Принципы построения гарантоспособных биллинговых информационных систем в жилищно-коммунальном хозяйстве

С. Е. Голиков

***Аннотация*— Качество предоставляемых жилищно-коммунальных услуг напрямую влияет на потребность людей в комфортных условиях проживания, а также позволяет создать среду для реализации принципов социально-ориентированной экономики. Биллинг или система расчетов за предоставленные услуги является основой функционирования жилищно-коммунального хозяйства (далее — ЖКХ). Важнейшей составляющей использования подобных систем является уровень надежности и безопасности сервисов и компонентов, реализуемых с использованием средств вычислительной техники. Недостаточный уровень надежности и безопасности информационных систем приводит к материальным потерям, снижению конкурентоспособности, сужению рынков сбыта, а также к более серьезным последствиям, связанных с гибелью людей, техногенными катастрофами и т.д. Арсенал методов теории надежности и средств оценки применительно к сервис-ориентированным структурам и программным средствам недостаточно эффективен. Это связано с тем, что методы классической теории надежности не могут адекватно описать объекты, работоспособность которых может быть нарушена не только отказами физической природы, но и стать следствием программных ошибок, информационных воздействий и т.п. Для проектирования биллинговых информационных систем автор предлагает использовать разработанный им механизм динамически настраиваемой инфраструктуры, позволяющий предоставлять требуемые услуги, которым можно оправданно доверять. Повышение гарантоспособности критических узлов информационной инфраструктуры обеспечивает требуемый уровень эластичности к отказам, сводит время восстановления к минимуму и обеспечивает непрерывность бизнес-процессов.**

***Ключевые слова*— гарантоспособные сервисы, адаптивная инфраструктура, биллинговые информационные системы.**

Статья получена 13 января 2021.

С. Е. Голиков — ФГАОУ ВО «Севастопольский государственный университет (e-mail: kcl@mail.ru).

I. Введение

Жилищно-коммунальное хозяйство Российской Федерации (далее – ЖКХ) является одной из базовых отраслей народного хозяйства, которая обеспечивает население жизненно необходимыми услугами. Реформы, проводимые в ЖКХ на протяжении последних лет, оказали положительное влияние на динамику развития отрасли. Государством были определены приоритетные принципы государственной политики: использование энергоэффективных технологий[1], создание государственной корпорации, осуществляющей поддержку муниципалитетов («Фонд содействия реформированию ЖКХ»)[2][3].

Биллинг в ЖКХ является основополагающим принципом функционирования. Биллинговая система в широком понимании должна не только начислять платежи, но и способствовать сбору платежей с населения любыми удобными для него способами, включая онлайн-платежи, прозрачное и правильное распределение их между получателями. Биллинговая система должна иметь интерфейс обмена с ГИС «ЖКХ», информационными системами органов соцзащиты, ресурсоснабжающих организаций, выступая единым центром сбора и обработки информации.

II. Постановка задачи

Действенным способом решения существующих проблем является создание муниципального информационно-расчетного центра на основе участия ресурсоснабжающих организаций, управляющих компаний, администрации с использованием единой квитанции. Присутствие администрации является необходимым фактором стабильности, так как именно глава администрации является лицом, ответственным за обеспечение жилищно-коммунальных услуг [4].

Единый информационно-расчетный центр (далее - ЕИРЦ) занимается начислением за жилищно-коммунальные услуги, приемом, расщеплением и транзитом платежей в управляющие и ресурсоснабжающие организации, доставкой квитанций. Прозрачность деятельности ЕИРЦ обеспечивает отсутствие злоупотреблений в виде временного привлечения средств, перераспределении денежных средств одним участникам расчетов в ущерб другим, минимальные трансакционные потери, контроль со стороны администрации. Исходя из вышесказанного, становится очевидным, что актуальным направлением становится разработка и внедрение механизмов

снижения операционного риска информационно-расчетного центра, в особенности его технологической составляющей. Технологическая составляющая операционного риска находится в корреляции с уровнем надежности и безопасности сервисов и компонентов, реализуемых с использованием средств вычислительной техники. Данное положение обусловлено тем, что недостаточный уровень надежности и безопасности информационных систем приводит к материальным потерям, снижению конкурентоспособности, сужению рынков сбыта, а также к более серьезным последствиям, связанных с гибелью людей, техногенными катастрофами и т.д. Теория надежности хорошо развилась применительно к техническим системам. Однако, арсенал ее методов и средств оценки применительно к сервис - ориентированным структурам, программным средствам недостаточно эффективен. Методы классической теории надежности не могут адекватно описать объекты, работоспособность которых может быть нарушена не только отказами физической природы, но и стать следствием программных ошибок, информационных воздействий и т.п.

III. Основная часть

Особенностью операционного риска является то обстоятельство, что низкая вероятность наступления рискового события влечет разрушительный характер последствий с финансовой точки зрения. Высокий уровень автоматизации расчетов в ЖКХ ведет к повышению значимости операционной составляющей наступления рискового события [5].

Операционные риски включают в себя человеческие риски (ошибки, воровство, болезни), технологические риски (сбои в работе, аварии, отказы техники, ошибки программного обеспечения), внешние риски (катастрофы, стихийные бедствия и т.п.). Источник операционных рисков, как правило, расположен внутри автоматизированной системы. Устранение порождающих его причин приведет к снижению вероятности возникновения операционного риска. В следствие того, что реализация услуг информационно-расчетных центров ЖКХ осуществляется в рамках специализированной автоматизированной системы, будем рассматривать операционный риск исключительно в рамках данной системы.

Наиболее значимой составляющей операционного риска в рамках автоматизированной системы можно считать информационно-техническую. Технологический риск возникает, если имеет место быть несоответствие используемых информационных технологий и процессов обработки информации, в том числе вследствие неадекватности политики и стратегии использования информационных ресурсов и технологий. Определим ключевые элементы противодействия возникновению рисковых событий в биллинговых системах ЖКХ:

1) наличие хорошо описанных бизнес-процессов и системы мониторинга. Должны быть выделены критически важные участки, процессы следует ранжировать по уровню критичности. Задачи по поддержанию работоспособности должны быть направлены на возобновление наиболее значимых функций в течение одного расчетного дня.

2) проработанные планы мероприятий по поддержанию работоспособности, предусматривающие возникновение наиболее вероятных сценариев, в том числе, техногенные катастрофы, террористические акты, прекращение подачи электричества. Автоматизированная система должна иметь достаточный уровень резервирования для того, чтобы успешно решать задачи по восстановлению работоспособности.

3) наличие антикризисных групп, процедур управления риском, хорошо налаженная горизонтальная и вертикальная коммуникации.

4) проведение регулярных тестов по каждому аспекту плана мероприятий. Планы на случай чрезвычайных происшествий должны регулярно тестироваться, пересматриваться, анализироваться на приемлемость и действенность.

В рамках данной статьи рассмотрим технологический операционный риск, устойчивость к сбоям архитектурного решения информационной системы. Под устойчивостью к сбоям понимается создание такого архитектурного решения, при котором обеспечиваются оптимальные производительность, надежность, безопасность и доступность при соответствии операционным и техническим требованиям к системе [6].

Биллинговая система должна, с одной стороны обладать свойствами классической надежности (в первую очередь, отказоустойчивостью), а с другой обеспечивать безопасность, прежде всего информационную. В связи с вышесказанным, с целью устранения дуализма понятий «отказоустойчивость-информационная безопасность» целесообразно по отношению к подобным системам использовать термин «гарантоспособность»[7].Гарантоспособность-способно сть информационной системы предоставлять требуемые услуги, которым можно оправданно доверять. Отказоустойчивость не рассматривается как свойство гарантоспособности, а определяется как механизм, который поддерживает другие свойства гарантоспособности, являясь стержнем, от которого зависят все составляющие [8].

Архитектура программного обеспечения биллинговых систем для обслуживания ЖКХ представляет собой взаимосвязанный комплекс компонентов, выполняющих определенную функцию или набор функций. Разные производители используют различные архитектурные стили. Наиболее часто используется клиент-серверная (N-уровневая) с элементами компонентной и многоуровневой. Данная архитектура позволяет разместить инфраструктурные элементы системы на различные физические устройства, что повышает гарантоспособность системы, не исключая возможность централизованного управления и доступа к данным. Компонентная архитектура упрощает функциональное наращивание путем повторного использования логических компонентов. Многослойность представления логики повышает функциональную безопасность системы. Наибольшее развитие получила трехуровневая архитектура, позволяющая разместить программные компоненты на

разных физических узлах. Преимуществами данного подхода являются [9]:

– прозрачная маршрутизация пары запрос-ответ;
– понижение сложности информационной системы;
– возможность использования балансировки загрузки вычислительных мощностей узлов;
– простота настройки и конфигурирования;
– горизонтальная масштабируемость.

Гарантоспособная информационная система – система, обладающая полным или частичным набором свойств, составляющих гарантоспособность. Причем в свойства должны входить как традиционные свойства теории надежности (готовность, безотказность), так и свойства информационной безопасности (конфиденциальность, целостность, доступность).

Для связи между элементами используются сообщения. Преимуществами данной архитектуры являются возможность функциональной декомпозиции программно-аппаратной среды, распределенное развертывание, обеспечивающие повышенную доступность, управляемость, эффективность использования ресурсов. Каждый уровень взаимодействует только с заранее определенным уровнем, остальные находятся в изоляции. Повышению конфиденциальности и безопасности способствует размещение бизнес-логики на сервере приложения, слой представления – на клиентских рабочих местах, а слой данных – в базе данных. Размещение бизнес-логики на отдельном устройстве гарантирует доступность обновлений для всех пользователей системы, изменения в настройках производятся в одном месте, ответственность за авторизацию пользователей переносится с потенциально небезопасного клиентского уровня на уровень сервера приложений, скрывая уровень размещения данных. Существует достаточно много промышленных серверов приложений. Основными недостатками подобных серверов являются высокая стоимость, сложность управления и достаточно низкое быстродействие. Слабым звеном централизованной обработки является отказоустойчивость сервера приложений, так как в случае выхода его из строя клиенты не смогут получить доступ к приложению. Одним из способов повышения гарантоспособности является использование различных методов резервирования, предусматривающих перераспределение запросов на исправные компоненты платформы. Использование резервирования позволяет достигнуть практически безграничное повышение надежности и безопасности инфраструктуры. Целесообразным является использовать резервирование с замещением, при котором резервный сервер включается в работу автоматически при перенаправлении на него запросов от клиентских приложений. При выходе из строя основного сервера приложений клиентское приложение автоматически подключается к одному из резервных серверов приложений, обеспечивая доступность данных. Даже в случае отсутствия доступного сервера приложений система останется работоспособной. Инфраструктура системы перестроится в 2.5 уровневую архитектуру, а обработка бизнес-логики и доступ к данным будет осуществляться при помощи стандартных средств применяемой системы управления базами данных (далее – СУБД).

В качестве механизмов автоматического дублирования сервера приложений используются:

– автоматическое переключение потоков данных на резервный сервер в случае отказа основного;
– автоматическое определение статуса сервера "основной" или "резервный" при старте системы и автоматическое разрешение конфликтов статуса при восстановлении основного сервера после сбоя;
– ведение протокола сбоев и переключений.

Предлагаемая топология биллинговой информационной системы представлена на рисунке 1.

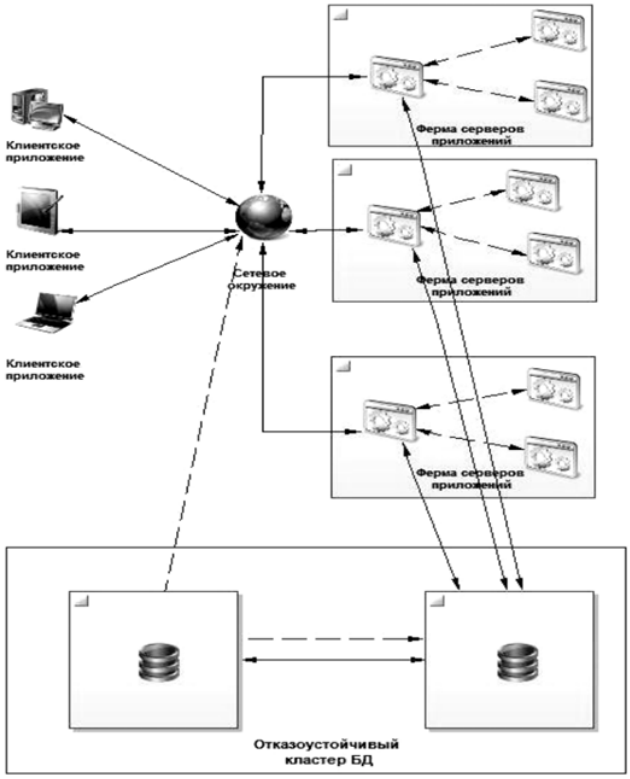

Рис. 1 - Топология гарантоспособной биллинговой системы

Сеть делится на несколько сегментов, в каждом из которых размещается ферма серверов приложений. Таким образом, устраняется единственная точка отказа – сервер приложений. В случае отказа одного из серверов приложений состояние и данные будут восстановлены на резервном сервере. В случае выхода из строя всех серверов приложение будет работать напрямую с базой данной. База данных также вынесена за пределы границ фермы серверов приложений.

Структура сервера приложений (клиентская и серверная часть) изображена на рисунке 2.

Используется асинхронный обмен сообщениями, что позволяет повысить эффективность взаимодействия в случае возникновения задержек и обрывов.

Вследствие того, что очереди являются общими ресурсами двух потоков, обращения к ним размещаются в критических секциях. Для синхронизации потоков используется алгоритм Питерсона.

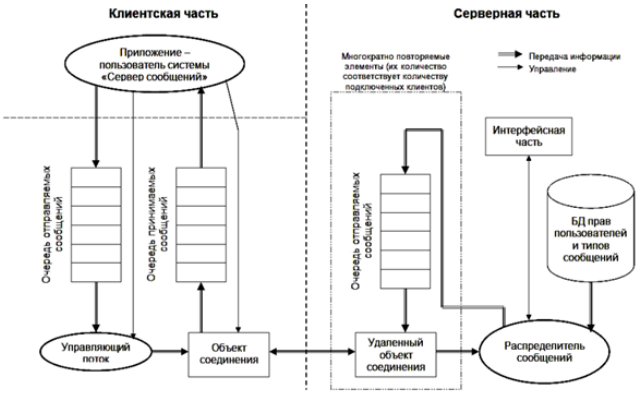

Рис. 2 - Структура сервера приложений

Объект соединения клиентской части платформы обеспечивает первичную обработку пересылаемой и поступающей информации (выделяет из общего потока системные сообщения), управляет очередями сообщений. Управляющий поток обеспечивает интерфейс работы с удаленным сервером. При наличии сообщения, которое необходимо отправить, объект - управляющий поток помещает его в очередь отправляемых сообщений и отсылает через объект соединения. Следующее сообщение посылается только после получения уведомления о готовности объекта соединения к передаче следующего сообщения.

Распределитель сообщений серверной части платформы предназначен для передачи сообщений от одного удаленного объекта другим, проверки прав подключаемых пользователей, создания новых удаленных объектов соединения. Распределитель сообщений также взаимодействует с объектами базы данных для проверки прав подключившихся пользователей. С целью исключения отказов все отправляемые сообщения сначала помещаются в очередь сообщений, а затем обслуживаются. Функцией распределителя сообщений является также наблюдение за удалением объектов отсоединившихся клиентов.

Удаленный объект соединения работает по принципу конечного автомата. Он имеет четыре основных состояния: инициализация, аутентификация клиентского соединения, прием общений, деинициализация. Через методы распределителя сообщений данный объект обеспечивает авторизацию клиентов, управляет каналом связи.

Запросы обслуживаются по методу FIFO.Связь между клиентом и сервером устанавливается через механизм аутентификации/авторизации. Логин и пароль через объект соединения передается на сервер, где происходит его верификация. После успешной аутентификации происходит определение доступа к операциям на основании принадлежности вызывающей стороны к той или иной роли. Связь между сервером приложений и базой данных обеспечивается отдельным соединением.

Таким образом, аутентификация клиента происходит через посредника - сервер приложений, сервер приложений использует собственные учетные данные для доступа к ресурсам, а не учетные данные клиента.

Учетные данные клиента используются для определения его принадлежности к той или иной роли.

В случае обрыва соединения клиент пытается снова установить соединение с текущим сервером приложения, по истечении времени таймаута - резервным, имеющим наибольший приоритет. При этом все сообщения, стоящие в очереди, сохраняются и передаются после подключения к новому серверу. В случае невозможности подключиться к серверу приложений, система адаптирует запросы для непосредственной работы с базой данных.

Коммуникации между клиентом и сервером защищаются с помощью протокола TLS. TLS использует цифровые сертификаты и криптографию с открытым ключом. Он обеспечивает шифрование данных, передаваемых по сети между клиентом и сервером приложений, а также между сервером приложением и базой данных, выявление возможных манипуляций, направленных на преодоление защиты или вмешательство в обмен, а также аутентификацию на основе сертификатов. Клиент запрашивает сервисы путем инициирования запросов к серверу. Запрос определяет действия, происходящие в конкретный момент времени. Форма запроса определяется протоколом обмена. Выполнение запроса вызывает выполнение соответствующего действия на сервере. После завершения запроса клиенту возвращается результат запроса.

IV. Заключение

Предложенный механизм динамически настраиваемой инфраструктуры биллинговой информационной системы существенно повышает гарантоспособность критических узлов информационной инфраструктуры, сводя к минимуму время восстановления, что позволяет сделать систему эластичной к отказам и обеспечить непрерывность автоматизированных бизнес-процессов. Данное решение может быть использовано для минимизации влияния функциональной составляющей операционного риска, например, в системе мониторинга наиболее значимых показателей работы предприятия. При разработке технологии проектирования гарантоспособных биллинговых систем имеет смысл опираться на модель жизненного цикла гарантоспособности, объединяющей моделирование процессов и решений по ее обеспечению и проверке.

В дальнейшем планируется разработать программный интерфейс и протокол обмена сервера сообщений с внешними системами и приложениями с целью стандартизации и унификации процедуры взаимодействия.

Библиография

[1] Указ Президента Российской Федерации от 7 мая 2012 г. № 600 «О мерах по обеспечению граждан Российской Федерации доступным и комфортным жильем и повышению качества жилищно-коммунальных услуг». Доступно по адресу: http://www.kremlin.ru/acts/bank/35264

[2] Федеральный закон от 21.07.2007 № 185-ФЗ «О фонде содействия реформированию жилищно-коммунального хозяйства». Доступно по адресу: http://docs.cntd.ru/document/902052609

[3] Концепция федеральной целевой прграммы «Реформирование и модернизация жилищно-коммунального хозяйства на период 2010-2020 годов. Доступно по адресу: http:// www.fondgkh-nso.ru

[4] Федеральный закон от 06.10.2003 N 131-ФЗ (ред. от 09.11.2020) "Об общих принципах организации местного самоуправления в Российской Федерации". Доступно по адресу:http://docs.cntd.ru/document/901876063
[5] С.В. Криворучко. Операционные риски платежных систем: уровни ответственности. Доступно по адресу:https://www.klerk.ru/bank/articles/77213/
[6] Fowler M. Patterns of Enterprise Application Architecture / M. Fowler. – Addison-Wesley Professional, 2003. –533 p.
[7] Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Depenable and Secure Computing//IEEE Trans. On Depenable and Secure Computing.-2004;1(1)-p.11-33.
[8] Kharchenko V., Popov V., Romanovsky A. On Dependability of Composite Web Services with Components Upgraded Online// Proc. Of Workshop an Architecting Dependable Systems (DSN 2004), Italy, 2004.-p.14-20
[9] Bernshtein Philip A. Middleware – A model for Distributed System Services / Philip A. Bernshtein // Communications of the ACM. – DOI:10.1145/230798.230809

Principles of building dependable billing information systems in housing and communal services

S.E. Golikov

***Abstract*— Housing and communal services (hereinafter - housing and communal services) is one of the most important areas of the socio-economic structure of society. The quality of the provided housing and communal services directly affects people's need for comfortable living conditions, and also allows creating an environment for the implementation of the principles of a socially oriented economy. Billing or a system of payments for services provided is the basis for the functioning of housing and communal services. In the modern world, calculations are impossible without the use of specialized information systems. The most important component of using such systems is the level of reliability and security of services and components implemented using computer technology. This situation is due to the fact that an insufficient level of reliability and security of information systems leads to material losses, a decrease in competitiveness, a narrowing of sales markets, as well as to more serious consequences associated with the death of people, man-made disasters, etc. Reliability theory has developed well in relation to technical systems. However, the arsenal of its methods and assessment tools as applied to service-oriented structures and software is not effective enough. This is due to the fact that the methods of the classical theory of reliability cannot adequately describe objects, the performance of which can be impaired not only by failures of a physical nature, but also be the result of software errors, information influences, etc. The author has applied a risk-based approach to the definition of fault tolerance and uses the term "dependability" (reliability in a broad sense). For the design of billing information systems, the author proposes to use the mechanism of a dynamically configurable infrastructure developed by him, which makes it possible to provide the required services that can be reasonably trusted. Improving the availability of critical nodes of the information infrastructure provides the required level of elasticity to failures, minimizes recovery time and ensures business continuity.**

Keywords: **dependable services, adaptive infrastructure, billing information.**

REFERENCES

[1] Ukaz Prezidenta Rossijskoj Federacii ot 7 maya 2012 g. № 600 «O merach po obespecheniju grazhdan Rossijskoj Federacii dustupnym I komfortnym zhiljem I povysheniju kachestva zhilischno – kommunalnych uslug ». Dostupno po adresu http://www.kremlin.ru/acts/bank/35264

[2] Federalnyi Zakonot 21.07.2007 № 185-FZ «O fonde sodejstvija reformirovaniju zhilischno-kommunalnogo chozajstva».Dostupno po adresu: http://docs.cntd.ru/document/902052609

[3] Konzepcija federalnoi celevoj programmy «Reformirovanije I modernizacija zhilischno-kommunalnogo chozajstva na period2010–2020 godov». Dostupno po adresu:www.fondgkh-nso.ru

[4] Federalnyi Zakon ot 06.10.2003 N 131-FZ (red. ot 09.11.2020) "Ob obschich principach organizaci I mestnogo samoupravlenija v Rossijskoj Federacii". Dostupno po adresu:http://www.consultant.ru/document/cons_doc_LAW_44571/

[5] KrivoruchkoS.V.Operacionnye riski platezhnychs ystem: urovnio tvetstvennosti. Dostupno po adresu: https://www.klerk.ru/bank/articles/77213/

[6] *6.* Fowler M. Patterns of Enterprise Application Architecture / M. Fowler. – Addison-Wesley Professional, 2003. –533 p.

[7] Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Depenable and Secure Computing//IEEE Trans. On Depenable and Secure Computing.-2004;1(1)-p.11-33.

[8] Kharchenko V., Popov V., Romanovsky A. On Dependability of Composite Web Services with Components Upgraded Online// Proc. Of Workshop an Architecting Dependable Systems (DSN 2004), Italy, 2004.-p.14-20

[9] Bernshtein Philip A. Middleware – A model for Distributed System Services / Philip A. Bernshtein // Communications of the ACM. – DOI:10.1145/230798.230809