5. Модели и методы анализа и синтеза сценариев развития социально-экономических систем: в 2-х кн. / Под ред. В.Л. Шульца и В.В. Кульбы. – М.: Наука, 2012. Кн. 1. – 304 с., кн. 2. – 358 с.

DOI: 10.25728/iccss.2022.53.89.025

Ходнев Н.Д., Краснов А.Е.

Хранение документов, аспекты информационной безопасности

Аннотация: Ценность и объем информации вырос. Организации всё чаще сталкиваются с проблемой хранения и доступности информации. Целью данной работы является анализ специфики хранения данных.

Ключевые слова: хранение данных, хранения данных в облаке, хранение данных на локальном сервере, информационная безопасность

Дистанционный формат обмена документами представляет значительный интерес, как для компаний, так и для образовательных учреждений. Он служит поддержке осуществляемых бизнес-процессов в масштабе реального времени. Помимо этого, с каждый годом увеличивается общий объем информации и ее ценность. Рабочие документы необходимо хранить и иметь к ним оперативный доступ для пополнения и использования. Также немаловажным требованием является безопасность обрабатываемых данных.

Цель данной статьи связана с анализом специфики хранения данных в облаке и на собственном сервере при использовании дистанционного формата взаимодействия.

Основной задачей работы является сравнение:

- соответствий международным стандартам;
- стоимости хранения данных;
- конфиденциальности доступа;
- надежности и целостности данных;
- масштабируемости системы.

В случае локального хранения данных сервер приобретается самой организацией и встраивается в общую инфраструктуру. Во многих случаях это физический носитель. Все данные на сервере контролирует, обслуживает и поддерживает все аппаратное и

программное обеспечение организация (непосредственно IT-отдел) или привлеченные извне эксперты. Такие сервера, как правило, закрыты для внешнего доступа и функционируют только внутри локальной сети.

При использовании облачного хранения данных, всю информацию размещают у сторонних поставщиков услуг, например Yandex. Поставщик облачных технологий сам заботится о приобретении, поддержке и т.д. аппаратного и программного оборудования, а также о всех издержках вспомогательной инфраструктуры для сопровождения этого решения. Организация управляет своими данными через учетную запись в интернете с помощью веб-браузера.

Оба этих решения сравниваются по следующим ключевым позициям: соответствие международным стандартам, стоимости хранения данных, конфиденциальность доступа, надежность и целостность данных, масштабируемость системы.

Соответствие международным и локальным требованиям. Если организация нацелена на внутренний рынок Российской Федерации, она должна соответствовать требования основополагающих документов, например, таких как: ФЗ № 149 «Об информации, информационных технологиях и о защите информации»; ФЗ № 152 «О персональных данных»; ФЗ № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» и других. При выходе на внешний рынок, организация должна соответствовать международным стандартам, например, регламенту GDPR и т.п.

При разворачивании собственной инфраструктуры, для соответствий всем требованиям придется нанимать эксперта в этой области и затратить много ресурсов и времени на реализацию. При обращении к поставщику облачных услуг, вы можете убедиться, что их решение имеет сертификат о подтверждении соответствия во всех ключевых областях, которые вам необходимы.

Стоимость. Локальное размещение сервера в краткосрочной перспективе требует вложения множества средств в оборудование, оплату лицензий, содержание IT-отдела, обслуживающего сервер и отдел (служба), обеспечивающий информационную безопасность. Помимо этого, после завершения всех циклов установки и настройки аппаратного и программного обеспечения придется содержать в

штате IT-отдела специалиста для поддержки работоспособности сервера и реагирования на инциденты. Стоимость обслуживания должна быть заложена в бюджет организации, так как аппаратное обеспечение может выйти из строя по разнообразным причинам.

Облачное решение имеет значительное преимущество над локальным размещением – отсутствие первоначальных капиталовложений. Организация оплачивает только ежемесячную или ежегодную подписку. Актуальность, безопасность, обслуживание и поддержка аппаратного и программного обеспечения находится в зоне ответственности поставщика облачных решений. Зачастую расходы на облачные технологии меньше, чем сумма, которая необходима на поддержание собственной инфраструктуры. Однако стоит отметить, что облачные технологии не являются панацеей и оправданность перехода на этот тип хранения данных необходимо рассматривать отдельно в каждом частном случае.

Конфиденциальность доступа. С точки зрения безопасности, размещение своих данных локально не снимает ответственности за разработку средств защиты информации. Даже несмотря на то, что локальные сервера, как правило, недоступны снаружи, необходимо разграничивать доступ ко всем данным. Это требует высокого уровня знаний в области информационной безопасности [1].

При использовании облачных решений, все ваши данные находятся в сети интернет. Эта технология обеспечивает наиболее высокий уровень защиты и избавляет организацию от лишних затрат на информационную безопасность. Облачные решения, как правило, поддерживает большая команда экспертов по кибербезопасности. Все накладные расходы на это выделяются за счет поставщика облачных решений. По оценке Gartner, облачные решения на 60 % меньше подвержены инцидентам, связанным с информационной безопасностью, чем размещение данных на собственных серверах.

Надежность и целостность данных. Часть организаций размещают ресурсы локально, так как штатным сотрудникам не требуется подключение к интернету, чтобы получить доступ к данным. Однако может случиться форс-мажор, например пандемия, впоследствии которого придется организовывать удаленный доступ и обеспечить защищенное подключение. Кроме того, для функционирования локального сервера требуется резервное питание

(например, генератор) для бесперебойной работы [2]. И создать систему резервного копирования данных, сохранность которых должна обеспечивать организации.

Для взаимодействия с облачным хранилищем необходимо быстрое и стабильное подключение к интернету. При отсутствии интернета нет возможности получить доступ к данным. Сбой подключения во время работы может привести к снижению продуктивности и частичной потере данных. Резервное копирование данных и бесперебойный доступ при хранении в облаке гарантирует поставщик облачного решения.

Масштабируемость. Если ваша локальная инфраструктура перестает справляться с рабочей нагрузкой [3], организации необходимо масштабировать свои вычислительные возможности, добавляя новое программное и аппаратное обеспечение. Для этого необходимо выделять бюджет и время. В случае если такой прирост нагрузки вносит временные рамки, то расходы могут оказаться неэффективными и неоправданными.

Облачные технологии позволяют автоматизировать эти издержки. Организация может масштабировать свои ресурсы путем повышения тарифного плана. Это экономит время на установку и введение в эксплуатацию аппаратного обеспечения. Также все эти изменения могут быть отменены в любой момент времени.

Каждый из двух подходов имеет свои плюсы и минусы и должны быть отдельно рассмотрены для каждого конкретного случая. Средний и малый бизнес всё чаще используют облачные решения для разворачивания своей инфраструктуры, так как это помогает сократить время на начальных этапах развития. Но в долгосрочной перспективе это может оказать негативные последствия. Облачные технологии не лишены изъянов, и очередное минорное обновление базы данных может сильно увеличить нагрузку и послужить причиной отказы от обслуживания со стороны базы данных.

Литература:

1. *Краснов А.Е., Мосолов А.С., Феоктистова Н.А.* Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность

информационных технологий. – 2021. – Т. 28 (1). – С. 106-120. DOI: 10.26583/bit.2021.1.09

2. *Кононов А.А., Котельников А.П., Черныш К.В.* Оценка защищенности критически важных объектов на основе построения моделей событий рисков // Труды ИСА РАН. – 2012. — Т. 62. Вып. 4. – С. 69-75. – URL: http://www.isa.ru/proceedings/images/documents/2012-62-4/t-4-12_69-75.pdf (дата обращения 10.10.2022).

3. *Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Калачев А.А.* Нейросетевой подход к проблеме оценивания эффективности функционирования организации на основе агрегирования показателей ее деятельности // Информатизация образования и науки. – 2017. – № 1 (33). – С. 141-154. – URL: https://informika.ru/pechatnye-izdaniya/zhurnal-informatizaciya-obrazovaniya-i-nauki/arhiv-vypuskov/2017/vypusk-n33/ (дата обращения 10.10.2022).

DOI: 10.25728/iccss.2022.54.97.026

Сомов С.К.

Влияние использования архивов магнитных носителей на некоторые показатели надежности распределенных систем обработки данных

Аннотация: В работе представлены результаты анализа влияния использования восстановительного резерва в виде архива магнитных носителей на показатели надежности работы распределенных систем обработки данных. Анализировались такие показатели надежности работы систем, как среднее время работы системы до отказа, вероятность отказа и вероятность безотказной работы системы заданных интервалах времени.

Ключевые слова: распределенные системы, оперативное и восстановительное резервирование данных, показатели надежности работы распределенных систем

В распределенных системах обработки данных (РСОД) различного назначения для обеспечения высокого уровня