Ознакомься со статьей ***Облачные угрозы: эксперты рассказывают о защите данных в облачных сервисах*** *на сайте* **Securenews**

https://securenews.ru/cloud_data/

В продолжение «облачной» темы одного из предыдущих материалов мы решили обратиться к проблеме безопасности облачных сервисов.

SecureNews не единожды сообщал о взломах и утечках информации из облачных сервисов. Например, мы рассказывали об атаке на сервисы Dropbox и OneLogin, а также о многочисленных утечках информации, связанных с незащищенными облачными серверами Amazon.

В этой связи мы решили обратиться к экспертам в сфере ИБ и облачных технологий, чтобы разобраться в том, смогут ли облачные хранилища стать заменой физических носителей, насколько такие сервисы безопасны и как пользователи могут защитить свою информацию, помещенную в «облако».

«За облачными хранилищами - будущее?» Заменят ли полностью облачные хранилища физические носители информации?

Алексей Федоров, директор рекомендательной системы по облачным сервисам Startpack

Алексей Федоров, директор рекомендательной системы по облачным сервисам **Startpack**:
«В прикладных задачах, вроде работы с документами, облачные хранилища действительно заменят физические носители. Такую модель используют Google и Microsoft в сервисах Google Диск и OneDrive соответственно. Облачные хранилища Dropbox, Яндекс Диск, Облако Mail.Ru изначально не имели возможности работы с документами, но ввели такую возможность. Совмещение работы с документами и их хранения настолько естественно, что еще в 2005 году хранилище Box позиционировало себя «как SharePoint, только лучше». Шесть лет существования Chromebook — ноутбука, где нет ничего кроме браузера, также показывает, что модель имеет право на существование. Вместе с тем, существуют прикладные задачи, для которых хранение файлов в «облаке» нецелесообразно: обработка видео, работа со звуком, инженерное проектирование. Большинство игр подразумевают наличие у пользователя компьютера с объемным жестким диском. Даже для запуска удаленного рабочего стола, тонкий клиент должен обладать какие-то базовыми функциями «на месте».

Алексей Шипов, руководитель по развитию облачной платформы ICL Cloud в компании ICL Services

Алексей Шипов, руководитель по развитию облачной платформы **ICL Cloud** в компании **ICL Services**:
«Сейчас мы наблюдаем взрывной рост использования облачных хранилищ для данных, генерируемых в социальных сетях. Ведь многие фото и видео, снятые на смартфоне, автоматом уходят в «облако». Использование «облака» для коммерческих данных растет чуть медленнее, но стабильно на 30-50% каждый год. Посмотрите, как Microsoft встраивает в Windows Server возможности быстрого переноса данных в

публичное «облако» Azure. Такие же тренды просматриваются и у остальных вендоров. Вероятно, уже через 5-10 лет больше половины данных будет храниться в «облаке». Однако, для особо ценной и важной информации не потеряет актуальности локальное хранение с использованием самых современных средств защиты, например, квантового шифрования».

Денис Полянский, руководитель направления защиты виртуализации и облачных платформ компании «Код безопасности»

Денис Полянский, руководитель направления защиты виртуализации и облачных платформ компании **«Код безопасности»**:
«У облачных хранилищ много преимуществ: высокая доступность, масштабируемость и так далее. И они продолжат набирать популярность в ближайшей перспективе. Но есть ряд аспектов, делающих облачную модель сложно применимой в некоторых кейсах. Например, невозможность получить согласие субъектов на передачу персональных данных на сторону провайдера или нежелание заказчика передавать определенный тип данных на сторону (клиентские базы, финансовые системы). Затруднение также может возникнуть, если есть проблемы с подключением к сети на стороне клиента, но продолжить работу надо (локально). Поэтому в ближайшее время стопроцентного вытеснения облачными сервисами локальной обработки данных не произойдет. Наиболее популярная и перспективная модель на сегодня – так называемые «гибридные облака», сочетающие в себе преимущества облачных сервисов и локального хранения и обработки данных. «Облака» хорошо зарекомендовали себя для резервного хранения информации на случай проблем в локальной инфраструктуре».

Рустэм Хайретдинов, генеральный директор компании «Атак Киллер»

Рустэм Хайретдинов, генеральный директор компании **«Атак Киллер»**:

«Полной замены, конечно, не будет, во всяком случае – в обозримом будущем. За сотню лет человечество не научилось обеспечивать людей электричеством со стопроцентной гарантией, то и дело происходят обрывы и «блекауты» из-за природных явлений и техногенных катастроф, то что же говорить про облачные сервисы. Есть информация, которую уже сегодня удобнее хранить в «облаках» – это «тяжелые», не часто нужные и при этом редко меняющиеся файлы, например – фильмы, музыку, фотографии. Но и для них хорошо бы пока иметь резервную физическую копию, особенно, если такая информация сделана вами и существует в единственном экземпляре. Для данных же, которые нужны постоянно и при этом они постоянно меняются, пока лучше использовать он-сайт или хотя бы гибридную архитектуру – хранить данные и в «облаке», и у себя».

Насколько безопасны облачные сервисы?

Алексей Федоров:
«Опасность использования облачных хранилищ можно поделить на два типа: потеря информации и утечка информации. Потеря информации сейчас невозможна почти в любом облачном хранилище, поскольку информация многократно копируется и хранится на разных серверах и в разных дата-центрах. Например, чтобы Google потерял файлы пользователя, нужно чтобы в одночасье исчезли два континента. Однако, отечественные облачные хранилища на заре появления имели прецеденты с потерей данных пользователей. Некоторые хранилища, по условиям пользовательского соглашения, удаляют данные, если пользователь не пользовался ими несколько месяцев.

Обычно для входа в облачное хранилище нужен логин и пароль, если злоумышленник узнал эти данные, он может получить доступ к хранящимся файлам. Так происходили утечки личных фотографий из iCloud знаменитостей».

Андрей Рыбин, заведующий сектором информационной безопасности Департамента информационных технологий (ДИТ) города Москвы

Андрей Рыбин, заведующий сектором информационной безопасности **Департамента информационных технологий (ДИТ)** города **Москвы**:

«Использование облачных сервисов не является безопасным. Основными угрозами информационной безопасности при использовании облачных технологий являются: хищение и потеря данных, взлом аккаунтов, уязвимости в интерфейсах и API, DDoS-атаки, действия инсайдеров, возможность проникновения хакеров, а также простая халатность провайдера. Кроме того, дополнительно появляются угрозы, связанные с использованием виртуальной инфраструктуры — динамичность виртуальных машин, атаки на гипервизор, как на ключевой элемент системы виртуализации, атаки на системы управления».

Чаба Краснаи, ИТ-евангелист компании Balabit

Чаба Краснаи, ИТ-евангелист компании **Balabit**:

«Для многих компаний, в основном МСБ-сектора, «облако» более безопасно, чем их собственная инфраструктура. У облачных провайдеров есть необходимая экспертиза и рабочая сила для обеспечения безопасности. В крупных компаниях, это зависит от информации, которой нужно управлять. Организации движутся в сторону гибридных «облаков», некоторые бизнес-процессы используют публичные «облака», а остальные — остаются в рамках внутренней инфраструктуры. Для определения уровня безопасности облачных сервисов нужна оценка рисков. Многие решения помогают защитить гибридную инфраструктуру, например, PAM-инструменты, которые контролируют и отслеживают активность администраторов в сетевом окружении».

Владимир Фоменко, руководитель хостинг компании King Servers

Владимир Фоменко, руководитель хостинг-компании **King Servers**:

«От технических сбоев облачные сервисы защищены явно лучше за счет нескольких факторов:

- *Для хранения применяется специализированное «железо», вероятность выхода из строя которого значительно ниже, чем у обычной домашней техники.*
- *Оборудование таких сервисов расположено в специализированных ЦОД, где оно защищено от перепадов напряжения и перегрева.*
- *Естественно, что для хранения данных применяются технологии резервирования, которые сохранят данные в случае выхода из строя оборудования.*

С точки зрения информационной безопасности такие сервисы достаточно надежны, чтобы получить доступ к данным мог только авторизованный владелец аккаунта.

Уязвимым местом будет только недостаточная забота о безопасности со стороны самого пользователя вроде установки простого пароля или подключение к хранилищу с

недоверенных устройств. С точки зрения надежности самих сервисов – если пользователя интересует сохранность данных, то крайне рекомендую пользоваться крупными сервисами и не надеяться на стартапы, которые предоставляют больше места на бесплатных аккаунтах. Вполне возможно, что для небольших компаний предоставление таких сервисов окажется невыгодным, и они через некоторое время закроются, как это было с сервисами vSeife и Copy. В подобном случае можно не успеть скачать свои данные обратно, и они будут потеряны».

Артем Марусов, эксперт Центра информационной безопасности компании «Инфосистемы Джет»

Артем Марусов, эксперт Центра информационной безопасности компании **«Инфосистемы Джет»:**

«Насколько безопасны облачные сервисы? К сожалению, однозначного ответа на этот вопрос нет. И даже профессиональное сообщество не может прийти к единому мнению на этот счет. Достаточно полистать профильные сайты и форумы, чтобы понять, что по теме уже было высказано (и продолжает высказываться) множество амбивалентных мнений, причем достаточно неплохо аргументированных. Сторонники облачных сервисов считают, что поскольку такие услуги предоставляют, как правило, крупные корпорации с серьезными ИТ и ИБ компетенциями, то и безопасность обеспечивается ими если не наивысшем, то на достаточно адекватном уровне. Противники же «облаков» не перестают перечислять факты крупных утечек данных из облачных сервисов, напоминая, что, пользуясь ими, мы, по сути, отдаем свои данные в некий «черный ящик», аспекты реализации которого нам неизвестны и, соответственно, не могут быть оценены адекватно. Лично я считаю, что необходимо принять тот факт, что стопроцентной гарантии защищенности от утечек не может обеспечить никто. В связи с этим, надо просто принять за правило:

1) Никогда не выкладывать в облачные сервисы в открытом виде информацию, утечка которой нежелательна для вас (рабочие и финансовые документы, личные файлы).

2) Если такой необходимости не избежать, то обязательно шифровать файлы перед их отправкой в «облако». Для этого можно использовать средства как простые (например, создание архивов, защищенных паролем), так и более продвинутые (ПО для создания шифрованных разделов)».

Как пользователи могут обеспечить безопасность своей информации, находящейся в «облаке»?

Ашот Оганесян, технический директор и основатель DeviceLock

Ашот Оганесян, технический директор и основатель **DeviceLock**:

«В первую очередь необходимо использовать двухфакторную аутентификацию (2FA) для доступа к облачным сервисам. Настоятельно рекомендуется хранить файлы на таких сервисах в защищенных контейнерах (как минимум в запароленных архивах). Организациям, активно использующим облачные хранилища для хранения и обмена информацией, необходимо проводить регулярное сканирование своих данных, хранящихся в «облаке», с помощью продуктов класса Data Discovery, выявлять те данные, которые попали в облачные хранилища случайно или в нарушение политик компании».

Алексей Федоров:

«Если данные крайне ценны, лучше не надеяться на одно хранилище и отправлять их в еще одно хранилище. Следует помнить, что если на устройство установлено клиентское приложение облачного хранилища, при порче файлов на диске вирусом, испорченные файлы загрузятся и в хранилище, заменив собой неиспорченные. И даже если хранилище позволяет откатываться к предыдущим версиям, исправить порчу будет довольно проблематично: восстанавливать придется каждый файл отдельно, глубины хранимых версий может не хватить. Потому хотя бы в одно хранилище лучше заливать файлы через браузер, не устанавливая клиентское приложение. Разумеется, стоит придумать для своей учетной записи сложный пароль: 10 и больше символов, буквы в разном регистре, цифры и специальные символы. Хранить пароль в контейнере паролей или запомнить».

Денис Суховей, руководитель департамента развития технологий компании «Аладдин Р.Д.»

Денис Суховей, руководитель департамента развития технологий компании **«Аладдин Р.Д.»**:

«Сегодня пользователи имеют возможность задействовать внушительный арсенал организационных и технических мер по обеспечению защиты информации в «облаке». Однако такой подход сводит на нет все преимущества самого «облака», так как повышает совокупную стоимость использования сервиса. В этом свете криптографическая защита конфиденциальной информации в «облаке» является безальтернативным вариантом. Шифрование данных решает сразу целый букет «облачных» проблем безопасности, среди которых противодействие утечкам важной и критичной для бизнеса информации, разграничение прав доступа, соответствие целому набору требований регулирующих организаций и, конечно, экономическая эффективность и простота решения».

Максим Захаренко, генеральный директор компании «Облакотека»

Максим Захаренко, генеральный директор компании **«Облакотека»**:
«Возможно обеспечение практически абсолютной конфиденциальности, если данные в «облако» передаются и хранятся там в шифрованном виде, а расшифровка происходит только на своем железе. Другое дело, что это очень неудобно и фактически такое практикуется редко, особенно, если это касается частных пользователей. Как только расшифрованные данные размещены в «облаке», конечно, безопасность существенно уменьшается, но вопрос, насколько эта безопасность актуальна, например, для фотографий из отпуска или для небольшого ИП, которому нечего «прятать» даже от налоговой».

Таким образом, на фоне возрастающей роли облачных сервисов пользователям необходимо с большей ответственностью подходить к размещению своей информации в «облаке». Безусловно, нельзя исключать того, что вы можете столкнуться с халатностью провайдера, но нельзя забывать, что защищать свои данные должен и сам пользователь. Поэтому мы присоединяемся к словам экспертов и настоятельно рекомендуем задействовать механизм двухфакторной аутентификации, устанавливать надежные пароли и дифференцировать хранение информации (пользоваться несколькими разными хранилищами и обратить внимание на гибридные «облака»).