекта управления в условиях деструктивных воздействий

Природа ГеоИС такова, что элементы структуры используют разные операционные системы, процессоры, а значит, и системы команд. Это означает, что множество допустимых управляющих воздействий $U_{\text{доп}}$, которые можно выдать на ОУ, также изменяется во времени и само по себе требует идентификации. Согласно ограничению, сформулированному в [3], считается, что множество $U_{\text{доп}}$ неизменно во все моменты времени T. Поэтому далее речь идет только об идентификации структуры ГеоИС и свойствах элементов структуры (доступность требуемой величины заданного типа производительности). Свойства элементов – четыре типа физической производительности ω – доступны для непосредственного измерения. Цель идентификации – определить, как именно производительность ГеоИС распределена в пространстве-времени. Поскольку измерение свойств элементов выполняется непосредственно и не вызывает затруднений, то моментом, который стоит изучить отдельно, является период идентификации.

В существующих исследованиях интервалы времени, в течение которых необходимо снимать параметры ОУ для его идентификации, либо постулируются вплоть до введения полного запрета на произвольное покидание узлами распределенной сети [32], либо ищутся эмпирически, либо задача определения интервалов игнорируется и считается решенной, например, в виде присвоения узлам «репутации устройства» – статистической вероятности того, что устройство в течении определенного времени не покинет структуру и будет решать выделенную ему задачу [33].

Такой подход допустим для медленно или предсказуемо изменяющихся ОУ, и не совсем подходит для описания ГеоИС в условиях ДВ. В некоторых работах [34–36] предлагается разбивать время контроля на интервалы в зависимости от частоты аппроксимирующих функций. Это предполагает решение дополнительной задачи о выборе количества интервалов и большую вычислительную нагрузку на каждый элемент структуры ГеоИС, что только усугубляет негативный эффект ДВ.

В сфере информационных технологий задача определения времени обновления данных об ОУ сводится к тому, чтобы вручную задать время опроса узлов сети (RIP, OSPF, BID и т. д.). Например, в протоколе RIP время обновления данных о сети рассчитывается эмпирически и задается вручную, апдейты таблицы маршрутизации рассылаются по умолчанию раз в 30 секунд. Очевидным достоинством подхода является простота, а недостатком тот факт, что если сеть изменяется быстрее, чем раз в 30 секунд, то маршрутизатор работает с недостоверными данными.

В протоколе EIGRP используется асинхронный режим, т. е. маршрутизатор, заметивший изменение сети, сам начинает рассылать уведомление соседям. К достоинствам подхода относится оперативная реакция на добавление узлов в сеть. Однако, если хост исчезает, то об этом никто не узнает.

Таким образом, необходим метод выбора интервала идентификации состава ГеоИС, позволяющий учитывать внезапно исчезающие узлы, не требующий больших вычислительных мощностей и статистических данных.

Постановка задачи идентификации состава ГеоИС

Поскольку ГеоИС – распределенная система, то каждая задача имеет свою точку входа, через которую задача загружается в систему, т. е. конкретный узел ГеоИС, который принял задачу к исполнению от пользователя. Следовательно, для решения задачи нет необходимости знать структуру всей ГеоИС целиком. Достаточно данных о ближайших элементах, которые могут участвовать в исполнении задачи. Поэтому задачу идентификации каждый узел ГеоИС решает для себя самостоятельно.

Если говорить про ГеоИС, то здесь существует закономерность: чем чаще снимаются данные об ОУ, тем точнее идентифицируется сам объект, но тем больше накладные издержки на передачу и обработку данных. Чем реже снимаются данные, тем накладные издержки меньше, но ниже качество идентификации ОУ, а значит, хуже и качество управленческого решения, так как оно принимается по данным, которые описывают устаревший ОУ, что приводит к потере выполняемых задач или к назначению задач на несуществующие узлы.

Соответственно, возникает задача: найти такой интервал времени t_{id} съема данных, идентифицирующих ОУ, чтобы они были адекватны ему с допустимой погрешностью ε:

$$t_{id}: \varepsilon \le |x^* - x|, \quad (2)$$

при ограничениях на накладные расходы производительности (ω_{id}) вычислителей, каналов связи, устройств ввода-вывода, накопителей:

$$\omega_{id} \le \omega_{id}^{\text{доп}},$$

где x – переданное значение параметра; x^* – текущее значение параметра ОУ. Для БН ГеоИС такой параметр всего один – количество доступных элементов N.

Задача идентификации формулируется как сатисфакционная, а не оптимальная в силу сильной неопределенности ГеоИС как ОУ, который имеет следующую природу [19].

Стохастическую, в которой полностью известно множество альтернатив дестабилизирующих факторов и вероятностное описание механизма выбора из этого множества альтернатив. Сбои и отказы, вызванные естественными причинами и действиями низкоквалифицированных специалистов, поток пользовательских задач, уже известных и не раз выполняемых ГеоИС, добавление/удаление узлов сети – все это описывается статистически.

Нестохастическую, то есть не детерминированную и не стохастическую, когда неизвестно множество альтернатив либо вероятностное описание, либо фактор имеет целенаправленный агрессивный характер и не может описываться средствами теории вероятностей. Это новые, неучтенные ранее задачи, запрограммированные пользователем, реализация киберугроз и прочее.

Возможно, сформулированная задача решена в [37], но в силу закрытости технологии, узнать об этом точно не удалось.

Будем считать, что при предоставлении достоверной информации о структуре объекта система идентификации (БН) достигает цели своей деятельности, а при предоставлении недостоверной информации – нет. Следуя этой логике, выражение (2) преобразуется к виду:

$$t_{id}: P_{id}(t) \in [P_{id}^* - \Delta P_{id}; P_{id}^* + \Delta P_{id}], \quad (3)$$

где P^*_{id} – требуемая ВЦД БН; ΔP^*_{id} – допустима погрешность ВЦД БН.

БН ГеоИС производит идентификацию элементов не в момент времени, а за интервал, поэтому далее в качестве наблюдаемого параметра используем не количество элементов, а изменение количества элементов ΔN, полученного не в момент

времени t_{id}, а за интервал наблюдения Δt. Описание в формате *IDEF*0 приведено на рисунке 9.

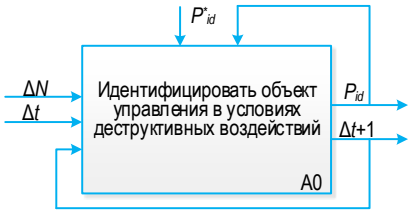


Рис. 9. Диаграмма *IDEF*0, описывающая метод идентификации

Fig. 9. IDEF0 Diagram Describing the Method of Identification

В ходе разработки метода идентификации выявлены закономерности, связывающие:

1) ресурсоемкость идентификации и время идентификации:

$$\omega_{id} = f_{\omega}(\Delta t); \quad (4)$$

2) время идентификации и количество элементов:

$$\Delta N = f_N(\Delta t); \quad (5)$$

3) количество элементов и вероятность идентификации:

$$P_{id} = f_{id}(\Delta N). \quad (6)$$

Из практических наблюдений установлена обратная пропорциональность зависимость (4):

$$\omega_{id} \sim \frac{1}{\Delta t}. \quad (7)$$

В реальных системах минимальное время опроса $t_{\min}$ ограничено техническими возможностями устройств, а максимальное $t_{\max}$ – выбирается, исходя из статистических наблюдений за системой и соображений целесообразности, например, 30 секунд, как в протоколе RIP. Следовательно, ресурсоемкость идентификации также находится в границах:

$$\omega_{id}^{\min} \le \omega_{id} \le \omega_{id}^{max}.$$

С учетом обратной пропорциональности (7) предпринималась попытка сформулировать закономерность (5) с использованием наименее ресурсоемких операций: сложения и умножения, как сокращенной записи сложения. Для этого сформулировано следующие допущение.

Допущение 1

Добавление новых элементов и удаление существующих имеет некоторую инертность. Следовательно, на конец текущего интервала времени Δt возможно сделать предположение о количестве элементов на следующем интервале времени Δt+1. В силу малого значения Δt, предполагается линейная зависимость, описывающая изменение элементов. На основании данных об изменении количества элементов в предыдущий момент времени Δt–1 и текущий момент Δt строится прямая и прогнозируется изменение в момент Δt+1 (рисунок 10). Количество новых элементов на начало интервала Δt считается равным количеству элементов на конец интервала Δt–1.

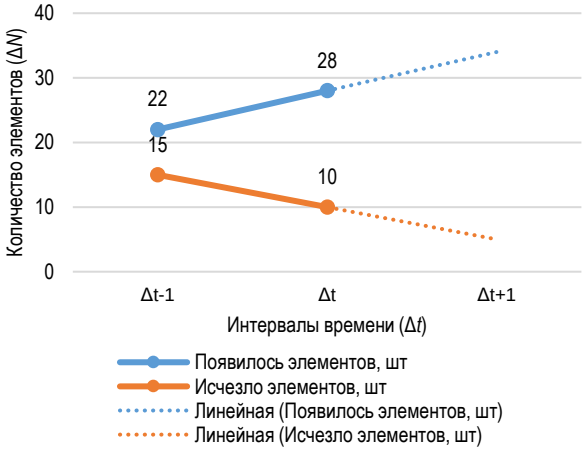


Рис. 10. Прогнозирование изменение состава

Fig. 10. Predicting Changes in the Composition

Закономерность (6) должна описывать два типа срывов целевой деятельности БН ОУ, вызванных ее промахами (ошибками I-го и II-го рода):

– элемента уже нет, а он помечен, как существующий;

– элемент существует, но в данных о структуре системы он отсутствует.

Оба промаха описываются количеством неучтенных системой идентификации элементов ΔN за интервал идентификации Δt.

Допущение 2

Появление (*r – аббр. от англ.* reproduction) и исчезновение (*d – аббр. от англ.* death) элементов – независимые друг от друга процессы. Однако технически идентификацию появления и исчезновения реализует один процесс, который управляет ВЦД БН через изменение времени идентификации (3). В настоящей работе временем идентификации t_{id} является интервал контроля Δt. И если этот интервал изменяется, то он изменяется и для идентификации появления элементов, и для идентификации исчезновения элементов. Поэтому в качестве действующей ВЦД БН используется минимальная величина:

$$P_{id} = \min\left(P_{r,id}, P_{d,id}\right) \in [P_{id}^{*} - \Delta P_{id}; P_{id}^{*} + \Delta P_{id}].$$

С учетом обратной пропорциональности зависимости (7) использовано самое простое, то есть частотное определение вероятности:

$$P_{failure} = \frac{\Delta N}{N} \Rightarrow P_{id} = 1 - P_{failure}.$$

Поскольку шаги метода одинаковы и для процесса появления новых элементов, и для процесса исчезновения известных, указание на вид идентифицируемого процесса опущено.

Шаги метода идентификации состава ОУ

Опишем пошагово содержание метода идентификации состава ОУ.

Шаг 1. Задать требуемую ВЦД БН P^*_{id}.

Пример. P^*_{id} = 0,9.

Шаг 2. Согласно частотному определению вероятности, вероятность срыва целевой деятельности системы идентификации на интервале Δt находится как отношение количества не идентифицированных элементов ΔN к общему количеству элементов N, идентифицированных на интервале Δt.

Из этого соотношения вычисляется допустимый процент изменения структуры на следующем интервале Δt+1 (см. допущение 1):

$$P_{failure} = \frac{\Delta N}{N} \Rightarrow P_{id} = 1 - P_{failure} \Rightarrow \Delta N = (1 - P_{id})N.$$

Пример. Пусть P^*_{id} = 0,9, тогда допустимый процент изменения структуры – 10 %. Пусть на конец интервала Δt появилось 120 новых элементов, значит, допустимое количество элементов, определяющее размер флуктуации 120 / 10 ∗ 100 = 12.

Шаг 3. Исходя из предположения о линейной зависимости (см. допущение 1), использовать уравнение прямой и определить следующий интервал времени, для которого изменение не превысит допустимое. Размер интервала Δt принять за единицу (см. рисунок 10).

Пример. На конец интервала Δt–1 было 80 новых элементов, на конец интервала Δt – 120 элементов, значит, на конец интервала Δt+1 будет 160 элементов. Допустимая флуктуация – 12 элементов.

Согласно уравнению прямой, решенному относительно x, следующая точка контроля имеет координату (2,3; 132):

$$x = \frac{(y - y_2)}{(y_1 - y_2)}(x_1 - x_2) + x_2 = \\ = \frac{(120 + 12 - 120)}{(80 - 120)}(1 - 2) + 2 = 2{,}3,$$

то есть новый интервал Δt+1 составляет 30 % от текущего интервала Δt.

Шаг 4. Если количество новых элементов убывает, действия – аналогичные.

Пример. На конец интервала Δt–1 было 40 новых элементов, на конец Δt – 10 элементов, значит, на конец интервала Δt+1 будет 20 элементов. Отрицательное значение говорит о том, что на конец интервала Δt+1 новых элементов будет больше, чем на интервале Δt. Допустимая флуктуация – 10 % от новых элементов на конец интервала Δt, то есть 1 элемент.

Согласно уравнению прямой, решенному относительно x, следующая точка контроля имеет координату (2,1; 9):

$$x = \frac{(y - y_2)}{(y_1 - y_2)}(x_1 - x_2) + x_2 = \\ = \frac{(10 - 1 - 10)}{(40 - 30)}(1 - 2) + 2 = 2{,}1,$$

то есть новый интервал Δt+1 составляет 10 % от текущего интервала Δt.

Шаг 5. Выполнять шаги 3–4, пока функционирует ГеоИС или не изменятся требования к ВЦД БН.

Из разработанного метода идентификации ОУ и технических ограничений реальных систем следует необходимое условие функционирования ГеоИС в условиях дестабилизации:

> Чтобы ГеоИС могла функционировать в условиях деструктивных воздействий, необходимо, чтобы время идентификации структуры ГеоИС t_{id} было не меньше, чем минимальное время опроса $t_{\min}$:
>
> $$t_{id} \geq t_{\min}.$$

Данное условие имеет дополнительную интерпретацию. В ГеоИС в динамическом режиме могут быть включены только те устройства, время идентификации которых больше минимального. Высокоскоростные объекты, например, противоракеты или невозвратные беспилотные летательные аппараты, должны регистрироваться в ГеоИС заранее и загружаться статически с указанием адресов и характеристик. В противном случае они не успеют зарегистрироваться в системе.

Эффективность предложенных методов адаптивного управления

Поскольку ближайший аналог к предложенному методу идентификации изложен в [35] (далее прототип), то именно с ним произведем сравнение.

В основе прототипа лежит теорема Котельникова, и период идентификации объекта контроля (ОК) $T_{\text{контр}}$ определяется из соотношения:

$$T_{\text{контр}} = \frac{1}{2f_{\text{в}}}, \quad (8)$$

где $f_{\text{в}}$ – максимальная частота в спектре контролируемого сигнала.

Для определения частоты $f_{\text{в}}$ в прототипе производится оценка условий функционирования ОК с помощью следующего алгоритма:

1) задать исходные данные:

– определить множество аппроксимирующих функций и указать точность аппроксимации;

– задать пределы и шаг изменения параметров аппроксимирующих функций;

– сформировать множество данных о времени и характере дестабилизирующих факторов, определить их классы;

2) определить интенсивности отказов ОК;

3) разделить дестабилизирующие факторы на однородные группы:

– отметить значения параметров для однородных групп A_i, …, A_j на временных осях;

– аппроксимировать значения каждой группы с заданной точностью непрерывными периодическими функциями, например, с помощью среднеквадратического приближения;

– построить вариационный ряд значений всех частот и определить наибольшее значение частоты;

4) исходя из выражения (8), определить оптимальный интервал контроля.

Метод, предложенный в настоящей работе, использует только один параметр контроля – количество доступных элементов N, поэтому сравнение производится, как если бы в прототипе также использовался только один параметр.

При прочих равных условиях можно утверждать, что в отличие от прототипа предлагаемый метод:

– *более адекватен* ГеоИС, так как прототип нуждается в сборе статистики для определения интенсивности отказа ОК либо применении экспертных оценок (шаг 2). В [35] не уточняется, каким именно способом это реализовано, но в любом случае, такой подход применим только для стохастических процессов, что охватывает только часть ДВ на ГеоИС;

– *точнее* подбирает интервал контроля, потому что не использует группировку (шаг 3 прототипа) и реагирует на каждое изменение параметра контроля;

– потребляет меньше вычислительных ресурсов системы, а значит *быстрее*, потому что, фактически, отсутствует самый ресурсоемкий шаг 3 прототипа. Точный выигрыш в производительности зависит от количества однородных групп, вида аппроксимирующей функции и т. д.;

– *потребляет меньше памяти*, так как хранит только допустимый процент изменения (число типа integer), против целого массива данных, требуемых прототипу: пределы и шаги аппроксимирующих функций, количество однородных групп, данные для размещения групп на временных осях, значения частот для вариационного ряда, наибольшее значение частоты и др. И так как работа с памятью – одна из самых медленных операций в процессоре, предложенный метод *быстрее прототипа*.

Для оценивания эффективности адаптации ГеоИС к ДВ с помощью предложенного метода разработана имитационная модель в среде MATLAB [12]. Цель адаптации – максимизировать ВЦД ГеоИС согласно выражению (1) или, что тоже самое, минимизировать риск ИБ P_{risk}, связанный с нарушением доступности ресурсов ГеоИС.

На модели изучалась зависимость ВЦД от следующих соотношений:

– количество входящих в ГеоИС задач / узлов ГеоИС (количество узлов было инвариантом и равнялось 10);

– минимальная производительность, требуемая задачами / максимальная доступная производительность узлов ГеоИС (производительность узлов была инвариантом и равнялась 10 условным единицам);

– максимальная длительность решаемых задач / максимальное время жизни узлов ГеоИС (время жизни узлов было инвариантом и равнялось 10 единицам модельного времени).

Поскольку в ходе анализа существующих публикаций аналогов разработанных методов, за исключением метода идентификации (его оценку см. выше), не выявлено, то изменение вероятности реализации риска ИБ ΔP_{risk}, рассчитывалось, исходя из вероятностей риска до P_{bm} и после P_m применения разработанных методов, по формуле:

$$\Delta P_{risk} = \frac{P_{bm} - P_m}{P_{bm}}.$$

На рисунке 11 представлены конфигурации ГеоИС, для которых применение разработанных методов позволило снизить риск нарушения доступности ресурсов ГеоИС на 10 и 50 %, соответственно. Поскольку изменялись характеристики потока задач, а узлов являлись инвариантом, то характеристики ГеоИС опущены, и оси на графике соответствуют характеристикам задач:

OX – максимальное количество решаемых задач;

OY – минимальная требуемая производительность задач;

OZ – максимальная длительность решаемых задач (сколько единиц модельного времени решается задача, если получает минимальную требуемую производительность).

Значения, откладываемые по осям, следует интерпретировать так:

OX – чем больше значение, тем меньше узлов доступно задачам для выполнения, то есть тем выше деградация структуры ГеоИС;

OY – чем больше значение, тем меньше производительности доступно задачам, то есть тем выше деградация функций ГеоИС;

OZ – чем больше значение, тем выше волатильность структуры и функций ГеоИС, то есть тем выше интенсивность деструктивных воздействий на ГеоИС.

Пример: Точка (7; 4; 2) соответствует конфигурации ГеоИС, в которой на 7 поставленных задач приходится 10 узлов, на 4 единицы требуемой производительности приходится 10 единиц доступной, максимальная длительность задач соотносится со временем жизни узлов ГеоИС как 2/10.

Точка (10; 8; 6) соответствует конфигурации ГеоИС, в которой на 10 поставленных задач приходится 10 узлов, на 8 единиц требуемой производительности приходится 10 единиц доступной, максимальная длительность задач соотносится со временем жизни узлов ГеоИС как 6/10.

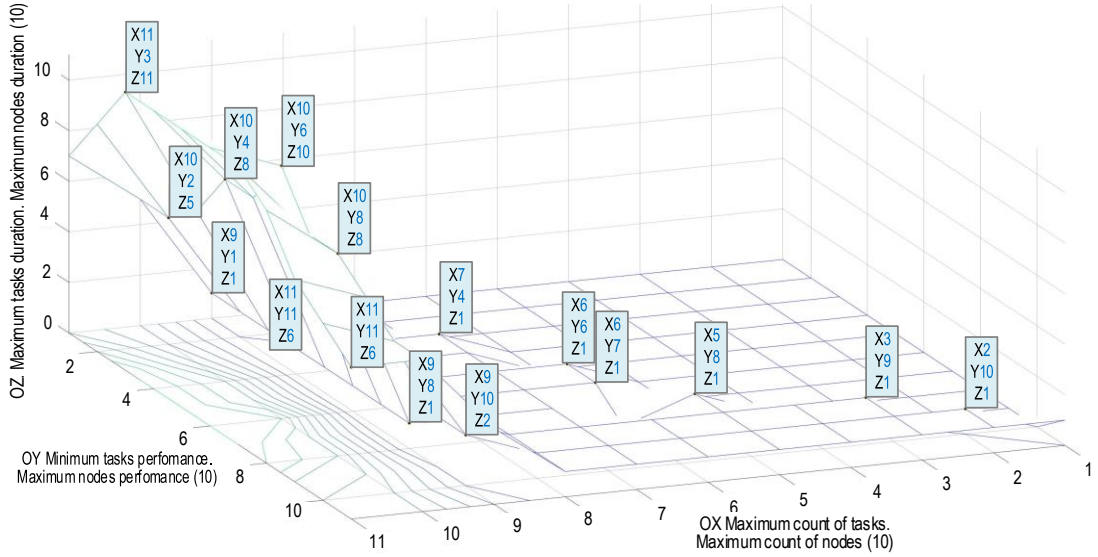
Как видно из графиков, если существует избыток ресурсов ГеоИС, то применение разработанных методов не имеет смысла, но в случае дефицита ресурсов применение разработанных методов снижает риски ИБ на 50 % и более.

Результаты относятся к любому типу ресурсов ГеоИС: вычислителям, каналам связи, накопителям, устройствам ввода-вывода. Их интерпретация на примерах нарушения доступности по уровням модели FIST, приведенных в начале статьи, выглядит следующим образом:

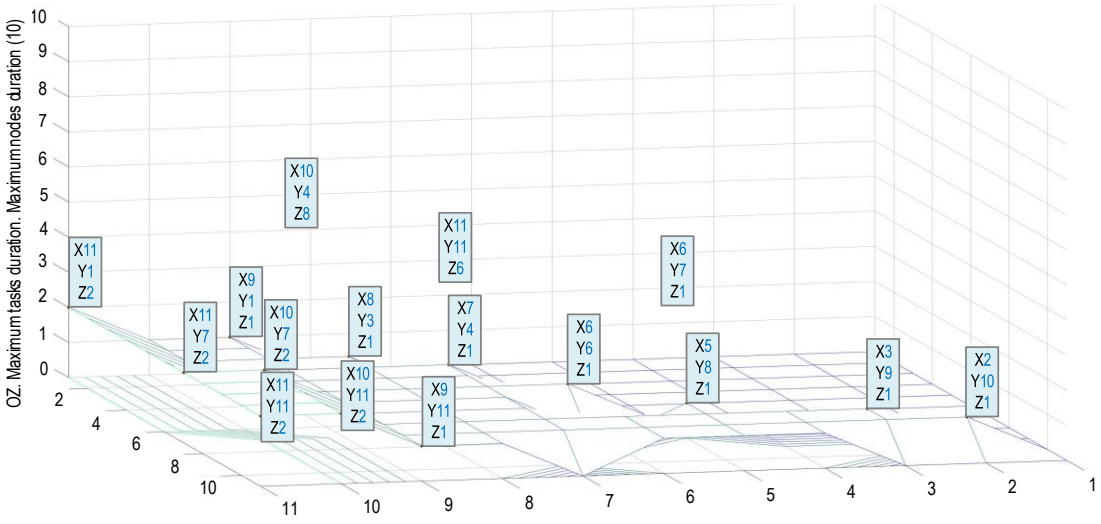
1) деструктивные воздействия УПО, а именно атаки типа *Slowloris*, *SYN / ACK flood*, *DHCP starvation* нейтрализуются подключением элемента, имеющего свободный пул адресов;

2) деструктивные воздействия УЛС ориентированы на нарушение работы предложенных методов. ГеоИС решает поставленные задачи с заданной ВЦД, если может обеспечить соответствующую свою конфигурацию (см. рисунок);

3) деструктивные воздействия УФС нейтрализуются согласно текущей ситуации и выбранной стратегии [12] посредством перераспределения задач или подключением новых элементов ГеоИС.



a)



b)

Рис. 11. Конфигурации ГеоИС, для которых риск нарушения доступности ресурсов снижается в результате применения разработанных методов на: a) 10 %; b) 50 %

Fig. 11. GeoIS Configurations, for which the Risk of Disruption of Resource Availability is Reduced as a Result of Applying the Developed Methods by 10%

Заключение

Обеспечение доступности ресурсов ГеоИС является важнейшей задачей ИБ. В том числе потому, что без доступности невозможно обеспечить другие аспекты ИБ, о чем говорит впервые сформулированное и доказанное необходимое и достаточное ее условие.

Наиболее адекватными ГеоИС являются модели и методы, применяемые для описания IoT.

Эффективность управления информационной безопасностью ГеоИС может оцениваться через ее ВЦД. Риск ИБ, связанный с нарушением доступности ресурсов ГеоИС, является дополнением ВЦД до единицы.

Предложенный метод адаптивного управления ГеоИС увеличивает ВЦД в условиях ДВ за счет ее реконфигурации и состоит из четырех шагов: предъявление требований к производительности, идентификации структуры, формирования пулов и решения задач с использованием внутренних резервов задач.

Идентификация структуры реализована отдельным методом, сохраняющим заданную вероятность идентификации объекта управления на протяжении всего времени функционирования ГеоИС за счет изменения интервала идентификации. Метод основан на предположении, что изменение объекта управления имеет инерцию.

Формирование пулов и решение задач с использованием внутренних резервов реализованы отдельными методами, опубликованными ранее.

Эффективность разработанных методов оценивалась с помощью имитационной модели. Применение разработанных методов позволяет достичь поставленной цели адаптации и снизить риски нарушения доступности ресурсов ГеоИС в условиях ДВ до 50 % от вероятности риска, имеющей место до применения методов.

Разработанные в статье методы могут применяться к любой информационной системе, имеющей в своем составе активные элементы. Однако это оправдано только в том случае, если информационная система имеет особенности, схожие с ГеоИС: распределенность в пространстве-времени, наличие всех типов данных, работа в реальном времени, существование риска ДВ как стохастического, так и агрессивного целенаправленного характера.

Список источников

1. Воронин А.В., Зацаринный А.А. Геоинформационная система как важнейший компонент системы принятия управленческих решений // Системы высокой доступности. 2019. Т. 15. № 3. С. 27–33. DOI:10.18127/j20729472-201903-02

2. Лисицкий Д.В., Кацко С.Ю. Пользовательский сегмент единого территориального геоинформационного пространства // Вестник СГУГиТ. 2016. № 4(36). С. 89–99.

3. Грызунов В.В. Концептуальная модель адаптивного управления геоинформационной системой в условиях дестабилизации // Проблемы информационной безопасности. Компьютерные системы. 2021. № 1. С. 102–108.

4. Грызунов В.В., Гришечко А.А., Сипович Д.Е. Выбор наиболее опасных уязвимостей для перспективных информационных систем критического применения // Вопросы кибербезопасности. 2022. № 1(47). С. 66–75. DOI:10.21681/2311-3456-2022-1-66-75

5. Данилин Г.В., Соколов С.С., Нырков А.П., Кныш Т.П. Мультисервисные сети: методы повышения защищенности данных в условиях сетевых атак // XXI век: итоги прошлого и проблемы настоящего плюс. 2020. Т. 9. № 2(50). С. 158–163. DOI:10.46548/21vek-2020-0950-0028

6. Грызунов В.В. Модель геоинформационной системы FIST, использующей туманные вычисления в условиях дестабилизации // Вестник Дагестанского государственного технического университета. Технические науки. 2021. Т. 48. № 1. С. 76–89. DOI:10.21822/2073-6185-2021-48-1-76-89

7. Грызунов В.В. Модель информационно-вычислительной системы, деградирующей в условиях информационно-технических воздействий // Труды Военно-космической академии имени А.Ф. Можайского. 2015. № 646. С. 93–102.

8. Растригин Л.А. Адаптация сложных систем. Рига: Зинатне, 1981. 375 с.

9. Сахаров В.В., Сикарев И.А., Чертков А.А. Автоматизация поиска оптимальных маршрутов и грузовых потоков в транспортных сетях средствами целочисленного линейного программирования // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2018. Т. 10. № 3. С. 647–657. DOI:10.21821/2309-5180-2018-10-3-647-657

10. Зализнюк А.Н., Присяжнюк С.П. Стратегическое планирование геоинформационного обеспечения систем управления // Информация и космос. 2016. № 4. С. 130–132.

11. Зегжда Д.П. Лаврова Д.С., Павленко Е.Ю. Управление динамической инфраструктурой сложных систем в условиях целенаправленных кибератак // Известия РАН. Теория и системы управления. 2020. № 3. С. 50–63. DOI:10.31857/ S0002338820020134

12. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability // Information and Control Systems. 2022. № 1. PP. 19–29. DOI:10.31799/1684-8853-2022-1-19-29

13. Кузнецова А.П., Монахов Ю.М. Постановка задачи адаптивного управления очередями для повышения доступности узлов в сетях TCP/IP с частыми потерями кадров // XIII международная научно-техническая конференция «Перспективные технологии в средствах передачи информации» (ПТСПИ-2019, Владимир, Россия, 3–5 июля 2019).

Владимир: Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, 2019. С. 75–78.

14. Kephart J.O., Chess D.M. The vision of autonomic computing // Computer. 2003. Vol. 36. Iss. 1. PP. 41–50. DOI:10.1109/ MC.2003.1160055

15. Angelopoulos K., Papadopoulos A.V., Silva Souza V.E., Mylopoulos J. Model predictive control for software systems with CobRA // Proceedings of the 38th International Conference on Software Engineering (ICSE '16, Austin, USA, 14–22 May 2016). ACM, 2016. PP. 35–46. DOI:10.1145/2897053.2897054

16. Peng X., Chen B., Yu Y., Zhao W. Self-tuning of software systems throughdynamic quality tradeoff and value-based feedback control loop // Journal of Systems and Software. 2012. Vol. 85. Iss. 12. PP. 2707–2719. DOI:10.1016/j.jss.2012.04.079

17. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия // Вестник Самарского государственного технического университета. Серия: Технические науки. 2020. № 1(65). С. 6–21.

18. Gatouillat A., Badr Y., Massot B. Smart and safe self-adaption of connected devices based on discrete controllers // IET Software. 2019. Vol. 13. Iss. 1. PP. 49–59. DOI:10.1049/iet-sen.2018.5029

19. Burlov V.G., Gryzunov V.V., Tatarnikova T.M. Threats of information security in the application of GIS in the interests of the digital economy // Journal of Physics: Conference Series. Proceedings of the XXIIIth International Conference on Soft Computing and Measurement (SCM'2020, 27–29 May 2020). 2020. Vol. 1703. P. 012023. DOI:10.1088/1742-6596/1703/1/012023

20. Young R., Fallon S., Jacob P. A Governance Architecture for Self-Adaption & Control in IoT Applications // Proceedings of the 5th International Conference on Control, Decision and Information Technologies (CoDIT, Thessaloniki, Greece, 10–13 April 2018). IEEE, 2018. PP. 241–246. DOI:10.1109/CoDIT.2018.8394824

21. Alfonso I., Garcés K., Castro H., Cabot J. Self-adaptive architectures in IoT systems: a systematic literature review // Journal of Internet Services and Applications. 2021. Vol. 12. P. 14. DOI:10.1186/s13174-021-00145-8

22. Moghaddam M.T., Muccini H. Fault-Tolerant IoT // Proceedings of the 11th International Workshop on Software Engineering for Resilient Systems (SERENE 2019, Naples, Italy, 17 September 2019). Cham: Springer, 2019. PP. 67–84. DOI:10.1109/JIOT.2017.2717704

23. Грызунов В.В. Методика решения измерительных и вычислительных задач в условиях деградации информационно-вычислительной системы // Вестник СибГУТИ. 2015. № 1(29). С. 35–46.

24. Бершадский А.М., Курилов Л.С., Финогеев А.Г. Исследование стратегий балансировки нагрузки в системах распределенной обработки данных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2009. № 4(12). С. 38–48.

25. Agrawal D., Jaiswal H.L., Singh I., Chandrasekaran K. An Evolutionary Approach to Optimizing Cloud Services // Computer Engineering and Intelligent System. 2012. Vol. 3. Iss. 4. PP. 47–55.

26. Фраленко В.П., Агроник А.Ю. Средства, методы и алгоритмы эффективного распараллеливания вычислительной нагрузки в гетерогенных средах // Программные системы: теория и приложения. 2015. Т. 6. № 3(26). С. 73–92.

27. Sakellariou R., Zhao H. A hybrid heuristic for DAG scheduling on heterogeneous systems // Proceedings of the 18th International Parallel and Distributed Processing Symposium (Santa Fe, USA, 26–30 April 2004). IEEE, 2004. P. 111. DOI:10.1109/IPDPS.2004.1303065

28. Багрич А.И., Кустов В.Н. Устройство для решения задач сетевого планирования. Авторское свидетельство SU 1575199 от 06.05.1988. Опубл. 30.06.1990.

29. Басыров А.Г., Кошель И.Н. Алгоритм планирования параллельных вычислений в деградирующей бортовой вычислительной системе космического аппарата // Труды Военно-космической академии имени А.Ф.Можайского. 2021. № 676. С. 17–26.

30. Басыров А.Г., Калюжный А.В., Широбоков В.В. Технология энергосберегающих функционально-распределённых вычислений в кластере микроспутников дистанционного зондирования Земли // Современные проблемы дистанционного зондирования Земли из космоса. 2020. Т. 17. № 2. С. 65–74. DOI:10.21046/2070-7401-2020-17-2-65-74

31. Бурлов В.Г., Грызунов В.В., Сипович Д.Е. Адаптивное управление доступностью в геоинформационной системе, использующей туманные вычисления // International Journal of Open Information Technologies. 2021. Т. 9. № 9. С. 74–87.

32. Jia B., Hu H., Zeng Y., Xu T., Yang Y. Double-matching resource allocation strategy in fog computing networks based on cost efficiency // Journal of Communications and Networks. 2018. Vol. 20. Iss. 3. PP. 237–246. DOI:10.1109/JCN.2018.000036

33. Sun Y., Lin F., Xu H. Multi-objective Optimization of Resource Scheduling in Fog Computing Using an Improved NSGA-II // Wireless Personal Communications. 2018. Vol. 102. PP. 1369–1385. DOI:10.1007/s11277-017-5200-5

34. Стародубцев Ю.И., Иванов С.А., Закалкин П.В., Вершенник Е.В. Методика определения оптимальной периодичности контроля состояния сложного объекта // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 3-4(153-154). С. 81–89.

35. Синев С.Г., Сорокин М.А., Стародубцев П.Ю., Сухорукова Е.В. Способ определения оптимальной периодичности контроля состояния процессов. Патент на изобретение RU 2623791 C от 25.01.2016. Опубл. 29.06.2017.

36. Фролков Е.В., Шатунов А.В. Способ определения периодичности контроля оперативного запоминающего устройства при функционировании в радиационных условиях космического пространства на солнечно-синхронной орбите. Патент на изобретение RU 2438163 C1. Опубл. 27.12.2011.

37. Disruption Tolerant Mobile Wireless Networks // Meshdynamics. URL https://meshdynamics.com/military-mesh-networks.html (дата обращения 20.07.2022)

References

1. Voronin A.V., Zatsarinny A.A. Geoinformation system as the most important component of management decision making system. *Sistemy vysokoy dostupnosti*. 2019;15(3):27–33. (in Russ.) DOI:10.18127/j20729472-201903-02
2. Lisitsky D.V., Katsko S.Yu. User segment of unified territorial geoinformation environment. Vestnik of SSUGT. 2016;4(36):89–99 (in Russ.)
3. Gryzunov V.V. Conceptual model of geoinformation system adaptive control under conditions of destabilization. *Information Security Problems. Computer Systems*. 2021;1:102–108. (in Russ.)
4. Gryzunov V., Grishechko A., Sipovich D. Selecting the most dangerous vulnerabilities for prospective information systems for critical applications. *Voprosy kiberbezopasnosti.* 2022;1(47):66–75. (in Russ.) DOI:10.21681/2311-3456-2022-1-66-75
5. Danilin G.V., Sokolov S.S., Nyrkov A.P., Knysh T.P. Multiservice networks: methods of increasing data security in the conditions of network attacks. *XXI Century: Resumes of the Past and Challenges of the Present plus*. 2020;9(2-50):158–163. (in Russ.) DOI:10.46548/21vek-2020-0950-0028
6. Gryzunov V.V. FIST geoinformation system model using fog computing in destabilization. *Herald of Dagestan State Technical University. Technical Sciences*. 2021;48(1):76–89. (in Russ.) DOI:10.21822/2073-6185-2021-48-1-76-89
7. Gryzunov V.V. Model of degrading computing system during software and hardware attack. *Proceedings of the Mozhaisky Military Space Academy*. 2015;646:93–102. (in Russ.)
8. Rastrigin L.A. *Adaptation of Complex Systems*. Riga: Zinatne Publ.; 1981. 375 p. (in Russ.)
9. Saharov V.V., Sikarev I.A., Chertkov A.A. Automating search optimal routes and goods flows in transport networks means the integer linear programming. *Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S.O. Makarova*. 2018;10(3):647–657. (in Russ.) DOI:10.21821/2309-5180-2018-10-3-647-657
10. Zaliznyuk A.N., Prisyazhnyuk S.P. Strategic planning of geoinformation support for control systems. *Information and Space*. 2016;3:130–132. (in Russ.)
11. Zegzhda D.P. Lavrova D.S., Pavlenko E.Y. Management of a dynamic infrastructure of complex systems under conditions of directed cyber attacks. *Journal of Computer and Systems Sciences International*. 2020;59(3):358–370. (in Russ.) DOI:10.1134/S1064230720020124
12. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability. *Information and Control Systems*. 2022;1:19–29. DOI:10.31799/1684-8853-2022-1-19-29
13. Kuznetsova A.P., Monakhov Yu.M. Setting the problem of adaptive queue management to increase the availability of nodes in TCP / IP networks with frequent frame losses. *Proceedings of the XIIIth International Scientific and Technical Conference on Promising Technologies in the Means of Information Transmission, PTSPI-2019, 3–5 July 2019, Vladimir, Russia.* Vladimir: Vladimir State University named after Alexander and Nikolay Stoletovs Publ.; 2019. p.75–78. (in Russ.)
14. Kephart J.O., Chess D.M. The vision of autonomic computing. *Computer*. 2003;36(1):41–50. DOI:10.1109/MC.2003.1160055
15. Angelopoulos K., Papadopoulos A.V., Silva Souza V.E., Mylopoulos J. Model predictive control for software systems with CobRA. *Proceedings of the 38th International Conference on Software Engineering, ICSE '16, 14–22 May 2016, Austin, USA*. ACM; 2016. p.35–46. DOI:10.1145/2897053.2897054
16. Peng X., Chen B., Yu Y., Zhao W. Self-tuning of software systems throughdynamic quality tradeoff and value-based feedback control loop. *Journal of Systems and Software*. 2012;85(12):2707–2719. DOI:10.1016/j.jss.2012.04.079
17. Basinya E.A. Software Implementation and Research of the System for Intellectually Adaptive Management of the Enterprise Information Infrastructure. *Vestnik of Samara State Technical University (Technical Sciences Series)*. 2020;1(65):6–21. (in Russ.)
18. Gatouillat A., Badr Y., Massot B. Smart and safe self-adaption of connected devices based on discrete controllers. *IET Software*. 2019;13(1):49–59. DOI:10.1049/iet-sen.2018.5029
19. Burlov V.G., Gryzunov V.V., Tatarnikova T.M. Threats of information security in the application of GIS in the interests of the digital economy. *Journal of Physics: Conference Series. Proceedings of the XXIIIth International Conference on Soft Computing and Measurement, SCM'2020, 27–29 May 2020*. IOP Publ.; 2020. vol.1703. p.012023. DOI:10.1088/1742-6596/1703/1/012023
20. Young R., Fallon S., Jacob P. A Governance Architecture for Self-Adaption & Control in IoT Applications. *Proceedings of the 5th International Conference on Control, Decision and Information Technologies, CoDIT, 10–13 April 2018, Thessaloniki, Greece*. IEEE; 2018. p.241–246. DOI:10.1109/CoDIT.2018.8394824
21. Alfonso I., Garcés K., Castro H., Cabot J. Self-adaptive architectures in IoT systems: a systematic literature review. *Journal of Internet Services and Applications*. 2021;12:14. DOI:10.1186/s13174-021-00145-8
22. Moghaddam M.T., Muccini H. Fault-Tolerant IoT. *Proceedings of the 11th International Workshop on Software Engineering for Resilient Systems, SERENE 2019, 17 September 2019, Naples, Italy*. Cham: Springer; 2019. p.67–84. DOI:10.1109/JIOT.2017.2717704
23. Gryzunov V. Problem Solving Method of Measuring and Calculating Tasks under Conditions of Data Computing System Degradation. *Vestnik SibGUTI*. 2015;1(29):35–46. (in Russ.)
24. Bershadsky A.M., Kurilov L.S., Finogeev A.G. Study of Load Balancing Strategies in Distributed Data Processing Systems. *University proceedings. Volga region. Technical sciences*. 2009;4:38–48. (in Russ.)
25. Agrawal D., Jaiswal H.L., Singh I., Chandrasekaran K. An Evolutionary Approach to Optimizing Cloud Services. *Computer Engineering and Intelligent System*. 2012;3(4):47–55
26. Fralenko V.P., Agronik A.Yu. Tools, methods and algorithms for the efficient parallelization of computational loading in heterogeneous environments. *Program Systems: Theory and Applications*. 2015;6(3-26):73–92. (in Russ.)

27. Sakellariou R., Zhao H. A hybrid heuristic for DAG scheduling on heterogeneous systems. *Proceedings of the 18th International Parallel and Distributed Processing Symposium, 26–30 April 2004, Santa Fe, USA*. IEEE; 2004. p.111. DOI:10.1109/IPDPS.2004.1303065

28. Bagrich A.I., Kustov V.N. Device for Solving Problems of Network Analysis. Copyright certificate USSR, no. 1575199 A1, 30.06.1990. (in Russ.)

29. Basyrov A.G., Koshel I.N. Algorithm for Scheduling Parallel Computing in a Degrading Spacecraft Onboard Computer System. *Proceedings of the Mozhaisky Military Space Academy*. 2021;676:17–26. (in Russ.)

30. Basyrov A.G., Kalyuzhnyy A.V., Shirobokov V.V. Technology of Energy-Saving Functional Distributed Computing in a Cluster of Earth Remote Sensing Microsatellites. *Current problems in remote sensing of the Earth from space*. 2020;17(2):65–74. (in Russ.) DOI:10.21046/2070-7401-2020-17-2-65-74

31. Burlov V., Gryzunov V., Sipovich D. Adaptive Accessibility Management in Geographic Information Systems Using Fog Computing. *International Journal of Open Information Technologies*. 2021;9(9):74–87. (in Russ.)

32. Jia B., Hu H., Zeng Y., Xu T., Yang Y. Double-matching resource allocation strategy in fog computing networks based on cost efficiency. *Journal of Communications and Networks*. 2018;20(3):237–246. DOI:10.1109/JCN.2018.000036

33. Sun Y., Lin F., Xu H. Multi-objective Optimization of Resource Scheduling in Fog Computing Using an Improved NSGA-II. *Wireless Personal Communications.* 2018;102:1369–1385. DOI:10.1007/s11277-017-5200-5

34. Starodubtsev Yu.I., Ivanov S.A., Zakalkin P.V., Vershennik E.V. Methods for determining the optimal frequency of complex object state monitoring. *Military Enginery. Scientific and Technical Journal. Counter-terrorism technical devices. Issue 16*. 2021;3-4(153-154):81–89. (in Russ.)

35. Sinev S.G., Sorokin M.A., Starodubtsev P.Yu., Sukhorukova E.V. *Method of Determination of Optimal Periodicity of Control of Processes State*. Patent RF, no. 2623791 C, 06.29.2017. (in Russ.)

36. Frolkov E.V., Shatunov A.V. Method of Determining Periodicity of Inspecting Random Access Memory During Operation in Radiation Conditions of Cosmic Space on Sun-Synchronous Orbit. Patent RF, no. 2438163 C1, 27.12.2011. (in Russ.)

37. Meshdynamics. *Disruption Tolerant Mobile Wireless Networks*. URL: https://meshdynamics.com/military-mesh-networks.html [Accessed 20th July 2022]

Статья поступила в редакцию 20.07.2022; одобрена после рецензирования 09.08.2022; принята к публикации 12.08.2022.
The article was submitted 20.07.2022; approved after reviewing 09.08.2022; accepted for publication 12.08.2022.

Информация об авторе:

Грызунов Виталий Владимирович

кандидат технических наук, доцент кафедры информационных технологий и систем безопасности Российского государственного гидрометеорологического университета
https://orcid.org/0000-0003-4866-217X