УДК 004.052.2

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ АВТОМАТИЗИРОВАННЫХ ИС

Сулейманов А.И.[1], Астапов В.Н.[1]

[1]Самарский Государственный Технический Университет, Самара, e-mail: Artur2378@yandex.ru

Статья посвящена обзору методов и средств, направленных на обеспечение высокой степени надежности автоматизированных информационных систем (ИС). Рассматриваются современные технологии и подходы, используемые для предотвращения и устранения сбоев в функционировании ИС. В статье освещаются аспекты проектирования, тестирования и мониторинга ИС с целью повышения их стабильности и устойчивости к внешним воздействиям. Проанализированы методы оптимизации процессов управления ИС с учетом требований к надежности. Результатом статьи является комплексный обзор современных тенденций и инноваций в области обеспечения надежности автоматизированных информационных систем.

Ключевые слова: надежность, автоматизированные информационные системы, технологии обеспечения надежности, мониторинг, стабильность, устойчивость к сбоям, оптимизация управления, инновации в области надежности.

METHODS AND MEANS OF ENSURING THE RELIABILITY OF AUTOMATED INFORMATION SYSTEMS

Suleymanov A.I.[1], Astapov V.N.[1]

[1]Samara State Technical University, Samara, e-mail: Artur2378@yandex.ru

The article is devoted to an overview of methods and tools aimed at ensuring a high degree of reliability of automated information systems (IS). Modern technologies and approaches used to prevent and eliminate failures in the functioning of IS are considered. The article highlights aspects of the design, testing and monitoring of IP in order to increase their stability and resistance to external influences. Methods of optimization of IP management processes are analyzed, taking into account reliability requirements. The result of the article is a comprehensive review of current trends and innovations in the field of ensuring the reliability of automated information systems.

Keywords: reliability, automated information systems, reliability technologies, monitoring, stability, fault tolerance, management optimization, innovations in the field of reliability.

Введение

В современном информационном обществе, где автоматизированные информационные системы (АИС) стали неотъемлемой частью повседневной жизни и корпоративных процессов,

вопрос обеспечения их надежности становится ключевым аспектом разработки и эксплуатации. С развитием технологий и увеличением объема данных, передаваемых и обрабатываемых в системах, возникают новые вызовы, связанные с обеспечением стабильной, безопасной и эффективной работы автоматизированных информационных систем.

Методы и средства обеспечения надежности АИС призваны удовлетворить растущие требования к стабильности и безопасности информационных технологий. Отказы в работе систем могут привести к серьезным последствиям, включая потерю данных, срыв сроков выполнения задач, а также угрозы для конфиденциальности и целостности информации.

Целью настоящего исследования является рассмотрение основных методов и средств, применяемых для обеспечения надежности автоматизированных информационных систем. В ходе исследования будут рассмотрены современные технологии, стратегии тестирования, алгоритмы защиты от угроз, а также методы восстановления после сбоев. Путем анализа и систематизации этих аспектов предпринимается попытка внести вклад в повышение общего уровня надежности информационных систем, содействуя их бесперебойной и безопасной работе в динамичной цифровой среде.

Данное исследование имеет актуальное значение в контексте постоянного развития информационных технологий и повышения их роли в современном обществе. Результаты и выводы могут быть полезны не только для специалистов в области информационной безопасности и системного администрирования, но и для широкого круга заинтересованных лиц, стремящихся понять и улучшить процессы обеспечения надежности автоматизированных информационных систем.

1 Общие сведения об обеспечении надежности информационных систем

В данной главе рассматриваются основные понятия и принципы, связанные с обеспечением надежности автоматизированных информационных систем. Анализируются актуальность проблемы, важность обеспечения стабильности в функционировании систем, а также выделяются основные вызовы и требования, стоящие перед современными информационными технологиями.

1.1 Актуальность проблемы

В наше современное время, когда информационные технологии проникают во все сферы нашей жизни, актуальность вопросов, связанных с надежностью автоматизированных информационных систем (АИС), становится весьма заметной. Все больше организаций и

частных лиц зависят от бесперебойной работы компьютерных систем для проведения своих операций, обмена информацией и хранения данных.

Основной вызов, с которым сталкиваются современные АИС, заключается в необходимости обеспечивать стабильную и надежную работу в условиях постоянных изменений в технологическом ландшафте и возрастающих угроз безопасности. С каждым днем растет объем обрабатываемой информации, и, соответственно, увеличивается потенциальный ущерб от сбоев в работе системы. [1]

Также, учитывая растущую сложность программных продуктов и увеличивающуюся сетевую взаимосвязь, важно не только предотвращать отказы в работе систем, но и эффективно реагировать на них, восстанавливая работоспособность в минимально возможные сроки.

Данная актуальность проблемы обуславливает необходимость систематического и глубокого анализа методов и средств, используемых для обеспечения надежности АИС. В частности, следует рассмотреть современные стратегии тестирования, анализа уязвимостей, и технологии восстановления после отказов. Понимание этих методов и их рациональное применение становятся фундаментальными для создания стойких к вызовам и устойчивых к сбоям информационных систем.

1.2 Значение обеспечения надежности

В контексте современной цифровой эры значение обеспечения надежности автоматизированных информационных систем (АИС) оказывается фундаментальным для различных сфер деятельности.

Стратегический аспект: обеспечение надежности АИС становится стратегическим фактором для бизнеса. Отказ в работе ключевых информационных систем может привести к серьезным финансовым потерям, утрате клиентов и ущербу репутации. Надежность системы становится неотъемлемой частью стратегического планирования и успешной деятельности организации.

Защита конфиденциальности и целостности: обеспечение надежности системы включает в себя защиту конфиденциальности и целостности данных. Это особенно важно в сферах, где обрабатываются чувствительные данные, такие как персональная информация клиентов, медицинские записи или финансовые транзакции. Гарантированная конфиденциальность и целостность данных укрепляют доверие к системе. [2]

Повышение эффективности бизнес-процессов: надежные информационные системы содействуют бесперебойной работе бизнес-процессов. Они обеспечивают стабильность операций, снижая временные задержки и обеспечивая непрерывный доступ к важной информации. Это, в свою очередь, способствует повышению эффективности деятельности и конкурентоспособности.

Загрязнение информационного шума: в условиях информационного шума, где большое количество данных требует обработки, надежность АИС выступает в роли фильтра, позволяя выделять важную информацию и минимизировать воздействие информационного шума. Это позволяет пользователям более эффективно взаимодействовать с данными, сосредотачиваясь на существенной информации.

Все эти аспекты подчеркивают, что обеспечение надежности АИС имеет глубокие и многогранные последствия для бизнеса, безопасности данных и взаимодействия с пользователями. Это становится необходимым условием для успешного функционирования в современной информационной среде.

1.3 Вызовы и требования

Сложность и динамичность информационных технологий создают ряд вызовов и требований к обеспечению надежности автоматизированных информационных систем (АИС). Рассмотрим ключевые аспекты этого подраздела.

Требования к адаптивности: современные АИС должны быть готовы к постоянным изменениям в технологической среде. Требуется не только обеспечение стабильной работы в текущих условиях, но и гибкость в адаптации к новым технологиям, стандартам и бизнес-процессам.[3]

Методы тестирования и оценки надежности: развитие сложных АИС требует совершенствования методов тестирования и оценки надежности. Критически важно выявлять потенциальные уязвимости и дефекты в системе на ранних этапах разработки, чтобы предотвратить их влияние на более поздних этапах.

Обучение персонала: пользователи и администраторы систем играют ключевую роль в обеспечении надежности. Эффективные программы обучения не только повышают компетентность персонала, но и содействуют сознательности в вопросах безопасности.

Соблюдение регулирований: в условиях строгих регуляторных требований в различных отраслях, обеспечение соответствия стандартам и законодательству становится неотъемлемым элементом обеспечения надежности.

Все эти вызовы и требования указывают на необходимость постоянного совершенствования методов обеспечения надежности АИС и подчеркивают динамичный характер этой области.

2 Методологии и подходы к обеспечению надежности

В этой главе рассматриваются различные методологии и подходы к обеспечению надежности автоматизированных информационных систем. Освещаются основные стратегии тестирования, анализа и обеспечения безопасности. Приводятся примеры успешных практик в области обеспечения надежности.

Методологии тестирования надежности

Методологии тестирования играют решающую роль в обеспечении надежности АИС. Различные стратегии, такие как функциональное, нагрузочное, исследовательское тестирование и тестирование на уязвимости, используются для выявления дефектов и проблем в работе системы. Регулярное и систематическое тестирование позволяет выявлять и устранять проблемы на ранних стадиях разработки, повышая уровень надежности.

Методологии управления рисками

Эффективное управление рисками включает в себя методологии для идентификации, анализа и оценки потенциальных угроз. Методы качественной и количественной оценки рисков помогают организациям принимать обоснованные решения относительно того, какие меры по обеспечению надежности следует принимать. Включение процесса управления рисками в жизненный цикл АИС способствует созданию более устойчивых и безопасных систем.

Принципы "безопасность по умолчанию"

Методологии разработки, основанные на принципе "безопасность по умолчанию", предполагают, что система должна быть построена с максимальной степенью безопасности изначально. Интеграция безопасности во все аспекты разработки, начиная с архитектуры и заканчивая кодированием, способствует созданию стабильных и защищенных АИС. [4]

Интеграция принципов DevOps

Принципы DevOps интегрируют процессы разработки и эксплуатации, обеспечивая непрерывность и автоматизацию. Это способствует более быстрой реакции на изменения и устранение дефектов. Использование DevOps-методологий также ускоряет выдачу обновлений и позволяет эффективно внедрять новые меры безопасности и надежности.

Постоянное улучшение и оценка

Методологии обеспечения надежности должны включать в себя стратегии постоянного улучшения и оценки. Регулярные аудиты безопасности, анализ инцидентов, сбор обратной связи от пользователей и постоянное обновление методов и инструментов являются неотъемлемой частью процесса обеспечения надежности АИС.

3 Технологии и инструменты обеспечения надежности

В данной главе рассматриваются современные технологии и инструменты, используемые для обеспечения надежности автоматизированных информационных систем. Происходит анализ средств тестирования, систем контроля доступа, средств защиты от вредоносных атак, а также инструментов резервирования и восстановления данных.

Мониторинг и аналитика

В данном контексте, мониторинг включает в себя использование инструментов, таких как **Prometheus, Nagios и ELK Stack**, для постоянного отслеживания состояния системы. Эти средства предоставляют реальное время видимости в производительность, доступность и безопасность компонентов системы. Аналитика, осуществляемая с использованием инструментов типа **Splunk и Grafana**, помогает обрабатывать и анализировать данные мониторинга, выявлять аномалии и предоставлять ценные инсайты.

Автоматизированное тестирование и тестирование нагрузки

Инструменты автоматизированного тестирования, такие как **Selenium, JUnit и Appium**, позволяют автоматизировать процессы тестирования функциональности и стабильности системы. Это сокращает время, необходимое для тестирования, и обеспечивает регулярность процесса. Инструменты тестирования нагрузки, вроде **Apache JMeter и Gatling**, используются для моделирования нагрузки и оценки производительности системы под различными условиями.

Средства обеспечения безопасности

В области безопасности используются программы антивирусной защиты, такие как **Kaspersky и McAfee**, чтобы обнаруживать и блокировать вредоносные программы. Также применяются системы обнаружения вторжений (IDS), такие как **Snort и Suricata**, для мониторинга сетевой активности и выявления подозрительных действий. Эти инструменты обеспечивают высокий уровень защиты от внешних и внутренних угроз. [6]

Использование искусственного интеллекта и машинного обучения

Алгоритмы машинного обучения и искусственного интеллекта применяются для анализа данных, выявления аномалий и предсказания возможных проблем. Эти технологии значительно повышают эффективность системы в предотвращении отказов, предоставляя интеллектуальные инструменты для обработки данных и выявления изменений в нормальном поведении системы.

Принципы безопасного программирования

Использование методов безопасного программирования становится ключевым элементом в создании устойчивых к атакам приложений. Это включает в себя правильное управление аутентификацией и авторизацией, санитарное программирование, шифрование данных, и другие практики, направленные на предотвращение уязвимостей и атак.

Все эти технологии и инструменты совместно обеспечивают комплексное обеспечение надежности АИС, позволяя эффективно предотвращать сбои, обеспечивать безопасность данных и обеспечивать стабильность работы системы. [7]

Заключение

В первой главе работы были рассмотрены общие принципы обеспечения надежности, включая понятия и методы расчета надежности. Во второй главе были затронуты вопросы методологии и подходов к обеспечению надежности, выделяя важность внедрения принципов безопасного программирования, регулярных аудитов безопасности и обучения персонала.

В третьей главе, посвященной технологиям и инструментам обеспечения надежности, была подчеркнута роль мониторинга и аналитики, автоматизированного тестирования, средств безопасности, резервного копирования и восстановления, а также было рассмотрено применение искусственного интеллекта и машинного обучения.

В процессе изучения различных программных комплексов был выявлен ряд успешных практик, таких как непрерывное тестирование, принципы безопасного программирования,

регулярные аудиты безопасности и использование искусственного интеллекта для анализа данных.

В работе особенно отмечено, что обеспечение надежности АИС — это многогранный процесс, требующий комплексного подхода, включающего технические, методологические и организационные аспекты. Результаты сравнительного анализа программных комплексов предоставляют ценную информацию для выбора наилучших решений в конкретных контекстах применения.

Однако, следует отметить, что область обеспечения надежности АИС постоянно развивается, и компании должны быть готовы к инновациям, постоянному обучению и улучшению своих практик.

Список использованной литературы

1. Майерс Г. Надёжность программного обеспечения/Мир. – М., 1980. – 360 с.
2. Липаев В.В. Надёжность программных средств /СИНТЕГ. – М., 1998. – 232 с.
3. Бандурова Елизавета Евгеньевна, Омельченко Татьяна Александровна МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ НАДЕЖНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ СИСТЕМ // NBI-technologies. 2021. №4. URL: https://cyberleninka.ru/article/n/mehanizmy-obespecheniya-nadezhnosti-obektov-informatsionnyh-sistem (дата обращения: 29.11.2023).
4. ГОСТ 27.001-95. Межгосударственный стандарт. Система стандартов "Надежность в технике". Основные положения. Минск: Межгосударственныйсовет по стандартизации, метрологии и сертификации, 1997 –3 с.
5. Смирнов О. С. Метод обеспечения надежности промышленных информационных систем // Управление инновациями: теория, методология, практика. 2012. №1. URL: https://cyberleninka.ru/article/n/metod-obespecheniya-nadezhnosti-promyshlennyh-informatsionnyh-sistem (дата обращения: 29.11.2023).
6. Казарин, О. В. Методология защиты программного обеспечения. Научные проблемы безопасности и противодействия терроризму / О.В. Казарин. - М.: МЦНМО, 2009. - 464 с.
7. Котляров, В. П. Основы тестирования программного обеспечения / В.П. Котляров, Т.В. Коликова. - М.: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2006. - 288 с.