

pressrelease

Совместное исследование Gemalto и центра Ponemon Institute. Между странами возникают существенные различия в отношении защиты данных в облаке

- В ходе исследования были обнаружены региональные различия мер по обеспечению информационной безопасности облака. Немецкие компании почти в два раза чаще обеспечивают безопасность конфиденциальной или секретной информации в облаке (61 %), чем британские (35 %), бразильские (34 %) и японские (31 %).
- Половина международных организаций считают, что в облаке платежная информация (54 %) и данные клиентов (49 %) подвергаются опасности.
- Более половины (57 %) компаний считают, что использование облачных сервисов повышает риск нарушения законодательства.

Амстердам, 16 января 2018 г. – Gemalto, мировой лидер в области цифровой безопасности, на данный момент может сообщить, что несмотря на то, что большинство глобальных компаний (95 %) используют облачные сервисы¹, уровень мер обеспечения безопасности в компаниях довольно сильно отличается в зависимости от рынка. Организации признают, что в среднем всего лишь две пятых (40 %) данных, которые хранятся в облаке, защищены с помощью решений по шифрованию и управлению ключами.

Данные, полученные в результате исследования «[2018 Global Cloud Data Security Study](#)» (Глобальное исследование безопасности облачных данных 2018 г.), проведенного исследовательским центром Ponemon Institute для компании Gemalto, свидетельствуют о том, что организации в Великобритании (35 %), Бразилии (34 %) и Японии (31 %) менее предусмотрительны, чем в Германии (61 %), в том, что касается обмена с третьими лицами секретной и конфиденциальной информацией, хранящейся в облаке. Чтобы лучше понять ключевые тенденции в управлении данными и мерах безопасности при использовании облачных сервисов, в ходе исследования были опрошены 3200 специалистов в области информационных технологий и ИТ-безопасности со всего мира.



Ведущая позиция Германии в области [информационной безопасности в облаке](#) распространяется и на внедрение контрольных мер, таких как шифрование и токенизация.

¹ <https://www.rightscale.com/lp/2017-state-of-the-cloud-report?campaign=7017000000vFyc>

Большинство (61 %) немецких организаций сообщили, что они защищают секретную и конфиденциальную информацию, хранящуюся в облачной среде, что превышает показатели США (51 %) и Японии (50 %). Уровень предпринимаемых мер по обеспечению безопасности возрастает при отправке и получении данных компаниями. В Германии их используют 67 % компаний, в Японии — 62 %, а в Индии — 61 %.

Следует отметить, что более трех четвертей (77 %) организаций по всему миру признают, насколько важно иметь возможность внедрять криптологические решения, например, шифрование. Недавно количество таких компаний возросло. Девять из десяти (91 %) организаций считают, что в течение следующих двух лет значение этой возможности возрастет. В прошлом году их количество составляло 86 %.

Управление конфиденциальностью и контроль в облаке

Несмотря на все более активное использование облачной обработки данных и преимущества, которые оно приносит, создается впечатление, что глобальные организации до сих пор относятся к ней с опаской. Половина из них сообщают, что платежная информация (54 %) и данные клиентов (49 %) в облаке подвергаются опасности. Более половины (57 %) глобальных организаций также считают, что в результате использования облака они могут с большей вероятностью столкнуться с нарушением законов о конфиденциальности и защите данных, но это число немного сократилось с 2016 года (с 62 %).

Ввиду такого предполагаемого риска почти все (88 %) компании считают, что новый Генеральный регламент о защите персональных данных (GDPR) потребует изменений в управлении облачными сервисами, а две пятых (37 %) утверждают, что это повлечет значительные перемены. Кроме трудностей в соблюдении требований законодательства, три четверти опрошенных (75 %) также сообщили, что в облачной среде намного сложнее соблюдать положения о конфиденциальности и защите данных, чем в локальных сетях, в частности наиболее сложным его считают компании из Франции (97 %) и США (87 %), от них немного отстает Индия (83 %).

Витая в облаках

Несмотря на широкое распространение облачных сервисов, в ходе исследования было выявлено, что многие компании незнакомы с используемыми решениями. Только четверть (25 %) специалистов по информационным технологиям и ИТ-безопасности сообщили, что они уверены, что знают все облачные сервисы, используемые в их компании, а треть (31 %) уверены, что разбираются в них.

Если рассмотреть этот вопрос более подробно, теневые ИТ продолжают создавать трудности. Более половины организаций в Австралии (61 %), Бразилии (59 %) и Великобритании (56 %) не уверены, что они знают все приложения, платформы и инфраструктурные службы для облачной обработки данных, используемые в их организациях. В других странах уровень уверенности выше, например, всего четверть компаний в Германии (27 %), Японии (27 %) и Франции (25 %) не уверены в своих знаниях.

К счастью, большинство (81 %) считает, что критично или, по крайней мере, очень важно иметь возможность использовать методы двухфакторной аутентификации для доступа к данным и

приложениям в облаке. Компании в Австралии активнее всех внедряют методы аутентификации. 92 % компаний согласны, что это поможет гарантировать, что доступ к определенным данным и приложениям получают только те, кто имеет на это право, обогнав Индию (85 %) и Японию (84 %).

«С одной стороны, отлично, что некоторые страны, например, Германия, серьезно относятся к вопросам информационной безопасности в облаке. С другой стороны, показатели остальных странах заставляют волноваться, — говорит Джейсон Харт (Jason Hart), генеральный технический директор по защите данных Gemalto. — Меньше половины считают, что облако усложняет защиту данных, когда все с точностью наоборот.

Преимущество облака заключается в его удобстве, масштабируемости и контроле издержек, что позволяет обеспечить различные варианты защиты для компаний, которые не смогут самостоятельно обеспечить или позволить себе такие возможности, в частности, в отношении безопасности. Однако, несмотря на то, что защитить данные в облаке проще, нужно искоренять убеждение, что использование облака автоматически обеспечивает безопасность информации. В качестве примеров уязвимости в защите данных посмотрите на недавние взломы Accenture и Uber. Независимо от того, где находятся данные, источник данных должен использовать соответствующие контрольные меры, например, шифрование или токенизацию. Как только они будут введены, все вопросы с соблюдением законодательства будут решены».

Методика исследования

Gemalto поручила провести исследование компании [Ponemon Institute](#), в рамках которого опросили 3285 специалистов в области информационной технологии и ИТ-безопасности из таких стран, как США (575), Великобритания (405), Австралия (244), Германия (492), Франция (293), Япония (424), Индия (497) и Бразилия (355).

Источники

- Получить более подробную информацию о региональных различиях или загрузить отчет можно на [сайте исследования «2018 Global Cloud Data Security Study»](#)
- Примите участие в *вебинаре* Gemalto и Ponemon Institute «Top Trends in Cloud Security», посвященном ведущим тенденциям безопасности облачных сервисов, который *пройдет 27 февраля — щелкните здесь, чтобы зарегистрироваться*
- Более подробная информация о [решениях Gemalto в сфере защиты облачных данных](#)
- Дополнительная информация об исследованиях Gemalto в сфере безопасности данных.

О компании Gemalto

Gemalto (Euronext NL0000400653 GTO)

3,1

180

2016

Gemalto

15 000.
, 30 - 112 , 43
48

[@gemalto](https://twitter.com/gemalto) Twitter.

www.gemalto.com

Контактная информация Gemalto для прессы:

(Tauri Cox)

(Sophie Dombres)

(Jaslin Huang)

+1 512 257 3916

tauri.cox@gemalto.com

+33 4 42 55 36 57 38

sophie.dombres@gemalto.com

+65 6317 3005

jaslin.huang@gemalto.com

(Enriqueta
Sedano)

+52 5521221422

enriqueta.sedano@gemalto.com

Текст данного коммюнике, являющийся переводом, ни в коем случае не должен считаться официальной версией. Единственная версия коммюнике, которая имеет силу, это коммюнике на языке оригинала, то есть на английском языке, она будет превалировать в случае несоответствия перевода оригиналу.