Вахрушев А.В. Системный подход в качестве надежности информационных систем // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 4(42) с. 120–127

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.052

СИСТЕМНЫЙ ПОДХОД В КАЧЕСТВЕ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Вахрушев А.В.
ФГБОУ ВО "КАЛУЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. К.Э. ЦИОЛКОВСКОГО", Калуга, Россия (248023, Калужская область, город Калуга, ул. Степана Разина, д.26), e-mail: ppetrov@yandex.ru

В данной статье исследуется системная инженерия и раскрывается суть системного подхода в обеспечении надежности информационных систем. Эта тема актуальна во всех областях применения информационных систем, включая стратегические и бизнес-процессы, где необходимо обеспечить высокое качество и надежность системы.

Ключевые слова: Оптимизация, надежность, информационная система.

A SYSTEMATIC APPROACH TO THE RELIABILITY OF INFORMATION SYSTEMS

Vakhrushev A.V.
KALUGA STATE UNIVERSITY. K.E. TSIOLKOVSKY", Kaluga, Russia (248023, Kaluga region, Kaluga city, Stepana Razina st., 26), e-mail: ppetrov@yandex.ru

This article explores system engineering and reveals the essence of a systematic approach to ensuring the reliability of information systems. This topic is relevant in all areas of information systems application, including strategic and business processes, where it is necessary to ensure high quality and reliability of the system.

Keywords: optimization, reliability, information system.

Введение

Суть системного подхода заключается в том, чтобы рассматривать каждый объект как часть более общей системы и в то же время как самостоятельную сложную систему. В современном мире развитие различных областей человеческой деятельности невозможно без широкого использования компьютеров и создания информационных систем. По мере возрастания сложности проектируемых систем, важное значение приобретают такие общесистемные вопросы, как выбор оптимальной структуры системы, определение наилучшего взаимодействия между ее элементами и оптимальных режимов их работы. Необходимость решения этих вопросов привела к появлению системного подхода к анализу больших систем. Основой системного подхода служит теория систем, разработанная биологом Л. фон Берталанфи. Кроме того, было разработано направление, названное исследованием операций, которое возникло в связи с военными задачами. Несмотря на широкое использование в других областях, первоначальная терминология этого направления часто сложно применима на практике.

Основная часть

Надежность - это способность объекта выполнять свои функции в течение определенного времени и в пределах установленных показателей. Объект может быть техническим изделием определенного назначения, которое рассматривается в процессе проектирования, производства, испытаний и эксплуатации. Эти объекты могут включать в себя различные системы и их элементы. Элемент - это простая составная часть изделия, которая в контексте надежности может быть составлена из множества деталей. Система - это совокупность взаимодействующих элементов, предназначенных для выполнения определенных функций в автономном режиме. Понятия элемента и системы могут меняться в зависимости от поставленной задачи. Например, станок может рассматриваться как система, состоящая из различных элементов, таких как механизмы и детали, при анализе его надежности, а при изучении надежности технологической линии он может рассматриваться как элемент.

Организации, которые стремятся к обеспечению надежности, обычно работают в средах, которые являются взаимодейственно сложными. Взаимодейственная сложность увеличивается, когда результаты неизвестны и могут быть потенциально неожиданными, когда социально-технические системы имеют несовместимые функции, и когда информационный поток является косвенным и неоднозначным. Тесная связь включает "процессы, зависимые от времени", "непрерывные последовательности операций", "единственный способ достичь цели" и "небольшую слабину". Отказы являются "неотъемлемыми свойствами" взаимодейственно сложных и тесно связанных систем, так как аварии, которые невозможно предвидеть или предотвратить, неизбежны в таких системах. Это "нормальные несчастные случаи". Среды, такие как строительство или программы информационной безопасности, которые требуют значительного управления технологиями и инфраструктурой, имеют высокий уровень социальной и технической взаимосвязи. В таких условиях люди, сложные технологии и материальные активы становятся критически зависимыми друг от друга. Эта взаимосвязь означает, что ошибка в любом конкретном процессе или деятельности может быстро привести к более серьезным событиям и потенциально привести к дестабилизации или сбою в целом, особенно в непредсказуемых процессах, таких как разработка программного обеспечения и управление.

Делоне и Маклин (1992 г.) предложили шесть критериев для оценки успешной работы информационной системы:

1. Качество информационной системы;
2. Качество предоставляемой информации;
3. Уровень использования информационной системы;
4. Удовлетворенность пользователей;
5. Влияние информационной системы на поведение пользователей;
6. Воздействие информационной системы на организацию.

Для полноценной оценки успешности информационной системы необходимо учитывать критерии, такие как качество самой информационной системы, качество предоставляемых ею данных, использование системы, удовлетворенность пользователей, воздействие системы на пользователей и ее влияние на организацию и ее эффективность.

Акцент на надежности также крайне важен, особенно в условиях конкуренции между организациями и на стратегически значимых объектах. Часто организации предпочитают не жертвовать надежностью ради повышения производительности. Если организации сосредотачиваются только на текущей прибыли, не учитывая издержек, связанных с обеспечением надежности информационных систем, они, скорее всего, столкнутся с потерей прибыли и значительными затратами при внедрении систем информационной безопасности.

Модель успешности информационных систем не может быть полной без надежной и устойчивой работы систем. В связи с повторяющимися сбоями в информационных системах, обеспечение надежности программного обеспечения может стать важной составляющей задач управления проектами. Разработка концепции надежности программного обеспечения может помочь менеджерам проектов не только выполнить поставленные задачи быстрее, но и обеспечить надежность программных продуктов, а также бесперебойную работу систем через резервирование и возможность многократного дублирования.

Общее понимание системного подхода в контексте информационных систем

Подход системы в информационных системах означает, что мы рассматриваем информационную систему в целом, а не как отдельные части, и учитываем, как их взаимодействие друг с другом и с внешней средой. Это помогает нам понять, что информационная система не только состоит из компонентов, таких как оборудование, программное обеспечение, сети и базы данных, но также включает процессы обработки информации, управления и безопасности данных. Мы видим информационную систему в ее полной сложности и динамике.

Другим важным аспектом системного подхода для информационных систем является учет влияния внешних факторов, таких как угрозы безопасности, изменения в бизнес-процессах или технологические новшества. Мы понимаем информационную систему как открытую систему, взаимодействующую со внешней средой, и учитываем эти внешние воздействия, чтобы приспосабливать систему к изменяющимся условиям.

Таким образом, системный подход для информационных систем предполагает рассмотрение системы в целом и ее взаимосвязи с внешним миром. Это помогает нам понимать систему в ее целостности и разрабатывать эффективные стратегии обеспечения ее надежности и устойчивости.

Анализ системы как целого

Анализ системы в целом - это метод и процесс изучения всех ее компонентов, процессов и взаимосвязей с точки зрения цельности. Этот подход помогает понять, как части системы взаимодействуют друг с другом и как эти взаимодействия влияют на работу системы в целом.

Анализ системы в целом включает в себя несколько аспектов:

1. Исследование структуры: изучение всех компонентов системы, их функций и взаимосвязей, включая аппаратное и программное обеспечение, структуру данных и сетевые элементы.
2. Процессы: изучение процессов, происходящих внутри системы, таких как обработка данных, взаимодействие между компонентами и управление ресурсами.
3. Взаимодействие с окружающей средой: учитывание взаимодействия системы с внешней средой, другими системами, пользователями, а также окружающими технологическими и бизнес-процессами.

4. Оценка производительности: изучение производительности системы, включая скорость работы, надежность и масштабируемость.

Цель анализа системы в целом заключается в создании полного и точного представления о ее работе в естественной среде, выявлении уязвимостей, рисков и проблем, а также разработке стратегий для улучшения работы системы, ее надежности и безопасности.

Обеспечение безопасности информационной системы

Обеспечение безопасности информационной системы означает защиту информации от несанкционированного доступа, вирусов, вторжений и утечек. Вот что включает в себя обеспечение безопасности информационной системы:

1. Защита от внешних угроз:
- Используются технологии, такие как брандмауэры и прокси-серверы, для обнаружения и предотвращения вторжений и вирусов.
2. Управление доступом:
- Разрабатываются стратегии управления правами доступа, аутентификация пользователей и мониторинг активности для предотвращения несанкционированного доступа.
3. Шифрование данных:
- Для защиты конфиденциальности и целостности данных используются криптографические методы.
4. Контроль целостности информации:
- Осуществляется контроль изменений в данных для обнаружения несанкционированного доступа или модификаций.
5. Аудит и мониторинг:
- Устанавливаются системы аудита и мониторинга для отслеживания действий пользователей и системных событий.
6. Физическая безопасность:
- Обеспечивается безопасность оборудования и помещений, где хранится критическая информация.
7. Обучение персонала:
- Сотрудники проходят обучение по безопасности информации и ознакамливаются с политикой безопасности.

Обеспечение безопасности информационных систем требует комплексного подхода, начиная от технических мер безопасности и заканчивая обучением персонала и разработкой стратегий реагирования на инциденты.

Анализ рисков и уязвимостей

Анализ рисков и уязвимостей в информационных системах - это процесс выявления и оценки потенциальных опасностей, которые могут негативно повлиять на работоспособность, конфиденциальность, целостность и доступность информации. Ниже приведены основные аспекты этого процесса:

1. Идентификация уязвимостей:
- Определение слабых мест в информационной системе, которые могут быть использованы злоумышленниками для несанкционированного доступа или атак.
2. Оценка вероятности и последствий:

- Оценка вероятности возникновения определенной угрозы и возможных последствий для информационной системы, включая финансовые потери, ухудшение репутации, нарушение бизнес-процессов и другие негативные последствия.

3. Разработка стратегий управления рисками:

- После выявления уязвимостей и оценки рисков, разрабатываются стратегии управления рисками, включая выбор технических, организационных и процедурных мер для смягчения рисков до приемлемого уровня.

4. Улучшение безопасности:

- На основе анализа рисков и уязвимостей принимаются меры по устранению или снижению уязвимостей, повышению защищенности и улучшению реагирования на угрозы.

5. Постоянный мониторинг и обновление:

- Процесс анализа рисков и уязвимостей должен быть постоянным, включая систематический мониторинг, обновление методов и технологий безопасности, а также адаптацию стратегий управления рисками к изменяющимся условиям и угрозам.

Анализ рисков и уязвимостей является важным этапом управления информационной безопасностью, направленным на предотвращение возможных проблем и минимизацию потенциальных угроз для информационной системы.

Восстановление и реагирование

Восстановление и реагирование в информационной безопасности - это процессы, которые направлены на восстановление работоспособности информационной системы после возникновения инцидента или нарушения безопасности, а также на предотвращение развития инцидента и минимизацию ущерба. Вот некоторые ключевые аспекты восстановления и реагирования:

1. Разработка плана реагирования на инциденты:

- Необходимо иметь четкий план действий, описывающий процедуры реагирования на различные виды инцидентов.

2. Обнаружение инцидентов:

- Разработка механизмов для быстрого обнаружения инцидентов безопасности.

3. Меры по устранению инцидента:

- Принятие мер по прекращению инцидента и минимизации его воздействия на информационную систему и бизнес-процессы.

4. Восстановление работоспособности:

- Восстановление систем и данных до нормального состояния после инцидента.

5. Анализ инцидента:

- Оценка последствий инцидента для выявления уязвимостей и организационных уроков, а также для предотвращения подобных инцидентов в будущем.

6. Улучшение процессов и профилактические меры:

- Внедрение улучшений в процессы реагирования и проактивные меры по предотвращению возможных угроз и инцидентов.

Восстановление и реагирование в информационной безопасности играют важную роль в обеспечении безопасности информационных систем и минимизации последствий возможных инцидентов. Реагирование на инциденты, оперативное восстановление и обучение на основе

анализа инцидентов позволяют улучшить защиту и повысить надежность информационных систем.

Заключение

Рассмотрение информационной системы с системным подходом имеет ряд преимуществ и является критически важным для обеспечения безопасности, эффективности и устойчивости информационных систем. Вот почему:

1. Целостность: Системный подход учитывает информационную систему как целое, что помогает предотвратить изоляцию уязвимых мест и улучшить целостность системы.
2. Комплексный анализ: Определение уязвимостей и рисков путем комплексного анализа всех компонентов и процессов системы.
3. Предотвращение каскадных отказов: Использование системного подхода позволяет выявить возможные каскадные отказы, что позволяет принимать меры для их предотвращения.
4. Обоснованные решения: Системный подход обеспечивает полное понимание информационной системы, что помогает принимать обоснованные решения, направленные на улучшение безопасности и надежности.
5. Улучшение управления рисками: Анализ системы как целого дает более точную оценку рисков и уязвимостей, что способствует разработке стратегий управления рисками и принятию мер для уменьшения уровня рисков.

Таким образом, системный подход играет важную роль в обеспечении надежности информационных систем, позволяя комплексно рассматривать систему, выявлять уязвимости, разрабатывать стратегии управления рисками и обеспечивать подходящее управление безопасностью.

1. Исследования: Для дальнейших исследований следует обратить внимание на следующие аспекты:
   - Разработка методов системного анализа и моделирования информационных систем с учетом их надежности и безопасности.
   - Проверка эффективности системного подхода в реальных условиях эксплуатации информационных систем различных масштабов.
   - Исследование влияния различных видов угроз на надежность информационных систем и создание методов для обнаружения, предотвращения и управления рисками.
2. Практическое применение: Для практического применения следует обратить внимание на следующие моменты:
   - Внедрение системного подхода в стратегии обеспечения информационной безопасности и управления рисками на уровне организации.
   - Интеграция системного подхода в процессы управления информационной безопасностью, включая разработку обучающих программ для персонала и оценку эффективности управления рисками.
3. Развитие технологий: Необходимо следить за развитием технологий и инструментов, поддерживающих системный подход в обеспечении надежности информационных систем, включая средства мониторинга, системы управления уязвимостями, технологии обнаружения вторжений и другие.

Продвижение исследований и разработка практической реализации системного подхода помогут эффективнее обеспечивать надежность и безопасность информационных систем, что в свою очередь способствует защите конфиденциальности, целостности и доступности информации.

Список литературы

1. "Information Security Management Handbook" (Хэндбук управления информационной безопасностью) от Tipton, Harold F., и Micki Krause.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems" ("Инженерия безопасности: Руководство по созданию надежных дистрибутивных систем") от Ross J. Anderson.
3. "Computer Security: Principles and Practice" ("Компьютерная безопасность: принципы и практика") от William Stallings и Lawrie Brown.
4. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies" ("Руководство по информационной безопасности: эффективные стратегии компьютерной безопасности и управления рисками") от Corey Schou и Steven Hernandez.
5. "Introduction to System Safety Engineering" ("Введение в инженерию систем безопасности") от Phil Hughes.
6. Делоне, В. Х.; Маклин, Э. (1992). «Успех информационных систем: поиски зависимой переменной». Информационные системы исследования. 3 (1): С.60–95. Дои:10.1287 / isre.3.1.60.
7. Делоне, В. Х. и Маклин, Э. (2002). Возвращение к успеху информационных систем. Материалы 35-й Гавайской международной конференции по системным наукам (HICSS), Большой остров, Гавайи, С.238-249.
8. Делоне, В. Х.; Маклин, Э. (2003). «Модель успеха информационных систем Делона и Маклина: последние десять лет». Журнал информационных систем управления. 19 (4): С.9–30.
9. Евдокимов О.Г., Гавдан Г.П., Резниченко С.А. Подход к оценке эффективности системы обеспечения информационной безопасности распределенной системы передачи данных // Безопасность информационных технологий. 2022. Т. 29. № 2. С. 57-70.
10. Забелина В.А., Ахвердиев В.И., Гоголь И.В., Овчинников С.С., Нестеров Ю.Г., Кротов Ю.Н. Создание рекомендательной системы для интернетмагазина на основе гибридной интеллектуальной информационной системы // Труды Международного научно-технического конгресса "Интеллектуальные системы и информационные технологии - 2022" ("ИС & ИТ-2022", "IS&IT'22"). Таганрог, 2022. С. 254-262

References

1. "Information Security Management Handbook" by Tipton, Harold F., and Mickey Krause.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross J. Anderson.
3. "Computer Security: Principles and Practice" ("Computer security: principles and practice") by William Stallings and Lawrie Brown.
4. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies" ("Information Security Handbook: Effective Computer Security and Risk

Management Strategies") from Corey Schou and Steven Hernandez.
5. "Introduction to System Safety Engineering" by Phil Hughes.
6. Delaunay, V. H.; McLean, E. (1992). "The success of information systems: the search for a dependent variable." Research information systems. 3 (1): 60–95. Doi:10.1287 / isre.3.1.60.
7. Delaunay, V. H. and McLean, E. (2002). Return to the success of information systems. Proceedings of the 35th Hawaii International Conference on Systems Sciences (HICSS), Big Island, Hawaii, pp. 238-249.
8. Delaunay, V. H.; McLean, E. (2003). "Delon and McLean's Information Systems Success Model: The last Ten Years." Journal of Management Information Systems. 19 (4): pp. 9–30.
9. Evdokimov O.G., Gavdan G.P., Reznichenko S.A. An approach to evaluating the effectiveness of the information security system of a distributed data transmission system // Information technology security. 2022. Vol. 29. No. 2. pp. 57-70
10. .Zabelina V.A., Akhverdiev V.I., Gogol I.V., Ovchinnikov S.S., Nesterov Yu.G., Krotov Yu.N. Creation of a recommendation system for an online store based on a hybrid intelligent information system // Proceedings of the International Scientific and Technical Congress "Intelligent Systems and Information Technologies - 2022" ("IS & IT-2022", "IS&IT'22"). Taganrog, 2022. pp. 254-262