И.Г. ХАЛИУЛЛИН, М.И. ЧУЧИН

Военный университет
Министерства обороны
Российской Федерации,
г.Москва

Особенности архитектуры облачных автоматизированных информационных систем

УДК 004.8

Аннотация. В статье представлены выводы из анализа особенностей архитектуры облачных автоматизированных информационных систем, проведенного с акцентом на защиту информации, хранимой и обрабатываемой в таких системах. Описаны новые возможности облачных технологий, используя которые потребитель получает дополнительные возможности контроля за доступом к информации и администрирования этого доступа.

Ключевые слова: информационная система, облачные вычисления, автоматизированная система, безопасность информации, геолокация, сетевые технологии

Наука и технологии представляют ядро национальной безопасности, промышленной конкурентоспособности, экономного потребления энергетических ресурсов, сохранения окружающей среды, лидерства в фундаментальных и прикладных науках любого государства. Уже активно обсуждается четвертая промышленная революция – глобальный процесс, связанный с переходом мировой экономики на принципиально новые технологии, основу которых во многом составляют искусственный интеллект и робототехнические решения. Этот процесс тесно связан с интенсивно развиваемыми облачными технологиями.

В настоящее время фактически происходит экспоненциальное возрастание объема информации для хранения, обработки, анализа, использования и защиты. Возможный способ эффективного решения

этих задач состоит в использовании функционально устойчивых автоматизированных информационных системах.

Автоматизированные информационные системы (далее – АИС) широко применяются в различных областях, в том числе, для управления ви чрезвычайных ситуациях. Они представляют собой аппаратно-программные технические устройства, которые используются для поддержки принятия управленческих решений в условиях чрезвычайных ситуаций и обеспечивают увеличение эффективности при принятии решений, повышение удобства пользования и расширение функциональных возможностей.

Использование облачных технологий позволит достичь определенных положительных результатов, таких как:

- для работы с системой потребуется только мобильное устройство и доступ к сети;

- если информация хранится в облаке, то при потере устройства не происходит потеря данных;

- облачные решения позволяют хранить все файлы в одном месте, что позволяет одновременно работать в одной центральной копии. Такая кооперация повышает общую производительность работы;

- ответственность за поддержку и обновление серверов будет возложена на поставщиков облачных сервисов. Также они смогут взять на себя и вопросы об аварийном восстановлении систем [1].

Однако, есть и определенные недостатки. Рассмотрим их более подробно. Кастомизация программного обеспечения – пользователь не имеет фактического доступа к программному обеспечению и не имеет возможности настроить его под свои собственные нужды. Также нужен постоянный и стабильный канал связи. И, конечно же, доверять информацию, а тем более конфиденциальную, невидимым защитникам на психологическом уровне является затруднительным.

В нашей стране оборонно-промышленный комплекс (далее – ОПК) является локомотивом многих наукоемких областей промышленности. Поэтому следует предположить, что именно ОПК будет главным инициатором масштабного внедрения облачных технологий.

Платформы на основе облачных автоматизированных информационных систем требуют постоянной, надежной работы в

условиях различных сбоев, стихийных бедствий и других разрушительных событий, которые могут привести к потере требуемого функционирования. Они зависят от распределенных информационных систем для всех аспектов их работы, поэтому живучесть этих критических информационных систем является важным вопросом.

Живучесть определяется способностью платформы продолжать предоставлять услуги в условиях различных типов отказов и сбоев. Основным механизмом, с помощью которого живучесть может быть достигнута в критических ситуациях, является ее функциональная устойчивость. Большая часть литературы по отказоустойчивым распределенным системам сфокусирована на терпимости к локальным дефектам путем их обнаружения и маскировки последствий этих неисправностей.

Главный предлагаемый принцип построения платформы состоит в том, что ее архитектура должна реализовать поддержку отказоустойчивости: обнаружение ошибок высокого уровня и скоординированного восстановления ошибок.

В целях оказания поддержки реконфигурации альтернативного сервиса для устранения ошибок в каждом узле его архитектура должна обеспечивать определенный набор возможностей. Эти критические сервисы обеспечивают основную поддержку, необходимую для изменения конфигурации, и они доступны для каждого процесса. Принимая во внимание процесс, который обеспечивает эти важные услуги, спецификация отказоустойчивости не обязательно должна быть связана с индексацией индивидуальной функциональности процесса. В качестве примера критической ситуации можно рассмотреть требование очевидной реализации, которую нужно будет запускать, а другие какие-то процессы останавливать в системе, подвергающейся реконфигурации для исправления ошибок. Таким образом, критические услуги, которые должны обеспечить эти процессы, являются способностью к запуску и остановке, которая надежно сохраняет состояние процесса в контексте применения. На самом деле, ни одно из этих действий не является тривиальным и не может быть оставлено полностью для использования основных услуг операционной системы [2].

Другой важный сервис, который должен обеспечить каждый узел для поддержания реконфигурации, является возможность переключения на альтернативный режим функциональных возможностей с помощью задания какого-либо параметра. Часто это не требуется. Чтобы процесс прекратился полностью и начался новый старт его необходимо разработать таким образом, чтобы обеспечить различные режимы функциональности и поддерживать переключение между режимами.

Следует подчеркнуть, что создание облачных автоматизированных информационных системах специального назначения (далее – ОАИС) ведется из предположения, что катастрофа в отличие от отказа (события возможного, прогнозируемого, вероятного) – это событие возможное, но невероятное, либо вероятность которого мала и не может быть обоснованно оценена в процессе проектирования. В противном случае речь шла бы не о катастрофе, а об условиях функционирования. Тогда основные элементы и подсистемы облачных АИС должны были бы создаваться исходя из требований отказоустойчивого функционирования в условиях воздействия огнем, в водной или химической агрессивной среде, в условиях поражения оружием (различных типов). Понятно, что стоимость таких систем была бы существенно выше по сравнению с информационными системами, которые ориентированы на нормальное функционирование.

Следовательно, свойство функциональной устойчивости АИС целенаправленно формируется (возникает) в этом случае в процессе ее функционирования и характеризуется соответствующей системой показателей. В частности, может быть предложен следующий перечень основных показателей качества функционирования облачных АИС: показатели доступности ОАИС (суммарное время простоев АИС по любым причинам), показатели, оценивающие риски возникновения и развития аварий и катастроф, показатели, оценивающие последствия аварий и катастроф для конкретных информационных процессов (продолжительность, масштаб и объем ущерба), показатели, оценивающие общие затраты времени и полноту выполненных операций, связанных с восстановлением работоспособности ОАИС, показатели, оценивающие, капитальные и

эксплуатационные затраты на обеспечение требуемого уровня устойчивости к катастрофам, затраты других видов ресурсов, показатели, оценивающие, степень критичности операций, выполняемых в информационных системах, значимость ресурсов и информации, используемой для обеспечения требуемого уровня устойчивости к катастрофам.

Функциональная устойчивость требует не только сохранности критически важных данных, но и обеспечения непрерывного (или прерываемого на некоторое время) функционирования АИС, а в случае невозможности реализации такого режима, в рамках ОАИС должно быть обеспечено с максимально короткие сроки восстановление ее работоспособности. В этих условиях целесообразно эффективность применения ОАИС оценивать не только показателем доступности, но и показателями функциональной устойчивости. Попутно можно отметить, что при отсутствии катастроф концепция обеспечения доступности к данным будет ориентирована на поиск технологий, обеспечивающих минимизацию потерь от плановых простоев.

В целом все решения по обеспечению восстановления и непрерывности функционирования любой информационной системы при наступлении катастрофы отличаются одним принципиальным параметром – временем восстановления функционирования (RTO – Recovery Time Objective), затрачиваемым с момента наступления катастрофы до перевода информационной системы в полностью рабочее состояние. Наряду с RTO, важнейшим понятием, определяющим требования к уровню непрерывности соответствующих информационных процессов, является понятие RPO (Recovery Point Objective – целевая точка восстановления, см. рис. 1) – согласованный интервал времени, предшествующий аварии, в течение которого допускается потеря данных. Иными словами, этот параметр показывает, насколько состояние системы и данных может откатиться назад при чрезвычайной ситуации [3].

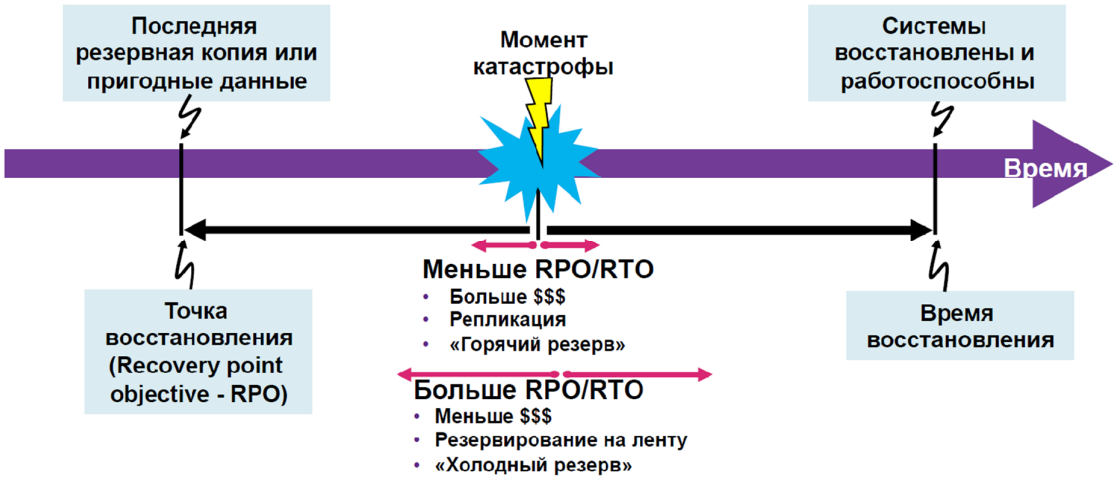

Рисунок 1 – Графическая иллюстрация целевой точки восстановления и целевого времени восстановления

Безусловно, необходимо активизировать работы по созданию действительно унифицированных средств объединенных органов управления, разработке современных алгоритмов их работы при решении различных боевых задач, формированию перечня систем и средств, которые планируется связать в сети на разных уровнях управления с обоснованием почему и, самое главное, для чего это нужно.

Сложные системы, состоящие из большого количества взаимодействующих узлов, проще разделить на отдельные подсистемы. После анализа простых систем необходимо снова попытаться их объединить в исходную систему и понять сложное явление в целом.

Единая интегрированная информационная сфера, функционирующая в реальном масштабе времени, позволяет значительно увеличить степень ситуационной боеготовности вооруженных сил, минимизировать неопределенность обстановки, ускорить процесс принятия решения и увеличить темпы операций.

Однако облачные технологии не решают полностью вопросы задержки запросов и ответов при резком увеличении абонентов. Новой перспективной парадигмой, расширяющей облачные вычисления к периферии сети, являются туманные вычисления. Внедрение туманных вычислений обусловлено решением ряда имеющихся недостатков облачных технологий, присущих для

необходимого выполнения задач специального назначения, таких как задержки запросов и ответов при резком увеличении абонентов, а также децентрализованного распределение ключевой информации.

Технология туманных вычислений позволяет прямо на краю сети внедрять новые приложения и сервисы для миллионов подключенных устройств. Симбиоз облака и тумана решает также проблему создания доверительных каналов на основе идентификаторов пользователей и их биометрических характеристик. А это в свою очередь ведет к решению проблемы децентрализованного распределения ключей.

Концептуальная архитектура инфраструктуры туман-облако показано на рисунке 2.

Рисунок 2 – Пример архитектуры из тумана и облака

Определение как новой парадигмы вычислений, туманные вычисления еще не стали полноценной идеей в обществе. Туманные вычисления представляют расширение облачных вычислений на границе сети, которая является виртуализированной платформой из пула ресурсов, который предоставляет вычисления, хранение и сетевые службы до ближайших конечных пользователей. Это «сценарий», где огромное число разнородных (беспроводных, а иногда и автономных) повсеместно и децентрализованных устройств общаются и сотрудничают между собой и с облаком для выполнения хранения и обработки заданий без вмешательства третьих сторон.

Эти задачи могут быть для поддержки базовых сетевых функций или новых услуг и приложений, которые выполняются в изолированной среде.

Характеристика туманных вычислений имеет свои преимущества из-за своего пограничного местоположения, и поэтому способны поддерживать приложения (например, дополненная реальность, видео в реальном времени обработки потока) с малой задержкой. Этот край также может предоставить богатый контекст информационной сети, такие как локальные состояния сети, статистику трафика и сведения о состоянии клиента, которые могут быть использованы туманные заявки на контекстно-зависимые оптимизации. Другой интересной характеристикой является расположение-осведомленность; не только географически определить собственное местоположение, но и может отслеживать устройства конечного пользователя для поддержки мобильности, которые могут быть поворотным фактором для геолокационных сервисов и приложений. Кроме того, взаимодействия между туманом и туманом, туманом и облаком становятся важными, поскольку туман может легко получить местный обзор, в то время как глобальный охват может быть достигнут только на более высоком уровне [3].

Повсеместное распространение интеллектуальных устройств и опережающее развитие стандарта виртуализации и облачных технологий позволяет реализовать туманные узлы. Туманные узлы, как правило, строится на существующих сетевых устройствах. Служба доставки и развертывания модели, похожая на облачные вычисления, позволяет предвидеть, что служба доставки моделей в туманных вычислениях может быть сгруппирована в три категории: программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктуры как услуги (IaaS). Мы также можем ожидать следующие модели развертывания: частный туман, туман сообщества, общественный туман и гибридный туман.

Аналогично понятие облачных вычислений для мобильных устройств и мобильный вычислительный край (далее – МВК) похожи на туманные вычисления. МВК относится к инфраструктуре, в которой обработка и хранение данных происходят за пределами мобильных устройств. В МВК акцент на богатые ресурсами туманные сервера как облачка, бегущие краем мобильных сетей. Туманные

вычисления зарекомендовали себя, как более обобщенная парадигма вычислений, особенно в контексте Интернета вещей.

Проверка подлинности как появление биометрической аутентификации в мобильных вычислениях и облачных вычислениях, такие как проверка подлинности отпечатков пальцев, идентификации лица, касания или нажатия клавиш на основе, и т.д., все это будет полезно для применения биометрической аутентификации, основанные на туманных вычислениях.

Внедрение «облачного» сервера, как следствие, требует и введение «личного кабинета», который обеспечит управление доступом к программам, данным и сервисам на различных уровнях. То есть пользователь может осуществить доступ к необходимым данным и сервисам с любого рабочего места системы.

Основными отличительными характеристиками реализации являются:

- взаимодействие пользователей с представляемыми «облаком» сервисами осуществляется через «личный кабинет», представляющий собой персонализированный интерфейс с набором инструментов для работы с «облачными» сервисами;

- аутентификация пользователей для доступа в «личный кабинет» производится криптографическими средствами;

- работа в «личном кабинете» осуществляется через веб-интерфейс браузера и доступна как с мобильных, так и со стационарных устройств;

- интерфейс «личного кабинета» персонализируется в соответствии с полномочиями пользователя и предоставляет доступ к сервисам «облака» только в разрешенном данному пользователю объеме (туманные вычисления).

Для реализации данных решений необходимо, чтобы на каждой виртуальной машине было установлено специальное программное обеспечение (далее – СПО). При этом безопасность информации в информационных системах будет определяться защищенностью каждого из компонентов облачной инфраструктуры, а также защищенностью модулей СПО, используемого при построении защищаемого рабочего места.

Система должна осуществлять идентификацию и аутентификацию «облачных» клиентов (в том числе стационарных,

мобильных и портативных), а также пользователей как работников-поставщиков облачных услуг, так и потребителей.

Для успешной реализации такой системы также необходимо прописать требования, основными из которых являются, по управлению доступом субъектов доступа к объектам доступа, по регистрации событий безопасности, по антивирусной защите, по обнаружению (предотвращению) вторжений, по обеспечению целостности СПО, а также по защите облачного сервиса, его средств и систем связи и передачи данных. И это еще не весь перечень требований по обеспечению защиты информации.

Главные преимущества использования ОАИС для потребителей состоят в улучшении производственных процессов, благодаря уменьшению капитальных и эксплуатационных затрат на персональную информационную инфраструктуру. Однако такие характеристики приводят к возникновению актуальных угроз информационной безопасности, которые связаны, с уменьшением уровня контроля процесса обработки информации, и с динамичностью модели предоставления ресурсов.

Таким образом, используя новые возможности при использовании облачных технологий, потребитель приобретает способность использования дополнительных средств контроля за доступом к информации, таких как разграничение физического доступа и иных организационных и технических мер. Это не позволит злоумышленникам реализовать мероприятия, которые позволили бы резко сократить количество имеющихся в доступе вычислительных ресурсов.

Литература

1. Давыдов А.Е., Максимов Р.М., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. М.: Мир, 2015. 520 с.

2. Тобин Д.С. Информационно-логическая модель процессов разработки программной платформы в органах военного управления // Известия Тульского государственного университета. Технические науки. 2020. № 9. С. 337-348.

3. Чучин М.И., Чижиков В.И., Шарифуллин С.Р. Робототехнические комплексы и автоматизированные информационные системы // Технические и технологические системы: Материалы VIII международной научной конференции «ТТС-16». Краснодар, 2016. С. 191-194.

4. Чучин М.И., Чижиков В.И., Шарифуллин С.Р. Анализ использования облачных технологий в распределенных информационных системах // Научные

чтения имени профессора Н.Е. Жуковского: Сборник научных статей VII Международной научно-практической конференции. М., 2017. С. 204-211.

5. Богомолов А.В. Методика формирования индекса состояния объекта по результатам многомерной статистической классификации // Информационные технологии. 2000. № 12. С. 45.

6. Тобин Д.С. Сетевая экспертно-аналитическая платформа как инструментальное средство поддержки принятия решений в распределенной среде // Вестник НГУЭУ. 2020. № 3. С.231-240.

7. Ронжин А.Л., Железны М. Цифровизация управленческих процессов в научно-образовательных организациях // Управленческое консультирование. 2018. № 10 (118). С. 109-117.

8. Кукушкин Ю.А., Богомолов А.В., Ушаков И.Б. Математическое обеспечение оценивания состояния материальных систем. Информационные технологии. 2004. № 7 (приложение). 32 с.

9. Богомолов А.В., Климов Р.С. Автоматизация обработки информации при проведении коллективных сетевых экспертиз // Автоматизация. Современные технологии. 2017. Т. 71. № 11. С. 509-512.

10. Юсупов Р.М., Ронжин А.Л. От умных приборов к интеллектуальному пространству // Вестник Российской академии наук. 2010. Т. 80. № 1. С. 45-51.

11. Ларкин Е.В., Богомолов А.В., Привалов А.Н. Методика оценивания временных интервалов между транзакциями в алгоритмах сжатия речевых сообщений // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2017. № 9. С. 23-28.

12. Larkin E.V., Bogomolov A.V., Privalov A.N., Dobrovolsky N.N. Discrete model of paired relay-race // Bulletin of the South Ural State University. Series: Mathematical Modelling, Programming and Computer Software. 2018. Vol. 11. № 3. Pp. 72-84.

13. Ронжин А.Л. Математические модели и средства многомодального интерактивного взаимодействия с робототехническими и киберфизическими системами // Математические методы в технике и технологиях - ММТТ. 2016. № 11 (93). С. 64-71.

14. Тобин Д.С. Особенности организации цепочек переходов при проведении сетевых экспертиз в закрытом блокчейне // I-methods. 2020. Т. 12. № 2. С. 1-10.

15. Ларкин Е.В., Привалов А.Н., Богомолов А.В. Дискретный подход к моделированию синхронизированных эстафет // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2020. № 2. С. 17-26.

SHISHOVEC@RAMBLER.RU