

все эти элементы в той или иной мере подвержены коррозии. Поэтому наработки до отказа резервуарных конструкций являются коррелированными (а значит и зависимыми) случайными величинами.

В статье нефтяной резервуар рассматривается как система, состоящая из последовательно соединенных элементов (днища, узла сопряжения стенки с днищем, цилиндрической стенки и кровли), отказы которых являются зависимыми событиями. Показывается, что зависимость вероятностных показателей надежности такой системы от соответствующих показателей конструктивных элементов выражается моделью «слабейшего звена».

Список литературы

1. Егоров Е.А., Семенец С.С. Систематизация фактора восстановления в моделях эксплуатационного состояния нефтяных резервуаров// Вісник ПДАБА.–2006.–№.2.–С.10-18.
2. Аугусти Г., Баратта А., Кашиати Ф. Вероятностные методы в строительном проектировании: Пер. с англ.– М: Стройиздат,1988.–584 с.
3. Відомчі будівельні норми України ВБН 2.2-58.2-94. Резервуари вертикальні сталеві для збереження нафти і нафтопродуктів з тиском насичених парів не вище 93.3кПа.– Київ,1994.–98 с.

МОДЕЛЬ ОБЕСПЕЧЕНИЯ СЕТЕВОГО ДОСТУПА ПО ТРЕБОВАНИЮ К ОБЩИМ ВЫЧИСЛИТЕЛЬНЫМ РЕСУРСАМ

А.В. Кнышова

(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

С появлением таких мощных и надежных «облачных» технологий (cloud technologies), появились такие сервисы: программное обеспечение как услуга (англ. Software as a Service, SaaS), платформа как услуга (англ. Platform as a Service, PaaS), инфраструктура как услуга (англ. Infrastructure as a Service, IaaS) [2]. Предполагалось, что они займут лидирующее место на рынке в 2012 году. Однако недавно проведенное исследование компанией PEER 1 показало, что из 85% респондентов, которые не используют эти технологии, 41% высказали мнение, что не применяли облачные технологии, потому что не владели достаточной информацией о них.

Суть данной технологии заключается в том, что облачные вычисления дают возможность хранить файлы и программное обеспечение удаленно, а не на жестком диске или сервере. Многие из нас уже пользуются этими технологиями и даже не подозревают об этом, будь то по работе или в личных целях. Примерами служат веб-почта, такая как Gmail и Hotmail, средства связи, такие как Skype, видеосайты, такие как YouTube и Vimeo и т.д.

Благодаря тому, что облачные вычисления включают программное обеспечение как услугу (SaaS), хранение файлов, синхронизацию файлов данных и файлов резервного копирования, многие предприятия могут иметь свои собственные частные «Облака», которые включают в себя конкретные услуги и доступ к ним возможен только для ограниченного числа людей.

Одна из причин, по которой многие предприятия применяют облачные вычисления – затруднение изменения и уничтожения их данных. Однако существуют некоторые потенциальные недостатки облачных вычислений, которые стоит иметь в виду. Обратная сторона в том, что многие обеспокоены вопросами безопасности, связанными с хранением своих данных в Сети. Недавний инцидент, произошедший с «облачным» хранилищем Dropbox, заставляет все больше задумываться о конфиденциальности информации [1]. Данные (изображения, документы) 15-ти млн. пользователей можно было просмотреть любому желающему.

Еще одной проблемой для пользователей и компаний, становится потеря подключения к Internet. Риски, связанные с этим, в нашей стране являются актуальными, поскольку исправление неполадок в работоспособности системы занимает обычно от 2 до 4 дней и это, как правило, вызывает огромные простои на предприятиях и потерю финансовых средств. Предприятиям, которые реализованы с помощью облачных вычислений, необходимо предпринять меры, чтобы снизить риск каких либо сбоев в работе Internet и понизить скорость передачи информации.

Как обеспечить защиту данных, размещенных в интернет-хранилище? На сегодня это является самой актуальной задачей и вот несколько простых мер безопасности.

Личная информация. При использовании веб-сервисов указывайте только самые необходимые сведения. Поля, необязательные для заполнения оставляете пустыми.

Банковские карты. Для совершения платежей в Сети пользуйтесь предоплаченными пластиковыми картами или виртуальной картой Visa (такую услугу предлагает, платежная система QIWI). Если даже злоумышленники завладеют данными, то даже в самом худшем случае они смогут воспользоваться только предоплаченным номиналом, который должен быть самым минимальным.

Шифрование. Используйте для своих фотографий и данных, помещенных в «облачное» хранилище, программу шифрования – например, FreewareBoxCryptor. Эта утилита работает в фоновом режиме и шифрует данные перед их отправкой в «облако». Для других сервисов применять утилиту TrueCrypt [1].

Главной проблемой этой технологии на сегодня является безопасность и от этого никуда не деться. Пока что, это новшество и все недостатки проявляются в огромных количествах. Всем хочется показать насколько «cloud technologies» уязвимы и небезопасны, но всему нужно время, чтобы устояться. За данными технологиями будущее, поскольку будет возможность использовать все необходимые ресурсы, не боясь за целостность, доступность и конфиденциальность имеющихся данных.

Список литературы

1. Леонов К., Васильев Г. Goofle Dods, Windows Live и другие облачные вычисления. Том 1 М.: Эксмо. 201206. 306 с.
2. <http://kanobu.ru/blog/id177990> (Облачные вычисления).