АНАЛИЗ РИСКОВ ИСПОЛЬЗОВАНИЯ ОБЛАЧНЫХ ХРАНИЛИЩ

Крень Н.С., Бакунович Д.С., Савенко А.Г.

Институт информационных технологий БГУИР, Минск, Беларусь, savenko@bsuir.by

Облачные хранилища получили большое распространение в последние годы. С развитием технологий стремительно увеличивается объём хранимой и обрабатываемой информации, а также требования к скорости обмена данными. В связи с этим возникает проблема рисков использования такого типа систем. Данная проблема может быть разделена на три вопроса: сохранность данных, доступность данных и конфиденциальность данных.

Сохранность данных напрямую зависит от конфигурации и качества обслуживания сервера. Применение RAID-технологий, настройка автоматического резервного копирования, своевременное техническое обслуживание сервера и другие подобные меры приводят к обеспечению максимально высокой сохранности, что положительно отражается на безопасности облачных хранилищ. Однако, в случае несоблюдения данных мер, вероятность потери информации куда выше, чем при хранении данных на локальном носителе.

На доступность данных влияют: настройки сервера, наличие доступа к интернету, аварии на линиях, DDOS-атаки и т.д. Повлиять на большую часть этих проблем не представляется возможным, если сервер не обслуживается самостоятельно и не находится в локальной сети (как и бывает в большинстве случаев). Минимизировать проблемы доступа в данном случае можно путём использования нескольких различных интернет-подключений. Чтобы иметь возможность получать данные из любой точки мира, рекомендуется использовать спутниковое подключение. Однако, полностью избежать проблем с доступом на данный момент невозможно в связи с возможными авариями и хакерскими атаками.

Наиболее важным вопросом является конфиденциальность хранимых данных. При использовании локального сервера, особенно без доступа в интернет, вероятность утечки данных минимальна. При использовании облачных хранилищ может возникнуть ряд проблем. Первая проблема, с которой можно столкнуться – это перехват данных при отправке на сервер, либо загрузке с сервера. Избежать данной проблемы можно путём использования зашифрованных соединений (FTPS, SFTP) либо шифруя данные локально, до начала передачи. Вторая проблема – это утечка данных прямо с сервера. Её возникновение возможно по различным причинам, таким как: уязвимости системы, неправильная конфигурация сервера, не добросовестный администратор и т.д. Третьей возможной проблемой является авторизация. Завладев данным для авторизации, злоумышленник может получить доступ ко всей информации хранящейся на сервере. Чтобы этого избежать, необходимо настроить двухфакторную аутентификацию и установить защиту от перебора пароля. Со стороны пользователя требуется хранить в секрете данные аутентификации и сопутствующие личные данные.

В заключении можно сказать, что при корректном использовании и настройке облачного сервера, хранение данных достаточно безопасно. Однако, остаётся открытым вопрос доступа к информации и её конфиденциальности.