Автоматизация и моделирование в проектировании и управлении. 2025. № 4 (30). С. 65-70.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2025. № 4 (30). P. 65-70.

Научная статья
Статья в открытом доступе
УДК 65.01
doi: 10.30987/2658-6436-2025-4-65-70

ПРОЕКТИРОВАНИЕ СИСТЕМ МОНИТОРИНГА И АЛГОРИТМОВ В ЦЕЛЯХ МИТИГАЦИИ РИСКОВ ИСКАЖЕНИЯ ДАННЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ОЦЕНКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Антон Олегович Попов[1], Сергей Александрович Шептунов[2], Татьяна Владимировна Карлова[3]
[1, 2, 3] Институт конструкторско-технологической информатики Российской академии наук, г. Москва, Россия
[1] kraz12345@mail.ru
[2] ship@ikti.ru
[3] karlova-t@yandex.ru

Аннотация. *Провелось исследование проблематики проектирования процесса мониторинга рисков искажения данных в целях повышения достоверности оценки эффективности деятельности предприятия на основе моделей и алгоритмов. Цель исследования в обосновании важности разработки автоматизированного подхода к проектированию процесса мониторинга и алгоритмов для реализации эффективного контроля достоверности данных, выявления ошибок и принятия необходимых решений для их устранения. Применены такие методы, как анализ существующих и разработка новых моделей и алгоритмов, тестирование на реальных данных. Результаты исследования применимы в разных отраслях деятельности современных предприятий, в которых ключевым аспектом деятельности выступает электронный документооборот, таких как финансовый и производственный сектор, питание и т.д.*

Ключевые слова: управление, риски, модели, информация, безопасность, данные, предприятия, алгоритмы, эффективность

Для цитирования: Попов А.О., Шептунов С.А., Карлова Т.В. Проектирование систем мониторинга и алгоритмов в целях митигации рисков искажения данных для обеспечения достоверности оценки эффективности деятельности предприятия // Автоматизация и моделирование в проектировании и управлении. 2025. №4 (30). С. 65-70. doi: 10.30987/2658-6436-2025-4-65-70.

Original article
Open Access Article

DESIGN OF MONITORING SYSTEMS AND ALGORITHMS TO MITIGATE DATA DISTORTION RISKS FOR ENSURING VALIDITY OF ENTERPRISE PERFORMANCE EVALUATION

Anton O. Popov[1], Sergey A. Sheptunov[2], Tatyana V. Karlova[3]
[1, 2, 3] Institute for Design-Technological Informatics of the Russian Academy of Sciences, Moscow, Russia
[1] kraz12345@mail.ru
[2] ship@ikti.ru
[3] karlova-t@yandex.ru

Abstract. *The study investigates the challenges associated with designing a process for monitoring data distortion risks to ensure validity of enterprise performance evaluation based on models and algorithms. The research aim is to emphasize the importance of developing an automated approach to designing a monitoring process and algorithms for carrying out effective control of data validity, detecting errors, and making necessary decisions for their elimination. The study employs such methods as analysing existing models and algorithms, developing new ones, and empirical testing on real-world data. The findings are applicable across various sectors of modern enterprise activities where electronic document circulation is crucial, including finance, manufacturing, food services, etc.*

Keywords: management, risks, models, information, security, data, enterprises, algorithms, efficiency

For citation: Popov A.O., Sheptunov S.A., Karlova T.V. Design of Monitoring Systems and Algorithms to Mitigate Data Distortion Risks for Ensuring Validity of Enterprise Performance Evaluation. Automation and modeling in design and management, 2025, no. 4 (30). pp. 65-70. doi: 10.30987/2658-6436-2025-4-65-70.

Введение

Необходимость информатизации является важной составляющей развития современного предприятия. С быстрым развитием научно-технического прогресса информатизация стала для предприятий важным средством повышения конкурентоспособности и адаптации к требованиям рынка. Важным аспектом деятельности любой организации является информационный поток, который обеспечивает существование любой системы предприятия, внутри которого они передаются. Стремительный рост объема данных в информационном потоке предприятия, ввиду значимости данных для принятия эффективных управленческих решений, является критическим фактором при управлении предприятием и требует определенных подходов при обработке и хранении данных для обеспечения их неизменности.

С высокой скоростью роста количества предприятий и их масштаба, основной деятельностью которых является предоставление услуг в интернете, а также постоянной цифровой трансформации бизнес-процессов в различных сферах, скорость возрастания объемов информации определяет небезопасность искажения данных. В настоящее время искажение данных становится одним из самых серьезных угроз безопасности, которая исходит от неконтролируемости использования информации внутренним персоналом. Внедрение эффективных мер безопасности, таких как шифрование данных, управление доступом и регулярные аудиты безопасности, становится критически важным.

В связи с вышесказанным, растет потребность в требованиях по обеспечению достоверности и надежности данных, что повышает потребность в системах мониторинга, отслеживающих риски искажения данных и аналитики, не соответствующей текущему состоянию по процессам и продуктам, ведущей к дальнейшим финансовым потерям.

Актуальность исследования проблематики современного подхода к проектированию систем мониторинга с целью минимизации рисков искажения данных при их обработке и хранении обусловлена критичностью значимости таких данных для предприятий.

При проектировании систем мониторинга необходимо учитывать различные комплексные факторы, влияющие на обработку и хранение информации для обеспечения информационной безопасности. В таких условиях необходимо выстраивать не только устойчивые решения, но и имеющие высокий уровень автоматизации, возможность масштабируемости и адаптации к постоянно изменяющимся требованиям, а также росту предприятия.

Цель исследования в подробном рассмотрении возможности применения системы мониторинга, для выявления потенциальных рисков искажения данных в организации, и их дальнейшего устранения.

В соответствии с целью сформулированы следующие задачи:

– определить источники искажения данных и проанализировать текущие требования к средствам контроля общего и прикладного назначения по снижению рисков получения избыточных привилегий, а также существующие подходы к проектированию мониторинга и сохранению целостности данных;

– описать и разработать пример процессов, влияющих на доступ к хранимым данным;

– разработать на основании примеров процессов систему мониторинга, которая будет применима для минимизации рисков искажения данных;

– оценить эффективность разработанной системы, сформировать рекомендации по внедрению адаптируемой системы мониторинга, сформулировать вывод.

Методология исследования

В условиях активного развития цифровой экономики и стремления множества организаций к развитию цифровой среды обнаруживается множество недостатков, связанных с консистентностью и безопасностью искажения данных, а также своевременностью принимаемых решений высшего менеджмента.

Информационные данные, возникающие в результате деятельности процессов организации, основанных на совокупности технических, технологических и организационных компонентов, в том числе относятся к количественным данным, применяющимся при: во-первых, формировании показателей деятельности организации для оценки эффективности и принятии управленческих решений; во-вторых, при других процессах предприятия, так как процессы предприятия могут быть взаимосвязаны между собой, в том числе основываться на ранее полученных результатах.

Информационные данные играют важную роль в управлении любым предприятием, ввиду чего достоверность таких данных имеет большое значение для управления предприятием, что повышает уровень зависимости от качества информационных данных. В виду повышенного объема данных и большого количества их процессов-производителей, возрастают риски искажения данных, по результатам как технических нюансов реализации процессов, так и в результате человеческого фактора. Искажения таких типов зачастую носят скрытый характер, увеличивая сложность дальнейшего расследования причин, выступая одной из причин неэффективных или не своевременно принятых управленческих решений. Наиболее актуальным этот вопрос становится при построении долгосрочной стратегии в условиях высокой изменчивости внешней среды.

Проблемы безопасности информационных данных, связанных с их искажением в цифровой среде, требуют комплексного подхода для выявления влияющих факторов, где один из первичных вопросов – это рассмотрение внутренних источников возникновения искажения. Не качественная информация приводит к не корректным решениям, основанным на не отображающих текущую ситуацию показателям. Особенно это критично для организаций, имеющих высокую нагрузку на информационные системы, и межсистемной интеграции.

Необходимо также принимать во внимание, что повышение контролируемости бизнес-процессов требует затраты зачастую больших ресурсов, в том числе человеческих и временных, которые могут быть материально не обоснованные, ввиду чего предприятия, особенно крупные, приоретизируют анализ рисков процессов, выставляя приоритет выше процессам, в которых реализация потенциальных не контролируемых рисков повлечет за собой существенные финансовые или репутационные потери. Такой подход, обусловленный ограничением ресурсов и массовостью процессов остается вне зоны контролей, что при некоторых условиях может иметь накопительный результат с дальнейшими существенными финансовыми потерями. Такой подход, несмотря на отрицательные стороны, является одним из наиболее эффективных при повышении контролируемости процессов.

Современным предприятиям необходимо обеспечивать достоверность данных на всех этапах жизненного цикла процессов от момента генерации до использования в других процессах, или аналитических целях. Актуальность исследования обоснована растущей потребностью в разработке методологических подходов к повышению устойчивости среды к рискам искажения, а также в необходимости в формировании единой системы контроля, где это технически возможно.

В виду вышеперечисленного на текущий момент имеется высокая потребность в разработке подхода мониторинга возникновения потенциальных рисков (известных или не известных) искажения информационных данных, включающих особенности архитектуры системы, факторов, которые влияют на возникновение искажения данных и требований. Важным аспектом исследования является анализ текущих практик контролирования рисков с целью выявления потенциальных искажений, а также выявления областей, требующих улучшения.

В текущем контексте актуальность приобретают информационно технологические общие контроли (ИТ-контроли), основными целями которых являются: обеспечение безопасности данных, соответствие нормативным требованиям, снижение рисков, повышение эффективности. Доступ к системам и компонентам систем, согласно основным принципам ИТ-контролей, должен базироваться на регламентном, авторизированном, разграниченном доступе.

Для снижения рисков искажения данных в цифровой системе организации используется система ИТ-контролей, связанных между собой, нацеленных в том числе на эффективность механизмов контроля доступа для изменения информации, в частности – к базам данных, как к одному их ключевых хранилищ информации, на которых в текущей статье сделан анализ и разработан подход к разработке мониторинга. В рамках ИТ-контролей с целью сохранения качества данных можно выделить следующие: контроль доступа, контроль изменений, контроль эксплуатации, контроль точности и полноты данных. Так как каждый контроль представляет множественный набор процедур – в данной работе сосредоточимся на контроле доступа, а именно на рисках, связанных с избыточностью прав. Выбор данной категории контролей и категорий рисков обусловлен фундаментальной ролью в сохранении информации при ограниченности ресурсов.

Каждая организация стремится унифицировать процесс выдачи прав в компоненты цифровой системы, выполняя это посредством одного решения, который может являться как

одним из модулей цифрового стороннего продукта, так и сервисной архитектурой разработанной самой компанией. Между системой управления доступом и иными компонентами, в том числе базами данных, должна быть налажена интеграции по выдаче ролей пользователям, в том числе через отдельный сервис, который учитывает специфики различных компонентов, в том числе различных типов систем управления базами данных, а также необходимых архитектурных решений, зависящих от роли применения типов баз данных. В типовом случае можно сказать, что доступ на изменение данных не должны иметь сотрудники, основной деятельностью которых не является поддержка процессов, а также у уволенных сотрудников не должно быть каких-либо прав.

Так как в цифровую среду организации доступ могут получить только сотрудники организации, либо в рамках предусмотренных процессов внештатные исполнители, что должно также отслеживаться иными процессами и контролями, источникам искажения данных являются сотрудники компании и внештатные исполнители либо по ряду событий не предумышленно получившие такие роли, либо с целью манипуляции данными.

Стандартным принципом в данном случае является принцип минимальных привилегий, основа которого в выдаче минимального набора ролей, необходимого для выполнения задачи. На агрегированном уровне, роли в базы данных с соответствующим набором прав для сотрудников возможно унифицировать в целях упрощения процедуры контроля и сопутствующих издержек человеческих ресурсов до следующих: только чтение, чтение и запись, администратор.

Описанное выше решение по предоставлению прав доступа должно иметь процессы, исходя из описанных требований на основании потенциальных рисков по контролям, такие как разграничение возможности выдачи ролей на уровне заявки запроса роли в зависимости от роли сотрудника в компании и его текущих ролей, журналирование, процессы периодической сверки текущих состояний по выданным ролям с компонентами, согласование заявок, отзыв ролей пользователя. Проверка соблюдения таких процессов, как правило, состоит из разового ручного аудита процесса при вводе процесса в эксплуатацию, и периодического ручного аудита текущего состояния выданных прав в СУБД по выборке. Однако риск получения избыточного доступа остается на уровне интеграционного сервиса, либо в результате технических сбоев или некорректной работы текущего процесса выдачи ролей.

Также в отличии от, например, процесса производства, аудит по выборке не является эффективным и гарантирующим, так как периодическое отклонение от ожидаемого процесса по тестированию части совокупности вероятнее всего, если это отклонение имеет не систематических порядок, отследить не получится, помимо того, что на такой аудит приходится достаточно большое количество человеческого ресурса, так как обычно аудиторы не имеют прямого доступа к объектам прав базы данных, получают результаты в виде выгрузок, и вынуждены обрабатывать и анализировать такие выгрузки в ручную, что в свою очередь уже содержит повышенный риск человеческого фактора. Дополнительно к перечисленному нельзя не уточнить, что в растущих организациях количество баз данных растет пропорционально, и достигает десятки или сотни тысяч баз данных, которые хранят чувствительные для организации данные.

В качестве примера рассмотрим подход при автоматизированном мониторинге в рамках контроля рисков предоставления привилегированного доступа не на уровне решения, предоставляющего роли, а на уровне непосредственно СУБД, что позволит нам получить действительную картину состояния, существенно сократить время на проведение проверок, а также сделать систему масштабируемой для любого количества экземпляров баз данных. Своевременное выявление таких рисков позволяет отслеживать промежуток сделанных пользователем изменений для дальнейшего расследования и приведения данных в соответствующее состояние, что позволяет получить достаточный уровень уверенности в качестве хранимых данных.

При разработке мониторинга стоит учитывать, что такой мониторинг возможен только при наличии определенных действующих архитектурных решений. Если на текущий момент в организации отсутствуют такие решения или их аналоги по причинам, не связанным с узкой спецификой деятельности, и сопровождающих ее архитектурных решений – вероятно, такая организация еще не достигла требуемого этапа зрелости процессов.

В модели мониторинга используются следующие инструменты и интеграции между ними:

– сервис поиска текущего адреса хостов по наименованию компонента цифровой системы (основан на получении событий по запускам сервисов из решения виртуализации), или аналог;

– сервис сводной информации по сервисам их компонентам, включающий списки баз данных, где можно определить по метке, проставляющийся на компоненты, находящиеся под контролем риска привилегированного доступа, необходимо ли проверять экземпляр базы данных, или аналог;

– сервис – провайдер авторизации и аутентификации;

– сервис мониторинга.

Алгоритм мониторинга (весь алгоритм выполняется автоматизировано сервисом мониторинга, за исключением корректировки данных):

– необходимо получить текущий список экземпляров баз данных, которые необходимо проверить на привилегированный доступ;

– необходимо получить текущие списки адресов экземпляров баз данных;

– получить из баз данных информацию о текущем состоянии доступов учетных записей;

– получить информацию о состоянии учетных записей из провайдера на предмет отсутствия блокировок и должностей таких сотрудников;

– проанализировать на соблюдение требований, текущее состоянии доступов учетных записей, учитывая роль сотрудников, владеющих учетными записями, и их статусов трудоустройства;

– по идентифицированным привилегированным правам вывести предупреждение об их наличии;

– проанализировать получение предупреждения для корректировки процессов выдачи ролей, и выполнить необходимые действия для корректировки данных;

– запустить алгоритм проверки повторно.

Проведенное исследование реализовано для обоснования автоматизированного подхода к процессу мониторинга.

Результаты исследования и обсуждение

По результатам внедрения реализованы проверки, что позволило привести состояния доступов в экземплярах баз данных к требуемому состоянию в результате выявления раннее не учтенных доступов в предыдущих проверках.

Помимо этого, выявили неточности процесса, которые состояли в определении сотрудников поддержки в компании по процессу выдачи ролей.

Внедрение системы мониторинга оказало положительное влияние.

1. Исключило вероятность искажения данных в результате охвата всех экземпляров, а также исключении человеческого фактора и неточности состояния доступов в выдающей их системе и промежуточных системах.
2. Существенно сократилось время для проведения оценки полноты данных.
3. Появилась возможность более полного описания негативных случаев.
4. Появилась возможность вести количественную аналитику, что позволило повысить эффективность определения изъянов в текущих процессах.

В возможности формализации процесса и унификации сущностей мы можем определить поход к проектированию процесса мониторинга, который позволит масштабировать проверку, условно не увеличивая расход временных или человеческих ресурсов:

– разработать и внедрить необходимые инструменты для мониторинга. Такие инструменты позволят решать не только задачи мониторинга, но и множество иных задач в рамках цифровой среды компании;

– на основании ранее существующего алгоритма ручной проверки разработать алгоритм для автоматизированной проверки в рамах мониторинга;

– на основании разработанного алгоритма реализовать техническое решение, интегрировав с необходимыми инструментами;

– внести изменения в соответствующую документацию при необходимости.

Помимо описанного выше использование системы мониторинга – была выявлена возможность использования статистических данных для построения аналитических прогнозов, что позволило выявлять проблемные участки процессов на основании

сопоставления отклонений с изменениями в штате, архитектуре сервисов и требований к выдаче прав. Это открывает возможность разработки проактивного инструмента прогнозирования, основанного на использовании искусственного интеллекта в интеллектуально-цифровой поддержке предприятия.

Заключение

По результатам исследования подтверждена необходимость проектирования автоматизированной системы мониторинга выявления потенциальных рисков искажения данных. Предложенный подход позволяет повысить качество данных, улучшить достоверность текущего состояния доступов в экземпляры баз данных, снизить нагрузку на человеческие ресурсы за счет повышения управляемости процессов контроля. Полученные результаты подтверждают применимость подхода в условиях масштабируемой и динамически изменяющейся информационной среды предприятия.

Список источников:

1. Попов А.О., Карлова Т.В., Шептунов С.А. Оценка достоверности данных электронной среды предприятия на основе моделей и алгоритмов интеллектуальной поддержки документооборота как ключевой фактор обеспечения эффективного управления предприятием //Автоматизация и моделирование в проектировании и управлении. – 2024. – № 1 (23). – С. 65-72.
2. Баранова О.В. Аудит информационных систем // Вестник финансовой Академии. – 2009. – С. 58-60.
3. Анисимов В.Г., Зегжда П.Д., Супрун. А.Ф. Риск-ориентированный подход к организации контроля в подсистемах обеспечения безопасности информационных систем // Проблемы информационной безопасности. Компьютерные системы. – 2016. – № 3. – С. 61-67.
4. Горбунов В.Л., Файзуллина. А.И. Предиктивный анализ информационных потоков в системах информационной безопасности телекоммуникационных комплексов // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 4. – С. 140-151.

References:

1. Popov A.O., Karlova T.V., Sheptunov S.A. Assessing the Reliability of Data in the Enterprise Electronic Environment Based on Models and Algorithms for Intelligent Document Management Support as a Key Factor for Effective Enterprise Management. Automation and Modelling in Design and Management. 2024;1(23):65-72.
2. Baranova O.V. Auditing Information Systems. Bulletin of the Financial Academy. 2009;1(49):58-60.
3. Anisimov V.G., Zegzhda P.D., Suprun A.F. The Risk-Based Method for Organization of Monitoring in Information Systems Security Facilities. Information Security Problems. Computer Systems. 2016;3:61-67.
4. Gorbunov V.L., Fayzullina A.I. Predictive Analysis of Information Flows in Information Security Systems of Telecommunication Complexes. Information Security Problems. Computer Systems. 2024;(4):140-151.

Информация об авторах:

Попов Антон Олегович
аспирант Института конструкторско-технологической информатики Российской академии наук.

Шептунов Сергей Александрович
доктор технических наук, директор Института конструкторско-технологической информатики Российской академии наук.

Карлова Татьяна Владимировна
доктор социологических наук, кандидат технических наук, ведущий научный сотрудник, профессор Института конструкторско-технологической информатики Российской академии наук.

Information about the authors:

Popov Anton Olegovich
Graduate Student of the Institute for Design-Technological Informatics of the Russian Academy of Sciences.

Sheptunov Sergey Aleksandrovich
Doctor of Technical Sciences, Director of the Institute for Design-Technological Informatics of the Russian Academy of Sciences.

Karlova Tatyana Vladimirovna
Doctor of Sociology, Candidate of Technical Sciences, Professor of the Institute for Design-Technological Informatics of the Russian Academy of Sciences

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.
Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 20.10.2025; одобрена после рецензирования 18.11.2025; принята к публикации 28.11.2025.

The article was submitted 20.10.2025; approved after reviewing 18.11.2025; accepted for publication 28.11.2025.

Рецензент – Пугачев А.А., доктор технических наук, доцент, Брянский государственный технический университет.

Reviewer – Pugachev A.A., Doctor of Technical Sciences, Associate Professor, Bryansk State Technical University.