УДК 004

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ СЕРВИСОВ

Молчанова А.Д., студентка 3курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *Безопасность, облачные сервисы, технологии.*

Уже давно никто не сомневается в том, что облачные технологии – это удобно и выгодно. Однако вопросы безопасности по-прежнему тревожат многих руководителей во всем мире.

Облачный сервер (облачное хранилище) – это услуга, предполагающая хранение данных в сети на серверах, предоставляемых в пользование клиентам третьей стороной.

На данный период времени облачные сервисы стали настолько популярными и непосредственно связаны с оснащением основных изготовителей компьютеров и разных гаджетов, что многие даже не думают в каком месте хранятся их данные и что с ними происходит.

Рисунок 1 - Облачные сервисы

В части доступности облачного сервиса все хорошо. Почти все поставщики облачных услуг обеспечивают значительную общедоступность обслуживания. Но давайте представим, где заканчивается зона

ответственности поставщика облачных услуг и где находитесь вы со своими устройствами доступа в Интернет.

Существует не мало факторов, по которым вам могут быть недоступны ваши информации, хранящиеся в облаке, при том что сам по себе облачный сервис будет полностью работоспособным. По этой причине настоящая общедоступность облака обслуживания существенно ниже объявленных в пользовательском соглашении и чисел.

Рисунок 2 - Преимущества и недостатки облачных сервисов

Преимущества облачного сервиса

1. Вы всегда сможете поделиться своими файлами с друзьями, предоставив доступ или отправив ссылку на файл.

2. В «облаке» можно хранить любую информацию (музыку, фотографии, видео, контакты, приложения), доступ к которым вы можете получить с любого мобильного устройства или компьютера, достаточно иметь интернет.

3. В случае неисправности компьютера, ваши файлы в «облаке» всегда останутся целыми и невредимыми.

Плюсы и минусы облачных сервисов

Несмотря на то, что формальных обязательств по обеспечению данных качеств информации у провайдера нет, все известные мировые

информационные технологии – компании при организации облачных сервисов обеспечивают достаточно высокий уровень защиты данных как от несанкционированного доступа к ним, так и от уничтожения по каким – то техническим причинам. То есть прямой атакой на ресурсы провайдера облачных услуг злоумышленники вряд ли смогут достигнуть цели. Основная уязвимость интернет – сервисов заключается в использовании практически только парольной защиты и применении не совсем надежных способов восстановления забытых защищенных данных – логинов и паролей (чаще всего- через электронную почту). Организациям при подключении облачных сервисов стоит сразу позаботиться реализацией какого-либо механизма двухфакторной защиты. Зрелость облачных сервисов в части обеспечения информационной безопасности на данный период времени оставляет желать лучшего.

Если вы хотите обеспечить дополнительную защиту информации в облаке, то следует использовать шифрование данных. Этот способ защиты возможен, если вы не планируете обрабатывать информацию в облаке (например, редактировать фотографии или текст), а только хранить и передавать данные в изначальном виде. Следует учесть сложности с распределением и управлением криптографическим ключом (особенно для больших организаций) и потери в мобильности (для доступа к данным у вас на устройстве должен быть актуальный криптографический ключ, хранящийся безопасным способом, а с этим могут возникнуть технические или технологические проблемы) .

Проводя анализ, многие предпочитают покупать торт, а не печь его самим. Причем облачный сервис, как правило, позволяет оперативно изменять параметры сервиса, что не просто удобно, а для большинства организаций необходимо при существенно возросших темпах изменений в требованиях бизнеса. Нельзя не отметить и значительно большую приспособленность облачных сервисов для мобильных пользователей, а бизнес и мы сами с каждым годом становимся все более мобильными .

Поэтому независимо от того, доверяете вы облакам или нет, они уже вошли и скоро войдут в вашу жизнь. И стоит уже сейчас задуматься о том какую информацию вы готовы доверить облакам и как можно минимизировать те риски, которые обсудили в данной статье.

Библиографический список

1. Облачные вычисления (мировой рынок). - Режим доступа: URL: http://www.tadviser.ru/index.php (дата обращения 15.03.16.).

2. Облачные хранилища данных.- Режим доступа: URL: http://www.topobzor.com/obzor-10-oblachnyx-xranilishh-dannyx/.html (дата обращения 16.03.16.).
3. Облачное хранилище для смартфона. - Режим доступа: URL: http://andro-ed.com/statja/cloud-storage-for-smartphone/ (дата обращения 16.03.16.).
4. Попов, А.А. Использование облачных технологий для формирования инновационной ИТ-инфраструктуры и управления многоквартирными домами / А.А. Попов // Вестник Тверского государственного университета. Серия: «Экономика и управление».- 2013.- № 21.- С. 163-176.

SECURITY DATA INFORMATION SYSTEMS IN THE ENTERPRISE

Molchanova A.D

Key words: *safety, cloud services, technologies.*

For a long time nobody doubts that a cloud computing – it is convenient and profitable. However safety issues still disturb many heads around the world.