19 февраля 2025

Как шифрование, стандарты и блокчейн усилят защиту облаков

Риски утечки информации из облачных хранилищ имеются всегда. Этому есть ряд причин. Однако то, что информация в облаке находится под большей угрозой, эксперты назвали одним из мифов рынка. Обсуждаем с ними, какие меры защиты сегодня наиболее эффективны и каким образом их усилить, используя, в том числе многоуровневую систему безопасности, технические средства шифрования и технологию блокчейн.

Без абсолютной гарантии, но под защитой

Защита файлов в облаке мало чем отличается от защиты файлов в корпоративной сети, которая подключена к Интернет. Все зависит от того, какие защитные механизмы применяет облачный провайдер, работающий по модели SaaS, или пользователь облачного сервиса, который построен по модели IaaS или PaaS, пояснил бизнес—консультант по информационной безопасности Алексей Лукацкий.

«Как показывает анализ известных облачных инцидентов, утечки происходят, как правило, по причине забывчивости пользователей, которые некорректно

сконфигурировали имеющиеся в их распоряжении механизмы защиты. Иногда это происходит, например, как в кейсе с Microsoft Azure или Snowflake, из-за взлома самого провайдера, который некорректно работал с аутентификационной информацией, ключами и токенами», — рассказал Алексей Лукацкий.

Современные SaaS—решения для хранения файлов и документов используют многоуровневую защиту: данные распределены между российскими дата—центрами, файлы проверяются антивирусом, угрозы отслеживаются круглосуточно, при этом абсолютной гарантии безопасности нет нигде, но риски сведены к минимуму, предупредил директор по продукту VK WorkSpace Петр Щеглов.

«Ключевой фактор эффективности защиты — соблюдение цифровой гигиены пользователями. Для корпораций, которым важен полный контроль над своими файлами, доступна on-premise версия: данные хранятся на их серверах с дополнительными системами защиты от утечек», — посоветовал Петр Щеглов.

«Риски утечки информации есть всегда, поскольку не бывает полностью защищенных ресурсов в Интернете, однако провайдеры сейчас прикладывают немалые усилия для того, чтобы сомнения бизнеса в уровне безопасности облака ушли в прошлое, приводят свои решения в соответствие с требованиями российских и международных стандартов», — напомнил руководитель отдела информационной безопасности Linx Cloud Григорий Филатов.

«Для любого облачного провайдера защита информации своих заказчиков входит в число главных базовых приоритетов, поэтому для сохранения конфиденциальности данных, предотвращения утечек и сохранности данных всегда принимаются усиленные профессиональные меры касаемо как информации, которую пользователи размещают в облаке, так и данных о самих пользователях — метаинформации», — напомнил директор департамента «Облака и данные» Рексофт Руслан Заединов.

«Распространенное мнение, что информация в облаке находится под большей угрозой — один из мифов рынка. Это когнитивная ошибка. Зачастую меры, которые принимает среднестатистический заказчик для защиты данных в своем периметре бывают слабее, чем меры, которые принимает для решения тех же задач среднестатистический облачный провайдер. Миф о том, что данные в облаке могут быть защищены хуже, вызван особенностью работы нашего мозга. Мы считаем, что если держать данные при себе, то так безопаснее — своя рубашка ближе к телу. А если отдать их кому-то на хранение, то информация может быть скомпрометирована или испорчена. Это естественное мышление, сохранившееся с первобытных времен, когда все, что было за пределами своей пещеры находилось в опасности. На самом деле с технической точки зрения это не так и риски утечки данных из облака и из собственной инфраструктуры одинаковы», — пояснил Руслан Заединов.

«Современные облачные хранилища обеспечивают высокий уровень защиты данных благодаря комплексным решениям безопасности, и ее основой выступает шифрование AES-256, признанное самым надежным на сегодняшний день», — подчеркнул директор облачного бизнеса ITGLOBAL.COM, корпорация ITG Евгений Свидерский.

«Многоуровневая система безопасности включает также строгую аутентификацию пользователей, постоянный мониторинг активности и автоматическое выявление аномального поведения. Риски утечки информации существуют всегда, но их можно минимизировать при правильной настройке систем безопасности и регулярном проведении аудитов. В ITGLOBAL.COM мы используем специализированные решения для защиты от программ-вымогателей, такие как NetApp Ransomware Protection, что существенно снижает риски компрометации данных», — рассказал Евгений Свидерский.

Современные облачные провайдеры обеспечивают высокий уровень защиты для хранения стандартных бизнес—данных, согласился руководитель департамента информационных технологий MONS ГК «КОРУС Консалтинг» Антон Егоров.

Антон Егоров
Руководитель департамента информационных технологий MONS ГК «КОРУС Консалтинг»

Если речь идет о критически важной информации, то риск утечки возрастает, поскольку ценность таких данных повышает вероятность целенаправленных атак. В обычных условиях облачные решения достаточно надежны для хранения типовой корпоративной информации, но специализированные данные, обладающие повышенной важностью, лучше хранить в изолированных, защищенных облачных сегментах — ресурсах с усиленными мерами информационной безопасности.

Степень защиты зависит от конкретного поставщика услуг, провайдеры предлагают разный уровень защищенности файлов в хранилищах, но большинство из них обеспечивает должную безопасность, особенно для сегмента B2C, убежден директор по информационной безопасности Т1 Интеграция и Т1 Облако Алексей Кубарев. Для B2B эксперт рекомендовал использовать специальные файлообменники, которые предлагают дополнительные меры по обеспечению информационной безопасности.

Чем больше атак, тем крепче защита

Сегодня сегмент Интернета подвергается намного большему количеству атак, чем три года назад, и атаки стали более таргетированными: они направлены на компрометацию объектов критической информационной инфраструктуры и других важных ресурсов, отметил Григорий Филатов.

«Такая ситуация стимулирует государство усиливать требования к применению отечественных средств защиты. В России активно разрабатываются аналоги решений для информационной безопасности, которые приобретались за рубежом. Инновационные отечественные средства защиты еще не появились, однако некоторые "фичи" российских

продуктов получили большое распространение, например такие, как блокировка по geo-ip», — рассказал Григорий Филатов.

«Общедоступные сервисы файлового обмена в корпорациях и крупных компаниях запрещены политиками информационной безопасности и не применяются для обмена чувствительными данными, поэтому такие сервисы не являются приоритетными для злоумышленников», — подчеркнул Алексей Кубарев.

«Однако важно принять меры по недопущению размещения чувствительной информации в этих сервисах. Если размещение такой информации все же необходимо, целесообразно использовать дополнительные настройки безопасности таких сервисов, предоставляемые провайдерами. К ним относятся шифрование загружаемых файлов, ограничение доступа по белому списку пользователей, а также обеспечение доступа к файлам по паролю», — посоветовал Алексей Кубарев.

«Стоит начать использовать хотя бы те механизмы, которые у нас имеются в распоряжении и не зависят от геополитики: установку прав доступа, многофакторную аутентификацию, управление криптографическими ключами, шифрование данных, мониторинг виртуальных потоков, межсетевое экранирование, регистрацию событий безопасности», — порекомендовал Алексей Лукацкий.

«Главное, чтобы такие механизмы предлагались облачными провайдерами. Пока, к сожалению, надо признать, что не все российские поставщики облачных услуг могут похвастать продвинутой системой информационной

безопасности: они находятся только в самом начале своего пути», — отметил бизнес-консультант.

Антон Егоров
Руководитель департамента информационных технологий MONS ГК «КОРУС Консалтинг»

Геополитическая обстановка и увеличение числа атак способствуют росту рисков, поэтому многие крупные облачные провайдеры давно внедрили дополнительные меры безопасности и используют дополнительные файерволы, применяют усовершенствованные схемы шифрования и ключи безопасности, проводят проверки точек подключения и валидацию пользователей с цифровыми отпечатками (совокупность параметров, которая позволяет идентифицировать устройство — прим. авт.), имеют возможность переводить критичные данные в отдельные защищенные сегменты с использованием стандартов, например, УЗ-1 – максимальным стандартом безопасности.

По словам эксперта, георазпределенность дата—центров обеспечивает доступ к информации даже в случае отключения одного из центров. Если у заказчика имеются критически важные данные, стоит обсудить с провайдером возможность использования специализированного защищенного пространства.

Антон Егоров
Руководитель департамента информационных технологий MONS ГК «КОРУС Консалтинг»

Таким образом, для стандартных бизнес-структур облачные решения сегодня предлагают надежную защиту, а для особо критичных данных существуют дополнительные опции, позволяющие значительно снизить риски утечек.

«Локализация данных в России — новый стандарт», — напомнил Петр Щеглов. Он добавил, что **использование зарубежных хранилищ несет риски блокировки аккаунтов** на основании регистрационных данных, источников платежей и даже ip-адресов, с которых в сервис приходят запросы на подключение.

«К примеру, диск VK WorkSpace не использует дата—центры в иностранных юрисдикциях. Мы помогаем перенести данные из зарубежных сервисов без потери структуры хранения файлов и метаданных, а регулярные учения (имитации атак, сбоев, аварий) обеспечивают нашу готовность к любым нештатным ситуациям», — отметил эксперт.

«В текущих условиях действительно требуется усиление мер защиты, и мы рекомендуем комплексный подход, включающий несколько ключевых направлений», — сказал Евгений Свидерский.

«Во—первых, необходимо внедрение систем Security Operation Center (SOC) для непрерывного мониторинга безопасности. Во—вторых, усиление контроля доступа через многофакторную аутентификацию и детальный анализ активности пользователей. Особое внимание следует уделить защите от целенаправленных атак. Здесь эффективно работает сочетание превентивных мер и систем быстрого реагирования на инциденты. Шифрование данных должно применяться на всех уровнях — от инфраструктуры до приложений. Также критически важно регулярно обновлять системы безопасности и проводить тестирование на проникновение для выявления потенциальных уязвимостей», — рекомендовал Евгений Свидерский.

«Усиление и новые методы защиты облачных систем нужны вне зависимости от изменений в геополитике — это базовая необходимость», — подчеркнул Руслан Заединов. Он пояснил, что и **корпоративные, и частные пользователи хранят информацию в облаке в том виде, в котором ее удобно использовать**: документ хранится в виде документа, фотография или скан — в виде графического файла, запись совещания — в виде аудио- или видеофайла, с которыми комфортно работать. **Риски утечки информации из облака такие же или даже меньше, чем из собственного периметра компании.** Однако они есть, поэтому важно обеспечить невозможность понимания и использования злоумышленниками скомпрометированных данных.

«Необходимо внедрять технические средства шифрования и обфускации (шифрования не только содержимого, но и самой структуры данных — прим. авт.), которые работают в середине цепочки между пользователем и облачным провайдером. Их задача — преобразовать информацию при передаче от пользователя в облако, чтобы даже провайдеру не было известно, что именно он хранит. При этом для конечного пользователя информация по-прежнему должна отображаться в удобном для потребления виде — картинки, документы, аудиозаписи. Некоторые облачные провайдеры предлагают частичное шифрование, при котором одна часть хранилища зашифрована, а другая нет. Это полумеры, которые могут оказаться неэффективны, поскольку ключи шифрования в данном случае хранятся на стороне облачного провайдера. Если само хранилище провайдера будет скомпрометировано, и злоумышленник получит доступ к ключам, то он сможет расшифровать все данные. Поэтому шифрование и обфускация данных должны происходить на стороне пользователя. В таком случае и для провайдера, и для возможных злоумышленников информация будет

выглядеть как случайные биты и байты», — убежден Руслан Заединов.

«Внедрение таких технологий — очевидный важный шаг, и уже есть понимание, как реализовывать подобные средства для индивидуального пользования», — добавил эксперт. Он предположил, что с внедрением подхода на уровне компании могут возникнуть некоторые технические сложности, поскольку корпоративным пользователям нужно не просто хранить данные, а обмениваться и совместно пользоваться одними и теми же файлами и базами данных. Однако эти трудности преодолимы на современном уровне развития технологий, и с этим однозначно стоит работать, резюмировал Руслан Заединов.

Блокчейн как посредник

Ученые Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» предложили усилить защиту файлов в облаке с помощью технологии блокчейн, который будет выступать в роли посредника между облачным сервисом и самим сервером.

«Блокчейн как посредник мог бы предоставить более надежный механизм хранения и удаления файлов. С помощью данной технологии, с одной стороны, можно обеспечить более высокую степень шифрования хранимых данных. С другой, цепочки блокчейн позволят хранить историю операций с

файлами. Поэтому, если облачный сервер попытается что-то сделать с файлом без разрешения, то это пользователю станет известно, и он может предотвратить утечку данных, например, введя новый механизм шифрования. Таким образом, пользователи сервиса получают более управляемую с их стороны систему хранения файлов и удаления по их запросу. При этом, облачный сервер по—прежнему предоставляет инфраструктуру не только для хранения самих файлов, но и для исполнения блокчейн—цепочек. В итоге, выигрывают обе стороны», — пояснил доцент кафедры систем автоматизированного проектирования СПбГЭТУ «ЛЭТИ» Сергей Кузьмин.

Он добавил, что блокчейн станет серьезной преградой для злоумышленников, которым удается достаточно регулярно получать информацию с облачных хран