УДК 338.364.4
DOI: 10.37890/jwt.v79.481

Концепция разработки компонентов безопасности на основе развития бизнес-процессов логистики компании

М.В. Фирсов
ORCID: 0009-0001-1377-1598
АО «Теплоэнерго», г. Нижний Новгород, Россия

Аннотация. В условиях продолжающейся цифровой революции, развития порождающего проектирования, машинного обучения, активного применения 3D-маркетинга в рекламе, технологий 3D-печати, новых принципов логистики и систем автоматизированного проектирования кардинально меняются бизнес-процессы предприятия. Возникает необходимость углубления ориентации бизнес-процессов на клиента, на предприятиях требует решения задача обеспечения низкой стоимости как самих бизнес-процессов, так и поддерживающих их компонентов безопасности. Ввиду сложности интеграции информационных систем необходимо заранее создавать концепцию разработки компонентов безопасности на основе развития бизнес-процессов логистики компании.
Очевидно, необходимо не просто учитывать аспекты информационной безопасности (ИБ) при совершенствовании бизнес-процессов, а рассматривать проблему комплексно, то есть разработать как концепцию, так и методику разработки, внедрения бизнес-процессов, их развития, оценки стоимости компонентов ИБ. Необходимо обеспечить гибкость и адаптацию внедряемых бизнес-процессов предприятия.

Ключевые слова: бизнес-процесс, 3D-маркетинг, машинное обучение, информационная безопасность, информационная система, система мониторинга.

The concept of developing security components based on the development of the company's logistics business processes

Michail V. Firsov
ORCID: 0009-0001-1377-1598
JSC Teploenergo, Nizhny Novgorod, Russia.

Abstract. In the context of the ongoing digital revolution, the development of generative design, machine learning, the active use of 3D marketing in advertising, 3D printing technologies, new principles of logistics and computer-aided design systems, the business processes of the enterprise are radically changing. There is a need to deepen the orientation of business processes to the customer, and enterprises need to solve the problem of ensuring low cost of both the business processes themselves and the security components supporting them. Due to the complexity of the integration of information systems, it is necessary to create in advance a concept for the development of security components based on the development of the company's logistics business processes.
Obviously, it is necessary not only to take into account the aspects of information security (IS) when improving business processes, but to consider the problem comprehensively, that is, to develop both a concept and a methodology for developing, implementing business processes, their development, and estimating the cost of IS components. It is necessary to ensure the flexibility and adaptation of the implemented business processes of the enterprise.

***Keywords*:** business process, 3D marketing, machine learning, information security, information system, monitoring system.

Постановка проблемы

Бизнес-процессы на практике конструируют в рамках ERP-систем (Enterprise Resource Planning), которые являются основным средством автоматизации управления предприятием. ERP-системы строятся по модульному принципу. При этом бизнес-процессы предприятия постоянно меняются, совершенствуются, появляются новые современные инструментальные средства разработки ПО. При разработке информационной системы необходимо учитывать ее комплексное развитие с учетом встраивания системы информационной безопасности. При непродуманной наперед автоматизации, без учета реалий развития бизнес-процессов, технического прогресса и современных инструментов разработки ПО предприятие получает автоматизированные устаревшие процессы и неэффективную информационную систему управления, возникают сложности интеграции разных информационных систем и обеспечения безопасности.

Цель статьи – представить концепцию разработки ИТ-компонентов и компонентов безопасности, ориентированных на запросы клиента и современные инструменты разработки ПО, представить методику оценки затрат на разработку ИТ-компонентов. В таких информационных системах возрастает роль современных средств мониторинга программ, 3D-маркетинга, порождающего проектирования, машинного обучения, а инновационные процессы частично перекладываются на клиента за счет применения инструментов «low code».

Методика расчета совокупной стоимости владения

В рамках применения общего экономического подхода можно применить методику расчета совокупной стоимости владения или стоимости жизненного цикла, которая используется для расчета экономического эффекта информационных систем (ИС).

Совокупная стоимость владения (от англ. total cost of ownership, TCO) – общая величина целевых затрат владельца с момента вступления в состояние владения до момента выхода из состояния владения и исполнения владельцем полного объёма обязательств, связанных с владением.

При этом затраты разделяют на капитальные (постоянные) и операционные(косвенные) [1].

Опустим методику формирования косвенных расходов в отечественной и зарубежной практике. В данной статье будем рассматривать ключевые аспекты, определяющие все затраты, в первую очередь это места возникновения и бизнес-процессы.

Отталкиваться будем из постулата, что система информационной безопасности (СИБ) должна соответствовать следующим принципам:

- должна быть прозрачной для администратора системы по ключевым показателям, охватывающим как объекты, так и процессы, события и их динамику вовлеченности в различные процессы;
- затраты на внедрение и поддержку СИБ не должны превышать потенциальные потери от возможных нарушений безопасности;
- пользователь имеет доступ только к тем функциям и данным, которые необходимы для выполнения его задач для снижения рисков несанкционированного доступа и злоупотребления;
- СИБ должна быть удобной и интуитивно понятной для пользователей;
- СИБ должна иметь механизмы для быстрого отключения или обхода в случае чрезвычайных ситуаций и сбоев;
- СИБ обеспечивает безопасность всех компонентов и данных, используемых в процессе обработки информации, включая серверы, сети, базы данных и приложения;

- разработчики СИБ не имеют привилегированного доступа и контроля над системой для исключения конфликта интересов [2, 3].
- Стоимостная составляющая системы защиты охватывает множество аспектов. Выделим в начале основные:
- затраты на оборудование и программное обеспечение: установка и поддержка физической и логической инфраструктуры, таких как серверы, межсетевые экраны, антивирусные программы, криптографические системы, электронно-цифровая подпись;
- затраты на персонал (администрирование и аудит);
- затраты на обучение и осведомленность сотрудников. Помимо IT-специалистов, все сотрудники организации должны быть осведомлены о принципах и практиках информационной безопасности. Бездействие или неосторожное отношение к безопасности может привести к потерям, включая утрату данных, взлом системы или нарушение конфиденциальности. Обучение сотрудников включает проведение семинаров, разработку политик и процедур, а также постоянное напоминание о безопасности информации. Сюда же можно включить затраты на построение моделей психологического поведения сотрудников и методов противодействия нежелательным моделям поведения.
- на предотвращение рисков и потенциальных угроз. Ведение пассивной политики безопасности и недостаточные меры защиты могут привести к потере репутации, судебным искам и другим потери для компании и ее клиентов. При этом расходы на поддержание информационной безопасности не могут превышать возможный ущерб.
- упущенные возможности вследствие эксплуатации устаревшего ПО для обеспечения бизнес-процессов компании и ИБ. Как правило, компания не использует передовые разработки в области маркетинга, облачных технологий, боится передавать любую информацию минуя узкоспециализированный сервер.

Методика разработки и внедрения компонентов ИС и ИБ.

Практические приемы разработки компонентов ИТ и обеспечения безопасности непосредственно связаны с бизнес-процессами предприятия, структурой компонентов ИБ и процессами создания программного обеспечения для функционирования бизнеса (рис.1).

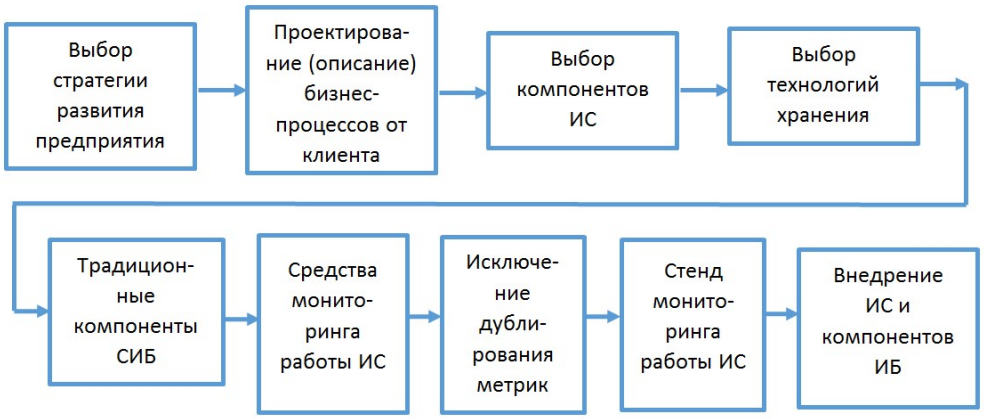

Рис. 1. Методика разработки и внедрения компонентов ИС и ИБ

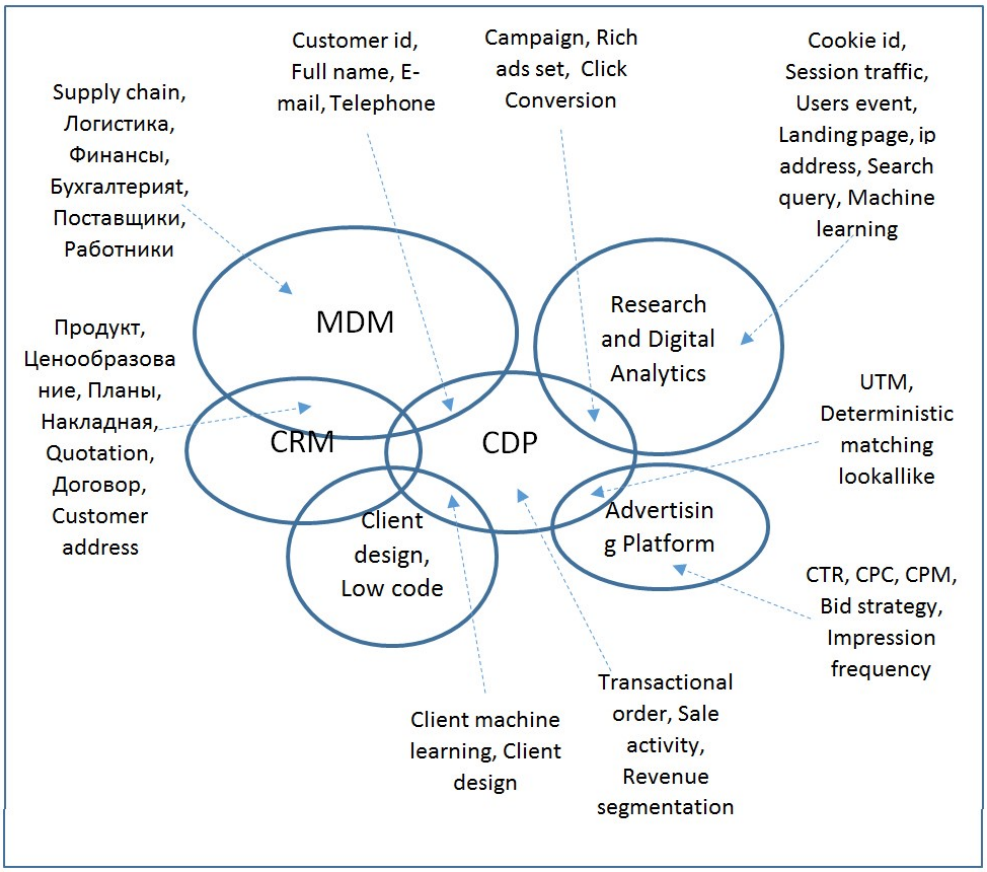

Рис. 2. Взаимосвязь модулей корпоративной ИС на основе схем Gartner

Развитие бизнес-процессов, ориентация их на клиентов приводит к изменениям подходов к разработке ИС [3, 4].

Развитие бизнес-процессов, ориентация их на клиентов, упрощение современных бизнес-процессов путем сокращения (выпадения) больших звеньев в виде физического обслуживания и транспортировки (за счет обработки информации через «облака», развития 3D-маркетинга, применения 3D-принтеров, автоматического конструирования в CAD), бурный рост именно автоматической (порождающего проектирования), а не автоматизированной разработки за счет машинного обучения приводит к изменениям подходов к разработке ИС [3, 4].

На текущем этапе основные перспективные области разработки ИС, выделенные Gartner, представлены на рис. 2.

На схеме видно появление новых названий модулей: CDP и MDM. Можно также выделить модули, связанные с клиентской разработкой требований к продукции и услугам. Например, на сайте компании.

При построении ИС необходимо учитывать:

- технологии хранения данных;
- логику построения бизнес-процессов;
- традиционные компоненты СИБ.

Технологии хранения предполагают:

- традиционные с использованием реляционных баз данных, которые построены на жестких правилах включения данных и соответствия таблиц, как правило без дублирования данных;
- новые большие хранилища сырой информации, работающие на современных технологиях разметки файлов, поиска внутри файла и архивирования. Допускают дублирование. Но его можно исключать для снижения издержек на хранение;
- нереляционные базы данных, в простом варианте в виде словарей для хранения информации в кэше;

Технологии хранения и бизнес-процессы вместе определяют разбивку комплексной ИС на специализированные модули и соответственно состав ИС, методологию проектирования модулей ИС (последовательность и приемы).

Рассмотрим наиболее критичные модули ИС, непосредственно связанные с клиентом.

Система управления мастер-данными MDM (Master Data Management System) используется в целях создания «золотой записи», то есть целостного и всестороннего представления о мастер-сущности и ее взаимосвязях, эталона мастер-данных, который используются всем предприятием, а иногда и между предприятиями для упрощения обмена информацией. Мастер-данные – это базовые данные, которые определяют бизнес-сущности (клиенты, поставщики, продукция, услуги, договора, счета), с которыми имеет дело предприятие.

Например, MDM-системы облегчают работу практически всех служб и отделов предприятия, как клиентских, так и производственных, финансовых.

MDM позволяет:

- повысить качество данных, исправить ошибочные и устаревшие записи, связанные с клиентами, сотрудниками, поставщиками, удалять дубликаты данных;
- упорядочить хранение клиентских данных;
- поднять уровень доверия к данным у руководства и улучшить качество принимаемых решений.
- унифицировать данные вместо применения разрозненных ИС.

Недостатки MDM сказываются на работе маркетологов, специалистов по работе с клиентским опытом, аналитиков и других сотрудников, отвечающих за рост и развитие компании [5].

MDM полагается на высокий уровень достоверности, порядка 90% и предполагает, что данные принадлежат конкретному человеку [5].

MDM-системы имеют дело с «твердыми» данными (транзакционными или справочными) и не включают в себя «мягкие» (например, на основе файлов cookie и IP-адреса) идентификаторы.

MDM обычно работают на реляционных базах данных SQL, что ограничивает маркетологов, поскольку это означает возможность работы только со структурированными данными и недопустимость обработки больших объемов неструктурированных данных.

MDM-системы не позволяют использовать данные для решения маркетинговых задач, например, для сбора информации о всех взаимодействиях, извлечения полезной информации из большого объема неструктурированных данных заказчиков для проведения аналитики.

CDP (Customer Data Platform) - платформа, которая действует как центр управления клиентскими данными внутри компании для повышения эффективности их использования.

CDP создана для обработки клиентских данных либо сырых неструктурированных данных компании по различным бизнес-процессам (сырье, исследования, технологии).

Для вовлечения использования сырых данных внутри компании необходима связь CDP с MDM.

Маркетинг и другие клиентские подразделения являются бизнес-заказчиками именно CDP для своих бизнес-процессов. Поэтому крупные компании обязательно инвестируют в CDP.

CDP позволяют:

- объединить все данные о клиентах в системах и источниках в режиме реального времени и обеспечивают полное, целостное представление о клиентах для команд роста или пользователей специфичных бизнес-процессов. В этом случае не требуется ожидать выгрузок списков для анализа и активации сегментов;
- использовать прогнозные модели и гипотезы для проведения эксперимента с большим набором данных;
- применять персонализированный маркетинг для целевой аудитории. Маркетологам важно доверие и практичность при использовании клиентских данных, уверенно доставлять сообщения на протяжении всего жизненного цикла клиента;
- активировать клиентские данные в любое время в режиме реального времени.
- монетизировать и обмениваться обезличенными данными о клиентах. Данная функция реализуется на биржах информации, где присутствуют собственники таких массивов информации.

Когда MDM-система и CDP-платформа используются вместе обе технологии могут друг друга дополнять.

Совместное использование MDM и CDP позволяет маркетологам объединять профили пользователей и устранять дублирование данных (адресов электронной почты, телефонных номеров, логинов, ников в социальных сетях).

Также с развитием инструментов Low code клиенты получают возможность использовать инструменты дизайна и машинного обучения (рис. 2).

Разработка компонентов СИБ

К традиционным компонентам СИБ также относятся:

- ПО, ограничивающее доступ по сети (межсетевые фильтры), антивирусы;
- общие системы мониторинга инфраструктуры.
- Для мониторинга работы ИС предприятия применяются:
- средства мониторинга бизнес-процессов и процессов работы основных программ, которые предоставляют широкие возможности для обеспечения ИБ и повышения эффективности бизнес-процессов (по времени, затратам, гибкости);
- системы мониторинга отдельных приложений.

К общим системам мониторинга инфраструктуры относится, например, универсальный инструмент Zabbix, который способен отслеживать динамику работы серверов и сетевого оборудования, собирать статистику для оптимизации их работы, реагировать на внештатные ситуации, предупреждать проблемы с нагрузкой Архитектура Zabbix включает четыре основных инструмента, позволяющих мониторить определенную рабочую среду:

- сервер - ядро, хранящее в себе все данные системы, включая статистические, оперативные и конфигурационные. Дистанционно управляет сетевыми сервисами, оповещает администратора о возникающих проблемах с оборудованием, находящимся под наблюдением;

- прокси-сервис, работающий от имени сервера и собирающий данные о доступности и производительности устройств. Данные при этом сохраняются в буфер и загружаются на сервер в отдельную БД (MySQL, PostgreSQL, SQLite или Oracle). Прокси-сервис необходим для снижения нагрузки на сервер, на процессор и на жесткий диск;
- агент - программа (демон), которая активно отслеживает работу локальных ресурсов (накопителей, оперативной памяти, процессора) и приложений и собирает статистику по ним. Отражение текущего состояния физического сервера осуществляются Zabbix-агентом при помощи таких метрик, как загруженность ядра (Processor load), время ожидания ресурсов (CPU io wait time), объем системы подкачки (Total swap space).
- веб-интерфейс, который является частью сервера системы и часто запускается на том же физическом узле, что и Zabbix.

Функционал Zabbix включает в себя общие проверки для наиболее распространенных сервисов - СУБД, SSH, Telnet, VMware, NTP, POP, SMTP, FTP. Если стандартных настроек системы недостаточно, их можно изменить самостоятельно или же пользоваться дополнением через API. Также к стандартным функциям системы относятся: контроль нагрузки на процессор - касается и общих, и отдельных процессов; сбор данных об объеме свободной оперативной и физической памяти; мониторинг активности жесткого диска и мониторинг сетевой активности; пинг для проверки доступности узлов в сети.

У проверок есть заданные шаблоны (Templates), которые упрощают создание новых вычислений. Есть несколько типов шаблонов - стандартизированные шаблоны для сетевых устройств, настройка шаблонов HTTP, настройка шаблонов IPMI, настройка шаблонов ODBC.

Для обработки данных в Zabbix используются триггеры - логические выражения со значениями FALSE, TRUE и UNKNOWN, которые можно создать вручную и протестировать на произвольных значениях перед использованием. У каждого триггера существует уровень серьезности угрозы, который маркируется цветом и передается звуковым оповещением в веб-интерфейсе.

В качестве примера мониторинга конкретного приложения рассмотрим мониторинг приложения Spring Boot с помощью Actuator, Micrometer, Prometheus и Grafana.

Как правило мониторинг с помощью Spring Boot Actuator внедряется в систему из нескольких приложений (микросервисов).

Например, это может быть система, включающая доступ к конечным точкам (http-адреса) по протоколу HTTP или JMX относительно универсального пути ресурса (URI) «/actuator». Например, это могут быть микросервисы:

- резервирования, которые состоят из общедоступных API для управления рабочими процессами резервирования;
- сама служба резервирования (основная база данных и стационарное ПО).

В Spring Boot Actuator можно видеть не только информацию о работоспособности (здоровье) приложения, но и о работоспособности инфраструктуры, например, MongoDB и Rabbitmq, поскольку они настроены автоматически.

Метрики Spring Boot Actuator включают:

- Метрики JVM, использование отчетов:
- Различные пулы памяти и буферов;
- Статистика, связанная со сборкой мусора;
- Использование потоков;
- Количество загруженных (выгруженных) классов;
- Метрики ЦП;

- Метрики файлового дескриптора;
- Метрики Logback: количество событий, зарегистрированных в Logback на каждом уровне журнала;
- Метрики времени безотказной работы: отчет о датчике времени безотказной работы и фиксированном датчике, представляющем абсолютное время запуска приложения;
- Метрики встроенного сервера Tomcat
- Метрики интеграции Spring
- Метрики MVC Spring
- Метрики Spring Webflux
- Метрики RestTemplate.

Spring Boot Actuator позволяет выполнять не только корпоративный мониторинг, но и визуализацию данных, однако ее нужно строить с нуля. Actuator обеспечивает управление зависимостями и автоматическую настройку Micrometer. Микрометр - библиотека поддержки метрик для приложения JVM поддерживает множество инструментов мониторинга, таких как Atlas, Datadog, Graphite, Prometheus и других., позволяет собирать информацию о памяти JVM, сборка мусора, диске.

Также Micrometer предоставляет «независимые от поставщика интерфейсы для таймеров, датчиков, счетчиков, сводок распределения и таймеров длительных задач с многомерной моделью данных, которая в сочетании с системой мониторинга измерений обеспечивает эффективный доступ к конкретной именованной метрике с возможностью детализации по ее измерениям».

Работа с многострочными трассировками стека Java. Многострочные события (трассировки стека) записывается в вывод журнала Spring Boot JSON, Promtail, а также многие другие парсеры, а потом отправляются в Loki.

Loki - система агрегации логов, отвечающая за хранение логов и обработку запросов. Loki спроектирован для простоты реализации в соответствии с принципами:

- простой старт;
- малое потребление ресурсов;
- отсутствие специального обслуживания;
- является дополнением к Prometheus для помощи в расследовании багов(ошибок)

Простота достигается за счет отсутствия индексации контента.

Индексируются только метаданные (labels). Сами данные затем сжимаются и сохраняются фрагментами (chunks) в различных файловых хранилищах (S3, GCS) или в файловой системе.

В результате поиск по тексту не такой эффективный, нет статистики по содержимому текста. Так как Loki является аналогом grep и дополнением к Prometheus, то эти недостатки несущественны, так как за счет сжатия достигается экономия в разы по сравнению с ELK, за использование которого к тому же необходимо платить огромные лицензионные сборы [6, 7].

В результате получаем комплексную систему мониторинга на уровне процессов работы программы, а также внешних физических объектов (для контроля безопасности отдельных объектов и инфраструктуры в целом).

Для удобства интерпретации получаемой от Spring Boot Actuator текстовой информации могут применяться Prometheus и Grafana, чтобы легко делать выводы из генерируемых данных.

Prometheus — это инструмент мониторинга с открытым исходным кодом, разработанный SoundCloud. Grafana — это открытая платформа для визуального мониторинга и аналитики данных временных рядов.

Источник данных Prometheus настраивается, чтобы можно было получать данные из Prometheus для отображения их в пользовательском интерфейсе.

Для мониторинга можно добавить и предварительно настроить свои панели (дашборды) для визуализации работоспособности наших приложений, а именно:

- Микрометр Java Щиток;
- Статистика Spring Boot;
- Производительность Spring.

Таким образом, мы располагаем необходимой инфраструктурой для выполнения корпоративного мониторинга нашего приложения.

Теперь мы будем моделировать нагрузку, состоящую из всех 3 вызовов API -

1. Сохранить бронирование
2. Получить все бронирования
3. Получить конкретное резервирование

Можно моделировать нагрузку с помощью Apache Bench, который обеспечивает более точный контроль с точки зрения тестирования производительности и бенчмаркинга. Таким образом, получается полноценный стенд для испытания работы микросервисов.

Если метрики начинают «сыпаться», срабатывают алерты (сообщения).

SRE-команды (программисты, отвечающие за функционирование сервисов) опираются на «бюджет ошибки» - допустимый период, в течение которого связанные сервисы могут работать ниже целевых уровней. С помощью бюджета можно измерять серьёзность инцидентов. Если, например, инцидент истратил 30% бюджета, его можно считать серьёзным. Это помогает SRE-инженерам не отвлекаться на неважные проблемы, которые регулярно возникают даже в самых оттестированных проектах.

Рис. 3. Методика расчета затрат на внедрение СИБ

В свою очередь, работа системы мониторинга предполагает затраты на формирование и контроль метрик - работу серверов метрик. Затраты зависят от объема и качества метрик в единицу времени, то есть нагрузки на сервер.

Grafana Cloud, например, позволяет получить разбивку по использованию ежемесячных метрик и связанных с этим затрат.

Часто клиенты планируют свои расходы на наблюдение в зависимости от общих расходов на ИТ (< 10%) в качестве базового показателя.

Можно отслеживать количество временных рядов с определенной меткой или набором меток, примененных с течением времени, чтобы понять, какой вклад вносят различные команды, среды или приложения в общее количество рядов. Получая эти данные в виде временных рядов, можно определить на панели мониторинга Grafana, как изменение метрик в определенный момент времени приводит к изменению бюджета по основным расходам. Методика расчета затрат приведена на рис.3.

Таким образом можно выявлять и неиспользуемые метрики с целью определенной работы с ними для уменьшения затрат. Опыт показывает, что можно сократить объем временных рядов на 20–50 %. Машинное обучение позволяет строить постоянно совершенствующиеся модели реагирования приложений, в том числе на основе набора алгоритмов машинного обучения[8]. Описанная схема построения ИТ-компонентов и компонентов СИБ представлена на рис.4 на примере системы резервирования заказов. Контроль бизнес-процессов компании осуществляется за счет использования брокера сообщений, парсеров, логов информации и ее анализа с помощью машинного обучения.

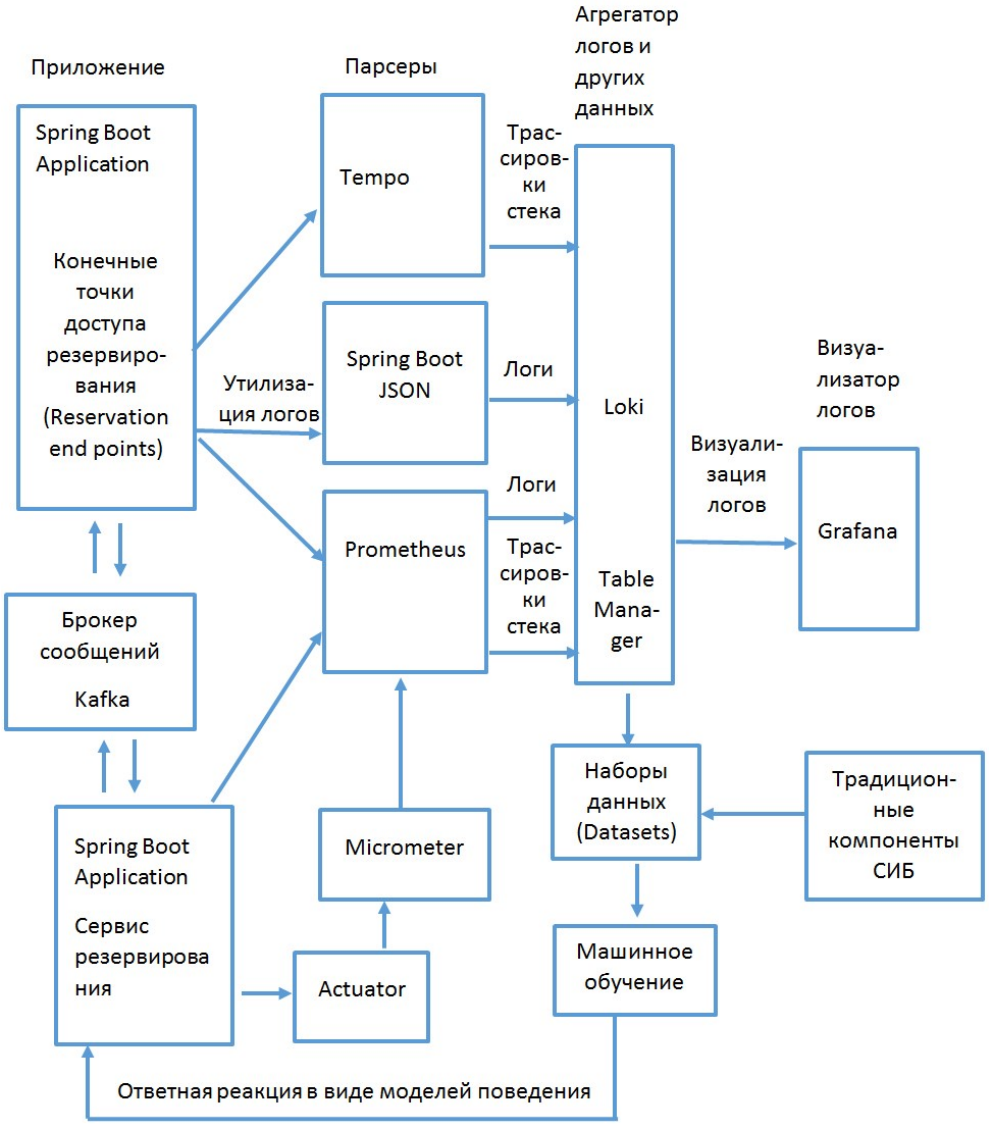

Рис. 4. Комплексная система мониторинга на основе Loki-Grafana в системе резервирования заказов

Заключение

Бизнес-процессы на практике конструируют в рамках IT-систем, которые являются основным средством автоматизации управления предприятием. IT-системы строятся по модульному принципу. При этом бизнес-процессы предприятия постоянно меняются, совершенствуются, появляются новые современные инструментальные средства разработки ПО. При разработке бизнес-процессов и реализующей их информационной системы необходимо учитывать комплексное развитие с учетом встраивания компонентов системы информационной безопасности.

Предложенная концепция разработки компонентов СИБ позволяет учесть основные запросы клиентов с точки зрения управления стоимостью компонентов ИБ и гибкости бизнес-процессов. Это обеспечивается во многом разработанной методикой создания и внедрения компонентов ИС и ИБ. За основу был взят

стратегический подход к развитию бизнес-процессов с учетом всех основных элементов менеджмента бизнес-процессов (цепочка поставок, маркетинг, реклама).

Уменьшение затрат на компоненты системы безопасности в разы становится возможным как за счет правильного проектирования бизнес-процессов, так и ориентации на сжатие данных, использование современных файловых хранили, open source компонентов и машинного обучения. Машинное обучение позволяет обеспечить дополнительную гибкость для осуществления постоянного во времени совершенствования бизнес-процессов предприятия.

Список литературы:

1. DDudko. Подходы к расчету совокупной стоимости владения и эксплуатации комплексных систем безопасности. Блог компании ГК ЛАНИТ. - 20 июл 2021. - https://habr.com/ru/companies/lanit/articles/566598/ (дата обращения 18.01.2024).
2. Кислова Д.А., Аветисян Т.В. Стоимостные аспекты информационной безопасности. XVI Международная студенческая научная конференция «Студенческий научный форум – 2024». - https://scienceforum.ru/2024/ (дата обращения 18.01.2024).
3. Фирсов М.В. Концепция создания ERP-систем / М.В. Фирсов. - М.: ТЕИС, 2004. – 93 с.
4. Фирсов М.В. Роль 3D-маркетинга в конструировании бизнес-процессов./ М.В. Фирсов // Маркетинговые коммуникации. - 2016.- №3.- С.164–172.
5. Cleverdata_team. MDM и CDP: различия систем. Как сделать выбор. - 12 дек 2023. - https://habr.com/ru/companies/lanit/articles/776862/ (дата обращения 18.01.2024).
6. Grafana Loki - Как хранятся данные. - APRIL 11, 2023. - https://tipoit.kz/how-loki-stores-data (дата обращения 18.01.2024).
7. MaxRokatansky. Loki — сбор логов, используя подход Prometheus. - 5 фев 2020. - https://habr.com/ru/companies/otus/articles/487118/ (дата обращения 18.01.2024).
8. Л. Ф. Тагирова, Н. Г. Семенова Проектирование адаптивных пользовательских интерфейсов интеллектуальных обучающих систем на основе нейросетевых технологий/ Н. Г. Семенова //Информационные технологии. – 2023. - №9. - С. 473–484.

References:

1. DDudko. Podhodi k raschetu sovokupnoi stoimosti vladenija i ekspluatacii kompleksnih system bezopasnosti. Blog kompanii GK Lanit [pproaches to calculating the total cost of ownership and operation of integrated security systems. Blog of the LANIT Group of Companies]. Available at: < https://habr.com/ru/companies/lanit/articles/566598> (accessed 18.01.2024).
2. Kislova D.A., Avetisan T.V. Stoimostnii aspekti informatsionnoi bezopasnosti [Cost aspects of information security]. XVI International Student Scientific Conference “Studencheskij nauchnii forum” [Student Scientific Forum – 2024]. Available at: < https://scienceforum.ru/2024> (accessed 18.01.2024).
3. Firsov M.V. Kontseptsiya sozdaniya ERP-sistem [The concept of creation of ERP-systems]. Moscow, TEIS, 2004, 98 p.
4. Firsov M.V. Rolj 3D-marketinga v konstruirovanii biznes-processov [The role of 3D marketing in business process design]. Journal of Marketing communications. 2016, no 3, pp. 164–172. (In Russ).
5. Cleverdata_team. MDM и CDP: raslichia system. Kak sdelatj vibor [MDM and CDP: system differences. How to make a choice]. Available at: < https://habr.com/ru/companies/lanit/articles/776862> (accessed 18.01.2024).
6. Grafana Loki - kak hranjatsja dannii [Grafana Loki - How data is stored]. Available at: < https://tipoit.kz/how-loki-stores-data> (accessed 18.01.2024).
7. MaxRokatansky. Loki – sbor logov, ispolzuja podhod Prometheus [Loki - collecting logs using the Prometheus approach]. Available at: <https://habr.com/ru/companies/otus/articles/487118> (accessed 18.01.2024).

8. L. F. Tagirova, N.G. Semenova. Proektirovanije adaptivnih poljzovateljskih interfeisov intellektualjnih obuchajushih system na osnove neirosetevih technologii [Designing adaptive user interfaces for intelligent learning systems based on neural network technologies]. Journal of Information technology. 2023, no 9, pp. 473–484. (In Russ).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Фирсов Михаил Владимирович, профессор, д.э.н., ведущий инженер-программист АО «Теплоэнерго», 603086, г. Нижний Новгород, б-р Мира, д. 14

Michail V. Firsov, Ph.D. in Economic Science, Professor, Doctor of Economics, Leading Software Engineer of JSC Teploenergo, 603086, Nizhny Novgorod, Mira Boulevard, 14

Статья поступила в редакцию 15.02.2024; опубликована онлайн 20.06.2024.
Received 15.02.2024; published online 20.06.2024.