

#### **Аннотация**

В данной статье рассматриваются облачные технологии в целом, приводятся основные угрозы безопасности и предлагаются мероприятия по минимизации этих угроз. Также рассматривается российский рынок облачных технологий и его проблемы.

**Ключевые слова:** облако; облачные технологии; угрозы; безопасность.

#### **Облачные технологии и их главные угрозы**

Облачные технологии (вычисления) – это технологии распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис. Центры обработки данных - это помещение, которое предоставляет услуги, необходимые для размещения наиболее крупных на данный момент вычислительных сред.

Из-за большого количества данных, которые сегодня часто переносятся в облака, площадки облачных хостинг-провайдеров становятся привлекательной целью для злоумышленников. Ниже представлены угрозы облачной безопасности по версии Cloud Security Alliance.

Угроза 1: утечка данных. Чтобы минимизировать эту угрозу, рекомендуется использовать многофакторную аутентификацию и шифрование.

Угроза 2: компрометация учетных записей и обход аутентификации. Решение: использование механизмов многофакторной аутентификации, в том числе одноразовые пароли, USB-ключи.

Угроза 3: взлом интерфейсов и API. Решение: использовать инструменты защиты и раннего обнаружения угроз, периодически запускать тесты на проникновение.

Угроза 4: уязвимость используемых систем. Решение: проводить регулярное сканирование на выявление уязвимостей, применять последние патчи и быстро реагировать на сообщения об угрозах безопасности.

Угроза 5: кража учетных записей. Решение: запретить передачу учетных записей пользователей и служб между собой, обратить внимание на многофакторную аутентификацию.

Угроза 6: инсайдеры-злоумышленники. Решение: использовать механизмы шифрования и взять под собственный контроль управление ключами шифрования.

Угроза 7: целевые кибератаки. Решение: проводить специализированное обучение сотрудников по распознаванию техник злоумышленника, применять профилактические методы, повышающие уровень безопасности инфраструктуры.

Угроза 8: перманентная потеря данных. Решение: отделять пользовательские данные от данных приложений, сохраняя их в различных локациях.

Угроза 9: недостаточная осведомленность. Необходимо понимать функционирование облачных сервисов, предоставляемых поставщиком услуг.

Угроза 10: злоупотребление облачными сервисами. Поставщикам услуг важно уметь распознавать таких участников, для чего рекомендуется детально изучать трафик и использовать инструменты мониторинга облачных сред.

Угроза 11: DDoS-атаки. Необходимо иметь план смягчения атаки до ее свершения.

Угроза 12: совместные технологии, общие риски. Решение: использовать стратегию «безопасности в глубину».

#### **Облачные технологии в России**

Несмотря на все больший рост популярности облачных вычислений, большинство российских компаний не готово к использованию облачных сервисов.

Как показал опрос TAdviser, препятствием к использованию облачных решений для 67% опрошенных остаются риски утечки или потери данных. Для 40% сдерживающий фактор - высокая стоимость услуги из-за не всегда корректной оценки миграции в облако. Еще 38%

респондентов ссылаются на ограничения или требования регулятора, не позволяющие активнее мигрировать в облака. Также к этому списку можно добавить два фактора: ненадежность и скептичность. В первом случае руководство компаний считает, что надежнее иметь свой физически осязаемый сервер в офисе. Во втором – часто явные преимущества новых технологий не могут перевесить предвзятое отношение и неготовность служб информационной безопасности следовать технологическим веяниям.

Стимулировать компании на переход на облачные технологии может фактор сокращения издержек, что отметили более 60% опрошенных. Несмотря на все опасения в связи с рисками потери данных, уже 57% опрошенных видят в облаках гарантию безопасности, обеспечиваемую на стороне провайдера. В первую очередь это представители интернет-ритейла, интернет-сервисов.

### **Заключение**

В погоне за сокращением эксплуатационных расходов многие компании мигрировали или планируют мигрировать на облачные технологии, несмотря на довольно большие риски в области безопасности.

Совместная работа провайдера и компании, пользующейся его услугами, поможет существенно сократить риски потери данных путем своевременного обнаружения и устранения угроз безопасности. Делая такой смелый шаг, руководству компании необходимо вкладывать больше средств и уделять больше внимания информационной безопасности.

### **Список литературы**

1. CISCO IoT course chapter 2 [Электронный ресурс] URL: <https://static-courseassets.s3.amazonaws.com/I2IoT20/en/index.html#2.1.1.6>
2. CSA Summit at RSA Conference 2017 [Электронный ресурс]. URL: <https://csacongress.org/event/rsa-summit-2017/>
3. Интерес к DevOps и аналитике больших данных преопределил высокие темпы роста рынка облачных услуг [Электронный ресурс] URL: <https://idcrussia.com/ru/about-idc/press-center/66013-idc-devops>
4. Ключевые игроки рынка облачных сервисов в России [Электронный ресурс] URL: <http://www.tadviser.ru/index.php>
5. Тенденции развития облачных технологий на российском рынке [Электронный ресурс] URL: <https://cyberleninka.ru/article/v/tendentsii-razvitiya-oblachnyh-tehnologiy-na-rossiyskom-rynke>