УДК 004.414.32:004.056

Архитектура и механизмы обеспечения надежности данных в прототипе системы автоматизации стратегического планирования

М.Ю. Бадерякова
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: zavadskaya-lina@list.ru
А.К. Бовт
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
А.С. Ермалицкая
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
В.А. Рычков
Старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва
E-mail: varychkov@mephi.ru

Аннотация: *В статье исследуются архитектура и механизмы обеспечения надежности данных в прототипе системы автоматизации стратегического планирования. Проведен анализ проблем целостности, доступности и конфиденциальности информации. Предложены решения, основанные на принципах избыточности, резервирования, контроля версий и современных криптографических методах. Особое внимание уделено интеграции информационной логистики для оптимизации потоков данных. Описаны ключевые принципы, применяемые при проектировании надежной системы.*

Ключевые слова: *надежность данных, стратегическое планирование, прототип системы, информационная безопасность, целостность данных, доступность данных, конфиденциальность данных, резервирование, контроль версий, информационная логистика, архитектура систем.*

Architecture and data reliability mechanisms in a prototype of a strategic planning automation system

M.Yu. Baderyakova
fourth-year undergraduate student at NRNU MEPhI, Moscow
E-mail: zavadskaya-lina@list.ru
A.K. Bovt
fourth-year undergraduate student at NRNU MEPhI, Moscow
A.S. Ermalitskaya

fourth-year undergraduate student at NRNU MEPhI, Moscow
V.A. Rychkov
Senior Lecturer of Department of Financial Monitoring
NRNU MEPhI, Moscow
E-mail: varychkov@mephi.ru

Abstract: *This article examines the architecture and mechanisms for ensuring data reliability in a prototype strategic planning automation system. Issues related to information integrity, availability, and confidentiality are analyzed. Solutions based on the principles of redundancy, backup, version control, and modern cryptographic methods are proposed. Particular attention is paid to the integration of information logistics to optimize data flows. Key principles applied in designing a reliable system are described.*

Keywords: *data reliability, strategic planning, system prototype, information security, data integrity, data availability, data confidentiality, backup, version control, information logistics, system architecture.*

Введение

Актуальность автоматизации стратегического планирования заключается в том, что в современной экономической среде, где высокая волатильность, глобальная конкуренция и быстро меняющиеся рыночные условия, способность организации к эффективному стратегическому планированию становится ключевым фактором ее выживания и долгосрочного успеха. Традиционные методы планирования уже не способны обеспечить необходимую скорость, точность и комплексность анализа. Сейчас же на смену им приходит эра автоматизированных систем, которые могут обрабатывать колоссальные объемы данных, моделировать различные сценарии развития и оценивать последствия решений.

Автоматизация стратегического планирования может решить ряд критических проблем:

1. Фрагментированность данных:

Информация, которая необходима для планирования, часто распределена по различным департаментам и системам, что создает неполную и противоречивую картину.

2. Низкая скорость принятия решений:

Ручной сбор и консолидация данных занимают недели и месяцы, в течение которых исходная информация устаревает, и организация упускает возможности или не успевает реагировать на угрозы.

3. Человеческий фактор и субъективизм:

Ошибки в расчетах, предвзятость оценок и ограниченность возможностей человека по анализу многокритериальных зависимостей снижают качество и обоснованность стратегических планов.

4. Отсутствие симуляции и прогнозирования:

Без мощных вычислительных инструментов крайне сложно построить и проанализировать множество альтернативных сценариев, оценив их вероятные результаты и риски.

Целью статьи является комплексное описание архитектуры и ключевых механизмов обеспечения надежности и безопасности данных, которые разработаны для прототипа системы автоматизации стратегического планирования. В работе детально рассматривается модульная структура прототипа, обосновывается выбор технологических решений, а также представляется многоуровневая система защиты данных, охватывающая контроль целостности на всех этапах жизненного цикла.

Теоретические основы информационных систем и безопасности данных в стратегическом планировании:

Основные принципы построения ИС:

Информационная система (ИС) для стратегического планирования является разновидностью корпоративных ИС и должна строиться на следующих принципах:

- Интеграция:

Способность объединять данные из разнородных внутренних (ERP, CRM) и внешних источников (рыночная аналитика, макроэкономические показатели), обеспечивая их консолидацию и унификацию.

- Модульность и масштабируемость:

Система должна состоять из функционально независимых, но слабосвязанных модулей (сбор данных, хранение, аналитика, визуализация). Это позволяет развивать и модернизировать каждый компонент независимо, а также наращивать вычислительную мощность по мере роста объемов данных и числа пользователей.

- Безопасность:

Принцип является сквозным и должен быть заложен в архитектуру на начальном этапе проектирования. Он включает в себя не только защиту от внешних атак, но и управление внутренним доступом, обеспечение конфиденциальности и аудит всех операций.

- Достоверность и актуальность данных:

Архитектура ИС должна включать механизмы, которые гарантируют высокое качество исходных данных и их своевременное обновление, так как решения, принятые на основе устаревшей или недостоверной информации, несут в себе высокие риски.

Понятие стратегических данных и их критичность:

Стратегические данные - это качественная и количественная информация, которая формирует основу для определения долгосрочных целей, выбора направлений развития и распределения ключевых ресурсов организации. К ним относятся:

- Внутренние данные: Исторические данные о продажах, финансовой отчетности, себестоимости, производительности.
- Внешние данные: Данные о рыночной доле, действиях конкурентов, макроэкономических трендах, регулирующих нормах, технологических инновациях.

Почему эти данные так важны? Потому что от них зависит будущее всей компании. Если эти данные потеряются, попадут не в те руки или в них внесут ошибки, это может привести к:

- Принятию катастрофических решений, влекущих за собой многомиллионные убытки или потерю конкурентных позиций.
- Утечке коммерческой тайны, что может быть использовано конкурентами.
- Потере доверия со стороны акционеров, партнеров и регуляторов.

Таким образом, вопрос защиты стратегических данных — это вопрос выживания и успеха бизнеса, а не просто пункт в списке задач технических специалистов.

Угрозы для данных в ИС стратегического планирования можно классифицировать по источнику возникновения:

Случайные ошибки и человеческий фактор:

- Некорректный ввод данных: Опечатки, неверные форматы, ввод в не те поля.
- Ошибочные действия персонала: Случайное удаление или изменение критических данных, неправильная настройка моделей анализа.
- Непонимание метрик: Неверная интерпретация данных аналитиками или руководителями.

Технические сбои и отказы оборудования:

- Выход из строя аппаратного обеспечения: Отказ серверов, систем хранения данных или сетевого оборудования.
- Программные сбои: Ошибки в коде приложений, прошивках или операционных системах.
- Потеря данных: Из-за повреждения носителей информации или сбоев в работе систем резервного копирования.

Умышленные действия и несанкционированный доступ:

- Внешние кибератаки: Целенаправленные атаки хакеров с целью хищения данных или их разрушения.
- Внутренние угрозы: Действия недовольных или скомпрометированных сотрудников, злоупотребляющих своими правами доступа для кражи или подмены данных.
- Несанкционированный доступ: Получение доступа к системе лицами, не имеющими на это прав, вследствие слабостей в системе аутентификации или авторизации.

Архитектура и механизмы обеспечения надежности прототипа системы, которые описываются в статье, направлены на комплексное противодействие всем перечисленным категориям угроз, тем самым формируя устойчивый фундамент для достоверного и безопасного стратегического планирования.

Архитектура прототипа системы автоматизации стратегического планирования:

Общее описание прототипа (клиент-сервер, веб-ориентированный и т.д.).

Прототип системы автоматизации стратегического планирования представляет собой веб-ориентированное клиент-серверное приложение. Данный подход был выбран в связи с рядом преимуществ:

- Кроссплатформенная доступность. Пользователи могут получить доступ к системе с любого устройства, имеющего веб-браузер, без необходимости установки дополнительного программного обеспечения. Это особенно важно в современных условиях, когда работа часто ведется удаленно с разных устройств.
- Безопасность. Прямой доступ к базе данных отсутствует - все взаимодействие происходит через строго регламентированный API, что значительно снижает риск атак и несанкционированного доступа к данным.
- Масштабируемость. Серверная часть может быть легко масштабирована горизонтально - добавлением новых серверов для распределения нагрузки, что обеспечивает стабильную работу системы при увеличении числа пользователей и объема данных.

Описание ключевых компонентов

База данных

В качестве системы управления базами данных выбрана PostgreSQL. Этот выбор обусловлен:

- Надежной поддержкой транзакций (ACID-свойства)
- Возможностями репликации для обеспечения отказоустойчивости
- Поддержкой JSONB для работы с полуструктурированными данными
- Высокой производительностью при сложных аналитических запросах

Принципы проектирования базы данных:

- Нормализация до 3-й нормальной формы для минимизации избыточности
- Использование индексов для оптимизации частых запросов
- Реализация ограничений целостности на уровне БД
- Разделение на схемы для логической группировки связанных таблиц

Серверная часть

Серверная часть реализована на Python с использованием Django REST Framework и включает:

- REST API - единую точку входа для всех клиентских запросов
- Модуль аутентификации - управление сессиями и JWT-токенами
- Бизнес-логику - алгоритмы анализа и прогнозирования
- Сервис данных - абстракцию для работы с БД
- Кэширующий слой - Redis для хранения часто используемых данных

API следует принципам Django REST Framework:

- Безопасность - встроенная защита от распространенных уязвимостей
- Производительность - оптимизированная работа с базами данных
- Масштабируемость - модульная архитектура фреймворка
- Админ-панель - готовый интерфейс для управления данными
- Документирование - автоматическая генерация документации

Клиентская часть

Клиентское приложение разработано на React и предоставляет:

- Адаптивный интерфейс - корректное отображение на разных устройствах
- Динамические дашборды - интерактивные панели управления с графиками
- Редактор планов - визуальный конструктор стратегических планов
- Систему уведомлений - оперативное информирование о важных событиях
- Ролевой интерфейс - различное представление для разных категорий пользователей

Взаимодействие компонентов

Взаимодействие между компонентами системы организовано по следующей схеме:

1. Пользователь через веб-браузер обращается к клиентскому приложению
2. Клиентская часть отправляет HTTP-запросы к REST API серверной части
3. Сервер обрабатывает запрос, выполняет бизнес-логику и обращается к БД при необходимости
4. Данные из БД возвращаются на сервер, где преобразуются в формат JSON
5. Сервер отправляет ответ клиенту, который отображает полученные данные

Для реального времени обновлений данных (например, уведомлений о изменениях) используется WebSocket соединение. Все передаваемые

данные шифруются с помощью HTTPS, а для доступа к API требуется аутентификация через JWT-токены.

2. Решения и проектирование надежной архитектуры

Для обеспечения высокой надежности данных в прототипе САСП (система автоматизации стратегического планирования) предлагается интегрированный подход, включающий в себя архитектурные решения, программные механизмы и организационные меры.

2.1. Важные аспекты, влияющие на проектирование

При проектировании решения были учтены следующие аспекты:

- Жизненный цикл данных. От момента создания до архивирования или удаления.
- Типы данных. Различные стратегические показатели, планы, аналитические отчеты, метаданные.
- Пользовательские роли. Разграничение прав доступа для различных категорий пользователей (руководство, аналитики, администраторы).
- Требования к производительности и масштабируемости. Система должна быть способна обрабатывать растущие объемы данных и запросов.
- Бюджетные и временные ограничения. Важно найти баланс между идеальным решением и реалистичными возможностями прототипирования.
- Стандарты безопасности. Применение общепринятых практик и рекомендаций по защите информации.
- Принципы информационной логистики. Оптимизация движения информации в системе.

2.2. Проектирование решения. Архитектура и механизмы

Таблица 1 – Предлагаемая архитектура прототипа САСП с акцентом на надежность данных включает в себя следующие компоненты и механизмы

Раздел	Наименование	Описание
2.2.1. Многоуровневая архитектура с распределенной обработкой	Уровень представления (Presentation Layer)	Пользовательские интерфейсы для взаимодействия с системой.
	Уровень бизнес-логики (Business Logic Layer)	Модули, реализующие алгоритмы стратегического планирования, анализа и принятия решений.
	Уровень данных (Data Layer)	Хранилища данных и механизмы управления ими.
	Распределенная база данных (Distributed Database)	Вместо единого централизованного хранилища, использование распределенной СУБД (например, с применением репликации) для

		повышения доступности и отказоустойчивости.
2.2.2. Механизмы обеспечения целостности данных	Валидация данных	На всех этапах ввода и обработки данных (на уровне представления, бизнес-логики и базы данных) должны применяться строгие правила валидации для отсеивания некорректной информации.
	Транзакции	Использование транзакционного подхода при модификации данных для обеспечения атомарности, согласованности, изолированности и долговечности (ACID-свойства).
	Контроль версий (Versioning)	Реализация системы контроля версий для всех критически важных документов и наборов данных. Это позволяет отслеживать изменения, восстанавливать предыдущие версии и проводить аудит.
	Резервное копирование и восстановление (Backup & Recovery)	Регулярное создание резервных копий данных (полных, инкрементальных, дифференциальных) и разработка четкой стратегии восстановления на случай аварии.
	Журналирование (Logging)	Ведение детальных журналов всех операций с данными (кто, когда, что изменил) для аудита и отладки.
2.2.3. Механизмы обеспечения доступности данных	Избыточность и резервирование (Redundancy & Redundancy)	
	Избыточность серверов	Использование кластерных решений или ферм серверов для распределения нагрузки и обеспечения непрерывной работы при отказе одного из узлов.
	Избыточность хранилищ	Применение RAID-массивов для защиты данных на дисках, а также репликации данных между разными физическими серверами или даже центрами обработки данных.

	Географическое резервирование	Размещение резервных копий или реплик данных в географически удаленных местах для защиты от региональных катастроф.
	Мониторинг и оповещение	Постоянный мониторинг состояния системы, производительности и целостности данных с автоматическим оповещением администраторов о любых аномалиях или сбоях.
	Балансировка нагрузки (Load Balancing)	Распределение входящих запросов между несколькими серверами для предотвращения перегрузок и повышения отзывчивости системы.
2.2.4. Механизмы обеспечения конфиденциальности данных	Аутентификация и авторизация	Строгие механизмы идентификации пользователей и разграничения прав доступа на основе ролевой модели (Role-Based Access Control, RBAC).
	Шифрование данных (Encryption)	
	Шифрование при хранении (Data at Rest Encryption)	Шифрование чувствительных данных в базе данных или файловой системе.
	Шифрование при передаче (Data in Transit Encryption)	Использование защищенных протоколов, таких как HTTPS, VPN, для передачи данных между компонентами системы и пользователями.
	Аудит безопасности	Регулярные проверки безопасности, тестирование на проникновение (penetration testing) и анализ уязвимостей.
	Маскирование данных (Data Masking)	Применение для непроизводственных сред (тестирование, разработка) методов маскирования реальных данных для защиты конфиденциальной информации.
	Управление доступом к сети	Использование фаерволов и сегментации сети для ограничения несанкционированного доступа к внутренним ресурсам САСП.

2.2.5. Информационная логистика в системе стратегического планирования

Информационная логистика играет важную роль в САСП, обеспечивая эффективное управление потоками информации от источников до потребителей. Она фокусируется на оптимизации процессов сбора, хранения, обработки и распределения данных, минимизации задержек и обеспечении качества информации.

Оптимизация сбора данных:

- Автоматизация. Максимальная автоматизация процессов сбора данных из внешних и внутренних источников (ERP, CRM, BI-системы, внешние базы данных, открытые источники).
- Интеграционные шины (ESB). Использование Enterprise Service Bus (ESB) для стандартизации и упрощения интеграции различных источников данных.
- ETL-процессы. Разработка эффективных Extract, Transform, Load (ETL) процессов для извлечения данных, их очистки, преобразования и загрузки в хранилище САСП.
- Управление потоками данных (Data Flow Management).
- Моделирование потоков. Четкое определение и документирование всех информационных потоков в системе, включая источники, преобразования, потребителей и расписания.
- Очереди сообщений (Message Queues). Применение очередей сообщений (например, RabbitMQ, Apache Kafka) для асинхронной передачи данных между модулями, повышения отказоустойчивости и снижения зависимости компонентов.
- Централизованный каталог данных. Создание каталога метаданных, описывающего все доступные данные, их происхождение, форматы, владельцев и правила использования.

Хранение и доступность данных:

- Дедупликация и нормализация. Оптимизация хранения данных для исключения дублирования и обеспечения их согласованности.
- Распределенное кэширование. Использование кэширующих серверов для ускорения доступа к часто запрашиваемым данным.
- Протоколы доступа. Стандартизация протоколов доступа к данным для обеспечения унифицированного взаимодействия.

Распределение информации:

- Каналы распространения. Предоставление различных каналов для доступа к стратегической информации (веб-интерфейсы, API, отчеты, дашборды, электронная почта).
- Персонализация. Возможность персонализации предоставляемой информации в зависимости от роли и потребностей пользователя.

- Подписка на события. Реализация механизмов подписки на изменения в стратегических данных, чтобы заинтересованные стороны оперативно получали уведомления.

2.3. Применяемые принципы и их краткие описания

При разработке решения были применены следующие ключевые принципы:

Таблица 2 – Принципы при разработке решения

Принцип	Описание	Пример
Принцип избыточности (Redundancy Principle)	Заключается в дублировании критически важных компонентов системы (оборудования, программного обеспечения, данных) для обеспечения их непрерывной работы в случае отказа одного из элементов.	использование RAID-массивов для дисков, репликация баз данных.
Принцип резервирования (Backup Principle)	Создание копий данных или состояния системы в определенный момент времени для возможности восстановления после сбоя или потери информации.	регулярное создание полных и инкрементальных резервных копий базы данных.
Принцип эшелонированной защиты (Defense in Depth)	Реализация многоуровневой системы безопасности, где каждый слой обеспечивает защиту, дополняя и усиливая другие. Отказ одного механизма не должен привести к полному пробою защиты.	сочетание фаерволов, систем аутентификации, шифрования и контроля доступа.
Принцип минимальных привилегий (Principle of Least Privilege, POLP)	Предоставление пользователям и процессам только тех минимально необходимых прав доступа, которые требуются для выполнения их функций, и не более того.	аналитику предоставляются права на чтение стратегических данных, но не на их изменение.
Принцип отказа по умолчанию (Fail-Safe Defaults)	Система по умолчанию должна быть в безопасном состоянии. Любое действие, требующее повышенных привилегий, должно быть явно разрешено.	при создании новой учетной записи, по умолчанию ей назначаются минимальные права, которые затем могут быть расширены.

Принцип «нулевого доверия» (Zero Trust Principle)	Ни одно устройство, пользователь или служба не должны быть автоматически доверенными, даже если они находятся внутри периметра сети. Каждый запрос должен быть аутентифицирован и авторизован.	даже внутренние сервисы должны обмениваться данными через защищенные соединения с проверкой подлинности.
Принцип открытости и стандартизации (Openness and Standardization Principle)	Использование открытых стандартов и протоколов для обеспечения совместимости, упрощения интеграции и снижения зависимости от конкретных поставщиков.	использование SQL для баз данных, RESTful API для взаимодействия сервисов.
Принцип модульности (Modularity Principle)	Разделение системы на независимые, слабосвязанные модули, каждый из которых выполняет свою специфическую функцию. Это упрощает разработку, тестирование, масштабирование и обслуживание.	отдельный модуль для сбора данных, отдельный для аналитики, отдельный для визуализации.
Принцип атомарности транзакций (Atomicity Principle)	Гарантия того, что транзакция либо полностью выполняется, либо полностью отменяется, не оставляя систему в промежуточном или несогласованном состоянии.	при обновлении стратегического плана, все связанные изменения в базе данных должны быть либо успешно применены, либо полностью отменены.
Принцип согласованности данных (Consistency Principle)	Гарантия того, что данные всегда остаются в согласованном состоянии после каждой успешной транзакции, соблюдая все определенные правила и ограничения.	если стратегический план требует положительных значений для ключевых показателей, система должна предотвращать ввод отрицательных значений.
Принцип управляемости (Manageability Principle)	Система должна быть спроектирована таким образом, чтобы ее было легко администрировать, мониторить, обновлять и восстанавливать.	наличие удобных инструментов администрирования, четкой документации, автоматизированных скриптов развертывания.

Заключение

Обеспечение надежности данных является важным фактором успешного функционирования любой информационной системы. Предложенная архитектура и комплекс механизмов, основанные на принципах избыточности, резервирования, контроля версий, криптографической защиты и эффективной информационной логистики, позволяют создать прототип САСП, способный выдерживать широкий спектр угроз и сбоев. Внедрение этих решений на ранних стадиях проектирования и разработки значительно снижает риски, связанные с потерей, искажением или несанкционированным доступом к стратегически важной информации, тем самым повышая доверие к системе и способствуя принятию более обоснованных управленческих решений. Дальнейшие исследования могут быть направлены на адаптацию предложенных механизмов к конкретным отраслевым требованиям и на изучение применения технологий машинного обучения для проактивного выявления и предотвращения угроз надежности данных.

Список использованных источников:

1. Кузнецов, М. А. Системы управления базами данных [Текст] / М. А. Кузнецов, М. Р. Когаловский. — Москва: Либроком, 2020. — 448 с. — ISBN 978-5-397-07241-6.

2. Рексфорд, Дж. Корпоративные системы безопасности [Текст] / Дж. Рексфорд; пер. с англ. А. Н. Тимошина. — Москва: Вильямс, 2019. — 512 с. — ISBN 978-5-8459-2055-2.

3. Таненбаум, Э. Распределенные системы. Принципы и парадигмы [Текст] / Э. Таненбаум, М. ван Стеен; пер. с англ. С. Д. Кулешова. — 2-е изд. — Санкт-Петербург: Питер, 2021. — 1184 с. — ISBN 978-5-4461-1497-9.

4. Гамма, Э. Приемы объектно-ориентированного проектирования. Паттерны проектирования [Текст] / Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес; пер. с англ. — Санкт-Петербург: Питер, 2022. — 366 с. — ISBN 978-5-4461-1502-0.

5. Особенности формирования информационно-образовательной среды в условиях цифровой трансформации [Электронный ресурс] // Pedagogical Review. — 2019. — № 3(25). — URL: https://eduherald.ru/article/view?id=21426 (дата обращения: 15.11.2024).