УПРАВЛЕНИЕ СЛОЖНЫМИ СИСТЕМАМИ

DOI: 10.18137/RNU.V9187.23.04.P.23 УДК 004.052.32

В.А. Бугаенко

ОЦЕНКА ЭФФЕКТИВНОСТИ МЕТОДОВ ОБЕСПЕЧЕНИЯ ОТКАЗОУСТОЙЧИВОСТИ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Статья представляет собой анализ эффективности методов обеспечения отказоустойчивости ИТ-инфраструктуры, а также оценку этих методов применительно к сетям промышленного интернета вещей. ИТ-инфраструктуру организации можно разделить на три укрупненных объекта: сетевое оборудование и программное обеспечение, аппаратный комплекс, программный комплекс. Для поддержания работоспособности всей системы можно выделить соответствующие группы базовых методов обеспечения отказоустойчивости, а также такие методы, которые относятся сразу к двум или трем группам: разделение сети, использование протоколов связи, отказоустойчивых серверов и балансировщиков нагрузки, резервное копирование и регулярное обновление программного обеспечения, обучение персонала, использование системы мониторинга и оповещения. Для полноценной работы без сбоев и отказов необходимо системное применение вышеперечисленных методов. Меры, исходя из экспертной оценки, обусловлены результатами предложенной матрицы. Целью данной работы является анализ и определение методов обеспечения отказоустойчивости, наиболее подходящих организациям, в которых действует технология промышленного интернета вещей. В работе применены теоретические и эмпирические методы научного исследования, в частности анализ, синтез, мысленный эксперимент, экспертная оценка. Результатом работы является предложение для системного обеспечения отказоустойчивости применительно к сетям промышленного интернета вещей.

Ключевые слова: обеспечение отказоустойчивости, ИТ-инфраструктура, промышленный интернет вещей, кибератака, сетевое оборудование, аппаратный комплекс.

V.A. Bugaenko

EVALUATION OF THE EFFECTIVENESS OF FAULT TOLERANCE METHODS IN THE INTERNET OF THINGS NETWORKS

Abstract. This essay represents an analysis of the effectiveness of methods for ensuring fault tolerance of IT infrastructure, as well as an evaluation of these methods in relation to industrial Internet of Things networks. The IT infrastructure of an organization can be divided into 3 expanded objects – network equipment and software, hardware complex, software complex. To maintain the workability of the entire system, relevant groups of fault tolerance methods can be identified, as well as such methods that relate to two or three objects at once – network separation, the use of communication protocols, fault-tolerant servers and load balancers, backup and regular software updates, personnel training, as well as the use of monitoring and notification systems. For full-fledged functioning without failures and rejections, the systematic application of the above methods is necessary. The article presents a proposal for the selection of measures based on expert evaluation and the application of specific measures, the choice of which is determined by the results of the proposed matrix. The aim of this work is to analyze and determine the methods of ensuring fault tolerance that are most suitable for organizations that use the technology of the industrial Internet of Things. Theoretical and empirical methods of scientific research were applied in the study, in particular analysis, synthesis, thought experiment, expert evaluation. The result of the work is a suggestion for system fault tolerance in relation to industrial Internet of Things networks.

Keywords: fault tolerance, IT infrastructure, industrial Internet of things, cyber attack, network equipment, hardware complex.

© Бугаенко В.А., 2023

Бугаенко Валерий Андреевич
аспирант, Российский экономический университет имени Г.В. Плеханова, Москва. Сфера научных интересов: интернет вещей, отказоустойчивость инфраструктуры. Автор пяти опубликованных научных работ.
Электронный адрес: bugaenkova@gmail.com

Введение

Отказоустойчивость – это способность системы сохранять свою работоспособность при возникновении ошибок и сбоев в ее работе. Она является одним из ключевых требований к современным информационным системам, особенно в условиях постоянно растущей нагрузки и увеличения количества пользователей [1]. С учетом тенденции активного распространения технологий интернета вещей в промышленном кластере возникает всё больше уязвимостей, связанных со стабильностью работы данной технологии и системы в целом. Одновременно, помимо возникающих проблем с устойчивостью, можно отметить отсутствие системных концепций по предотвращению реализации угроз кибератак на инфраструктуру и сеть, в которой реализована технология интернета вещей.

По данным аналитического исследования российского разработчика продуктов для защиты и предотвращения кибератак Positive Technologies, во втором квартале 2023 года наиболее распространенными кибератаками стали утечки конфиденциальной информации (67 %) и нарушение основной деятельности (44 %) [2]. В то же время в аналитическом отчете Ростелекома-Солара отмечается, что в первом квартале 2023 года количество кибератак продолжает расти, более актуальным стало направление киберразведки; также в 2023 году станет еще более актуальным вопрос своевременного реагирования на киберинциденты на фоне общего роста числа событий информационной безопасности [3].

В данной статье предложен системный подход оценки применения комплекса, состоящего из нескольких методов, для обеспечения отказоустойчивости системы с применением технологии промышленного интернета вещей.

В настоящее время существует ряд базовых методов обеспечения отказоустойчивости, которые могут быть использованы для стабильной работоспособности объектов ИТ-инфраструктуры. Этой теме посвящены многочисленные научные исследования, в том числе работы А.А. Тарасова [4], Д.А. Беспалова, С.М. Гушанского, Н.М. Коробейникова [5], М.А. Волкова [6], С.В. Зотова [7] и др.

Целью данной статьи является анализ методов обеспечения отказоустойчивости ИТ-инфраструктуры и определение методов, наиболее подходящих для использования в системах промышленного интернета вещей.

В работе применены теоретические и эмпирические методы научного исследования, в частности проанализированы различные методы обеспечения отказоустойчивости и исходя из результатов анализа проведен синтез системы, обеспечивающей работоспособность ИТ-инфраструктуры при поломках, сбоях и атаках. Также применен метод мысленного эксперимента – новый системный метод для применения в сетях интернета вещей. Для реализации предложенного метода необходима экспертная оценка применяемых средств по отношению к объектам защиты от отказов.

Методы обеспечения отказоустойчивости ИТ-инфраструктуры

В работе организации можно выделить три основных объекта обеспечения отказоустойчивости ИТ-инфраструктуры [8; 9]:

сетевое оборудование и программное обеспечение – коммутаторы, концентраторы, маршрутизаторы, веб-серверы, брандмауэры, прокси-серверы, антивирусные программы;

аппаратный комплекс – серверы, рабочие станции, маршрутизаторы, элементы питания и охлаждения, структурированные кабельные системы, корпоративные ЦОДы и др.;

программный комплекс – программы для решения внутренних задач, приложения для взаимодействия с клиентами, программы для работы аппаратного комплекса и управления им и др.

Для стабильной работы сетевого оборудования и программного обеспечения выделяются такие методы сохранения отказоустойчивости, как разделение сети и использование протоколов связи.

Разделение сети для обеспечения отказоустойчивости информационной системы заключается в разделении их на отдельные логические сетевые домены, например, внутренний сетевой домен организации и внешние сетевые домены, каждый из которых защищен разным набором средств безопасности. Примером такого набора может служить внедрение шлюза безопасности между двумя связанными сетями для контроля и управления доступом и информационного потока между ними. Применение данного подхода необходимо для фильтрации трафика между доменами и для блокирования неавторизованного доступа. Такой инструмент также называется межсетевым экраном. Разделение сети позволяет снизить вероятность неработоспособности всей системы в случае отказа одного из доменов сети, а также повышает отказоустойчивость сети в целом. Недостатком этого метода являются дополнительные затраты на оборудование для разделения сети и управления ею [10; 11].

Другим важным методом обеспечения отказоустойчивости информационных систем является **использование сетевых протоколов**, которые обеспечивают надежность передачи данных. На физическом уровне задача решается применением цифровых кодов, позволяющих эффективно работать в условиях помех и отслеживать искажения (по возможности выполнять коррекцию ошибок) при передаче данных. На уровне передачи пакетов самым очевидным решением при одноадресной передаче является подтверждение со стороны получателя об успешном принятии всех пакетов, переданных по сети. К такому типу относится TCP-протокол – протокол управления передачей – в противовес протоколу UDP. В последнем передача пакетов осуществляется без подтверждения их получения. Решение о том, успешно ли был принят пакет, реализуется с помощью проверки контрольных сумм пакета. Использование протоколов связи может снизить затраты на подключение и настройку сетевых устройств, так как многие протоколы уже имеют встроенные механизмы для автоматической настройки и оптимизации сети [6, с. 56; 10].

Однако некоторые протоколы связи имеют ограничения на максимальную пропускную способность, что может ограничить скорость передачи данных в сети. Помимо этого, некоторые протоколы связи могут требовать обновлений и исправлений для поддержания их актуальности и функциональности. Некоторые протоколы связи не поддерживают все необходимые функции для обеспечения отказоустойчивости и безопасности сети или требуют определенных типов оборудования для работы, что может ограничивать их использование в различных сценариях [10].

Для обеспечения стабильной работы аппаратного комплекса выделяются такие методы обеспечения отказоустойчивости, как использование отказоустойчивых серверов и балансировщиков нагрузки.

Использование отказоустойчивых серверов – метод обеспечения отказоустойчивости, который заключается в использовании серверов с несколькими узлами, работающими параллельно и предоставляющими высокую доступность системы. Если один из узлов выходит из строя, система продолжает работать на оставшихся узлах. Однако в этом случае требуется дополнительное оборудование и ресурсы для установки отказоустойчивых серверов и поддержания их работы [10–12].

Балансировщики нагрузки также могут быть использованы для обеспечения отказоустойчивости системы. Они распределяют нагрузку между несколькими серверами и обеспечивают высокую доступность системы в случае сбоев, а также снижают время простоя при сбоях. Недостатком является необходимость дополнительных ресурсов для балансировки нагрузки и настройки балансировщиков [1; 10; 12].

Для обеспечения стабильной работы программного комплекса выделяются такие методы обеспечения отказоустойчивости, как резервное копирование и регулярное обновление программного обеспечения.

Резервное копирование данных – один из наиболее распространенных методов обеспечения отказоустойчивости аппаратного комплекса. Этот метод заключается в создании копий данных на различных носителях, таких как жесткие диски, серверы, сетевые хранилища или облачные сервисы, а также иные системы хранения данных. Преимуществами данного метода является возможность быстрого восстановления данных из резервных копий при потере данных или сбое системы. Также это может быть плюсом с точки зрения обеспечения безопасности: резервные копии могут быть использованы для восстановления системы в случае взлома или других угроз безопасности. Кроме того, возможно применение методов зеркалирования серверов баз данных. Этот метод часто не требует дополнительных затрат [10]. Недостаток метода – необходимость большого количества дополнительных ресурсов как для хранения резервных копий, так и для их покупки или аренды. Резервирование и восстановление данных может занимать длительное время, соответственно, в случае внезапных ошибок часть данных может не успеть сохраниться, что приведет к их утере. Помимо прочего, остается риск повреждения самих резервных копий, что приведет к потере некоторых или даже всех данных. Еще одним недостатком данного метода является потенциальная возможность доступа к резервным копиям более широкого круга лиц, что может привести к утечкам сохраняемой таким образом информации [12–15].

Регулярное обновление программного обеспечения – метод, позволяющий исправлять ошибки и уязвимости в работе системы, что повышает ее отказоустойчивость и безопасность. В то же время этот метод может приводить к временным простоям системы при обновлении, а также требует дополнительных ресурсов на установку и обновление программного обеспечения [1].

Для обеспечения стабильной работы ИТ-инфраструктуры в целом выделяются такие методы обеспечения отказоустойчивости, как обучение персонала, использование системы мониторинга и оповещения.

Обучение персонала оказывает косвенное влияние на обеспечение отказоустойчивости информационных систем через развитие компетенций работающих с ними сотруд-

ников. В соответствии с внутренней документацией организации (внутренние приказы, политики, регламенты и др.) все правила, требования, инструкции и руководства пользователя и администратора должны быть доведены до сведения работников. Если же для работы необходимы новые навыки и умения, то организация может обеспечить дополнительное повышение квалификации своих сотрудников. Выполнение данного требования необходимо в связи с тем, что своевременная и квалифицированная реакция специалиста на возникающие инциденты может предотвратить более глобальные в рамках организации сбои и простои в работе и тем самым повысит отказоустойчивость. Недостатки: время, затраченное на обучение персонала, может быть ограниченным; персонал может безответственно отнестись к обучению или следованию правилам, что приведет к негативным последствиям; обучение не всегда может быть эффективным, если персонал не работает в команде и не имеет опыта работы с системой [15].

Мониторинг и оповещение также являются важными методами обеспечения отказоустойчивости. Системы мониторинга отслеживают состояние оборудования, программного обеспечения, работу всех компонентов сети; также их функционал включает в себя обнаружение ошибок и их исправление до того, как они вызовут проблемы, прогнозирование вероятности возникновения сбоя, чтобы успеть предпринять действия для предотвращения или смягчения последствий сбоя. Например, системы могут использоваться для выявления и исправления ошибок при передаче данных. Если проблема обнаружена и устранена быстро, то система может продолжать работу без задержек [16]. Оповещения отправляются пользователям или администраторам системы, чтобы они могли вовремя отреагировать и принять меры для устранения проблемы. Среди отрицательных сторон применения такого рода систем – необходимость в дополнительных средствах на установку и обслуживание систем мониторинга, возможность ошибочной сигнализации о проблемах, что может привести к ненужным действиям, возможная неэффективность применения некоторых систем мониторинга в определенных условиях или для определенных типов оборудования [7; 9; 16].

Перечисленные методы используются в различных сферах, таких как консалтинг, банковское дело, медицина, промышленность. Они помогают снизить риски сбоев и повысить надежность и доступность систем. Оценим возможность и эффективность их применения для обеспечения отказоустойчивости сети промышленного интернета вещей.

Оценка эффективности методов обеспечения отказоустойчивости в системах интернета вещей

Технологии интернета вещей представляют собой внедрение в ИТ-инфраструктуру организации систем реального времени, подразумевающих быструю реакцию на события [6, с. 70], и «умных» устройств – ов-систем и иных устройств, подключенных к системе управления через интернет. Промышленный интернет вещей – это расширение интернета вещей, которое используется промышленными секторами и позволяет внедрить в производство прогностическую аналитику и искусственный интеллект. В настоящее время технология промышленного интернета вещей широко используется для выполнения таких функций, как идентификация, отслеживание, коммуникация, мониторинг, управление сервисами и др., а также в различных сферах: здравоохранении, транспорте и логистике, связи, энергетике, банковской сфере, оборонной, ракетно-космической, горнодобывающей, металлургической, химической промышленности и др. [17].

Системы с применением технологий интернета вещей подразумевают разделение по времени реакции на изменение входных данных; реакция должна быть без каких-либо за-

держек вне зависимости от условий или своевременной, то есть некоторая задержка не критична [6, с. 71].

В то же время при внедрении данной технологии в сеть организации могут возникнуть некоторые проблемы. Из них чаще всего выделяют следующие [17; 18].

1. Сложность интеграции новых устройств в существующую инфраструктуру; изначальная архитектура ИТ-инфраструктуры организации часто не подразумевает возможности увеличения количества объектов, что необходимо при внедрении технологий интернета вещей, состоящей из системы управления и множества различных устройств – от датчиков до систем мониторинга событий информационной безопасности.

2. Необходимость обучения персонала работе с новыми устройствами и программным обеспечением; помимо разработки всей необходимой для модернизации инфраструктуры документации, которую работники должны изучить, необходимо обеспечить повышение квалификации сотрудников с учетом направления их деятельности.

3. Ограниченные ресурсы для поддержки и сопровождения новых устройств; даже если архитектура предусматривает увеличение количества устройств, необходимо обновить некоторые виды оборудования, поскольку они могут не принимать или передавать данные для аналитики и своевременной реакции, не получать команды от центра управления и др.

4. Риск потери данных из-за ошибок или сбоев в работе устройств; устройства могут выйти из строя, отключиться или начать неправильно работать по причине сбоев, ошибок и кибератак, что может послужить причиной потери данных, например, если они не сохранены или если произошла ошибка во время сохранения.

5. Необходимость обеспечения безопасности данных и защиты от кибератак; поскольку технологии интернета вещей подразумевают работу и передачу данных и команд через интернет, то есть риск кибератак, воздействующих как на данные, так и на оборудование.

6. Недостаток опыта и знаний для разработки и внедрения решений промышленного интернета вещей; на данный момент данные технологии являются сравнительно новыми, из-за чего опыта внедрения таких решений немного, что может обернуться некоторыми рисками при их внедрении в структуру организаций.

7. Трудности в обеспечении совместимости и взаимодействия между устройствами разных производителей; производители разрабатывают специальное программное обеспечение для своих решений, что является проблемой для управления системой в целом.

Также помимо проблем при внедрении остается актуальной угроза кибератак на всю ИТ-инфраструктуру, скачков напряжения, несанкционированного доступа, вирусов, перегрузки сети и др. [1]. Их объектом может выступать как сетевая инфраструктура, так и аппаратный или программный комплекс.

В связи с этим внедрение отдельных из перечисленных выше методов не позволяет перекрыть все проблемы, решение которых обеспечивает отказоустойчивость. Соответственно, необходимо подойти к данному вопросу системно и применять комплекс методов по обеспечению стабильной работы системы и оборудования, наиболее соответствующих специфике ее функционирования. Это может быть как весь комплекс методов, так и его часть. Для этого необходимо тщательно проработать архитектуру систем и инфраструктуры, определить все слабые стороны, через которые можно проникнуть во внутреннюю сеть или повредить оборудование, то есть провести аудит безопасности.

Для определения наиболее эффективного комплекса методов воспользуемся матрицей оценки уровня защиты элементов системы. Структура матрицы представлена в Таблице.

Таблица

Матрица оценки уровня защиты методами обеспечения отказоустойчивости

Метод/объект защиты	Сетевая инфраструктура	Аппаратный комплекс	Программный комплекс
Разделение сети	2	0	0
Протоколы связи	3	0	0
Отказоустойчивые сервера	0	2	0
Балансировщики нагрузки	0	3	0
Резервное копирование	0	1	3
Регулярное обновление ПО	0	0	2
Обучение персонала	3	3	4
Мониторинг и оповещение	3	3	4
ИТОГО, интегральная оценка	11	12	13

Источник: таблица разработана автором.

Столбцы матрицы соответствуют объектам защиты, строки – возможным способам нивелирования проблем – методам обеспечения отказоустойчивости, причем это могут быть как решения для одного объекта, так и комплексные решения, закрывающие собой сразу несколько из них. Значения матрицы представляют собой экспертную оценку влияния соответствующего метода на отказоустойчивость объекта защиты – балл от 0 до 5, где 0 – нет влияния данного метода на объект защиты; 1 – небольшая степень влияния; 2 – влияние ниже среднего; 3 – средняя степень влияния; 4 – влияние выше среднего; 5 – максимальная степень защиты объекта. Эффективность выбранного комплекса решений рассчитывается путем суммирования полученных оценок по столбцам матрицы. Для обеспечения минимального достаточного уровня надежности и стабильности работы необходим суммарный уровень защиты от 6 баллов по каждой категории объектов защиты. Соответственно, даже при использовании метода, обеспечивающего 5-балльную защиту, этого будет недостаточно.

В таблице представлен расчет эффективности для исходных данных, соответствующих условному примеру, где в ИТ-инфраструктуру организации, использующей сети промышленного интернета вещей, могут быть внедрены следующие методы обеспечения отказоустойчивости. Таким образом, предложенные решения могут применяться для обеспечения устойчивости функционирования систем промышленного интернета вещей.

Заключение

В рамках исследования были выделены основные методы обеспечения отказоустойчивости и работоспособности ИТ-инфраструктуры – сетевого оборудования и программного обеспечения: обучение персонала, использование системы мониторинга и оповещения, резервное копирование, регулярное обновление программного обеспечения, использование отказоустойчивых серверов и балансировщиков нагрузки, разделение сети и использование протоколов связи.

Сеть интернета вещей представляет собой комплексную систему, состоящую из разных элементов – устройств, собирающих данные; систем и оборудования, которые обрабатывают и анализируют данные; сетевой составляющей для обеспечения передачи данных от устройства к системе управления и обратно.

Таким образом, с учетом наиболее актуальных проблем, возникающих при внедрении промышленного интернета вещей в инфраструктуру и системы организации, будет целесообразно использование совокупности методов обеспечения отказоустойчивости: резервное копирование, протоколы связи, мониторинг состояния сети и оборудования, а также обучение персонала. Совместное применение этих методов гарантирует непрерывность работы сети и минимизирует время простоя в случае сбоев.

Литература

1. *Гаврилов А.* Как повысить отказоустойчивость ИТ-оборудования // ITGLOBAL.COM. 2022. 6 декабря. URL: https://itglobal.com/ru-ru/company/blog/kak-povysit-otkazoustojchivost-it-oborudovaniya/(дата обращения: 15.08.2023).

2. Актуальные киберугрозы: II квартал 2023 года // Positive Technologies. 2023. 29 августа. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 31.08.2023).

3. Кибератаки на российские компании в I квартале 2023 года // Ростелеком-Солар. 2023. 26 апреля. URL: https://rt-solar.ru/analytics/reports/3445/ (дата обращения: 19.08.2023).

4. *Тарасов А.А.* Функциональная реконфигурация отказоустойчивых систем : монография. М. : Логос, 2020. 152 с. ISBN 978-5-98704-654-8. EDN RBBGSL.

5. *Беспалов Д.А., Гушанский С.М., Коробейникова Н.М.* Операционные системы реального времени и технологии разработки кроссплатформенного программного обеспечения : учебное пособие / Южный федеральный университет. Ч. 1. Ростов-на-Дону; Таганрог : Изд-во Южного федерального университета, 2019. 139 с. ISBN 978-5-9275-3367-1. EDN UYZWZD.

6. *Волков М.А.* Информационные технологии : учебное пособие. М.; Вологда : Инфра-Инженерия, 2023. 136 с. ISBN 978-5-9729-1309-1.

7. *Зотов С.В.* Построение отказоустойчивой инфраструктуры SaaS-сервиса // Научно-исследовательские публикации. 2017. № 3 (41). С. 34–42. EDN ZULPKN.

8. *Семенов А.Б.* Структурированные кабельные системы для центров обработки данных : монография. 2-е изд. М. : ДМК Пресс, 2023. 233 с. ISBN 978-5-89818-413-1.

9. Что такое ИТ-инфраструктура // Хостинг Евробайт. 2022. 14 февраля. URL: https://eurobyte.ru/articles/chto-takoe-it-infrastruktura/ (дата обращения: 28.07.2023).

10. *Кенин А.М., Колисниченко Д.Н.* Самоучитель системного администратора. 6-е изд. СПб. : БХВ-Петербург, 2021. 608 с. ISBN 978-5-9775-3629-5.

11. *Савин И.В.* Технология кластеризации для обеспечения отказоустойчивости // Известия Тульского государственного университета. Технические науки. 2019. № 3. С. 191–194. EDN ZTDDXX.

12. *Савин И.В.* Особенности обеспечения отказоустойчивости, сохранности и доступности данных // Известия Тульского государственного университета. Технические науки: научный журнал. 2019. № 3. С. 118–122. EDN NVLXJU.

13. *Купцов С.С.* Исследование методов обеспечения отказоустойчивости вычислительных систем // Форум молодых ученых. 2018. № 6-2 (22). С. 399–403. EDN VKEGCT.

14. *Бопп В.А.* Технология резервного копирования. Преимущества и недостатки // Известия Тульского государственного университета. Технические науки. 2019. № 3. С.134–138. EDN OPJMKX.

15. *Амосов А.* Принципы построения отказоустойчивых ИТ-систем // PC Week. 2016. 11 июля. URL: https://www.pcweek.ua/themes/detail.php?ID=152353 (дата обращения 23.07.2023).

16. Basic fault tolerant software techniques // GeeksforGeeks. 2023. 6 февраля. URL: https://www.geeksforgeeks.org/basic-fault-tolerant-software-techniques/ (дата обращения: 12.08.2023).
17. *Сюй Л.Д., Хе В., Ли С.* «Интернет вещей» в промышленности: обзор ключевых технологий и трендов // Control Engineering Россия. IIoT апрель 2017. С. 12–18. URL: https://controleng.ru/wp-content/uploads/iot_12.pdf (дата обращения: 12.08.2023).
18. *Черепанов Н.В.* Проблемы внедрения технологии промышленного интернета вещей // Инновации и инвестиции. 2019. № 11. С. 160–163. EDN KJWJTS.

References

1. Gavrilov A. (2022) How to increase the fault tolerance of IT equipment. *ITGLOBAL.COM*. December 6. URL: https://itglobal.com/ru-ru/company/blog/kak-povysit-otkazoustojchivost-it-oborudovaniya/ (accessed 15.08.2023). (In Russian).
2. Current cyber threats: The second quarter of 2023. *Positive Technologies*. 2023. August 29. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (accessed 31.08.2023). (In Russian).
3. Cyber-attacks on Russian companies in the first quarter of 2023. *Rostelecom-Solar*. 2023. April 26. URL: https://rt-solar.ru/analytics/reports/3445/ (accessed 19.08.2023). (In Russian).
4. Tarasov A.A. (2020) *Funktsionalnaya reconfiguratsiya otkazoustoychivykh sistem* [Functional reconfiguration of fault-tolerant systems]. Moscow : Logos Publ. 152 p. ISBN 978-5-98704-654-8. (In Russian).
5. Bespalov D.A., Gushansky S.M., Korobeynikova N.M. (2019) *Operatsionnyye sistemy realnogo vremeni i tekhnologii razrabotki krossplatformennogo programmnogo obespecheniya* [Real-time operating systems and cross-platform software development technologies]. Part 1. Rostov-on-Don; Taganrog : Southern Federal University Publ. 139 p. ISBN 978-5-9275-3367-1. (In Russian).
6. Volkov M.A. (2023) *Informatsionnyye tekhnologii* [Information technologies]. Moscow; Vologda : Infra-Engineering Publ. 136 p. ISBN 978-5-9729-1309-1. (In Russian).
7. ZotovS.V. (2017) Building a fail-safe infrastructure for SaaS service. *Nauchno-issledovatelskie publikatsii* [Scientific publications]. No. 3 (41). Pp. 34–42. (In Russian).
8. Semenov A.B. (2023) *Strukturirovannye kabelnye sistemy dlya tsentrov obrabotki dannykh* [Structured cabling systems for data processing centers]. 2nd edition. Moscow : DMK Press. 233 p. ISBN 978-5-89818-413-1. (In Russian).
9. What is IT infrastructure. *Eurobyte*. 2022. February 14. URL: https://eurobyte.ru/articles/chto-takoe-it-infrastruktura/ (accessed 28.07.2023). (In Russian).
10. Kenin A.M., Kolisnichenko D.N. (2021) *Samouchitel sistemnogo administratora* [Tutorial for a system administrator]. 6th edition. St. Petersburg: BHV-Petersburg. 608 p. ISBN 978-5-9775-3629-5. (In Russian).
11. Savin I.V. (2019) Clustering technology for fault tolerance. *Izvestiya Tula State University. Technical sciences*. No. 3. Pp. 191–194. (In Russian).
12. Savin I.V. (2019) Features of ensuring the reliability of stability, preservation and availability of data. *Izvestiya Tula State University. Technical sciences*. No. 3. Pp. 118–122. (In Russian).
13. Kuptsov S.S. (2018) Research of fault tolerance methods of computing systems. *Forum molodykh uchenykh* [Forum of Young Scientists]. No. 6-2 (22). Pp. 399–403. (In Russian).
14. Bopp V.A. (2019) Backup technology. Advantages and disadvantages. *Izvestiya Tula State University. Technical sciences*. No. 3. Pp. 134–138. (In Russian).
15. Amosov A. (2016) Principles of building fault-tolerant IT systems. *PC Week*. July 11. URL: https://www.pcweek.ua/themes/detail.php?ID=152353 (accessed 23.07.2023). (In Russian).

16. Basic fault tolerant software techniques. *GeeksforGeeks*. 2023. February 6. URL: https://www.geeksforgeeks.org/basic-fault-tolerant-software-techniques/ (accessed 12.08.2023).
17. Li Da Xu, Wu He, Shancang Li (2017) "Internet of Things" in industry: An overview of key technologies and trends. *Control Engineering Russia IIoT* April 2017. Pp. 12–18. URL: https://controleng.ru/wp-content/uploads/iot_12.pdf (accessed 12.08.2023). (In Russian).
18. Cherepanov N.V. (2019) Challenges of introduction of Industrial Internet of Things. *Innovation and investment*. No. 11. Pp. 160–163. (In Russian).