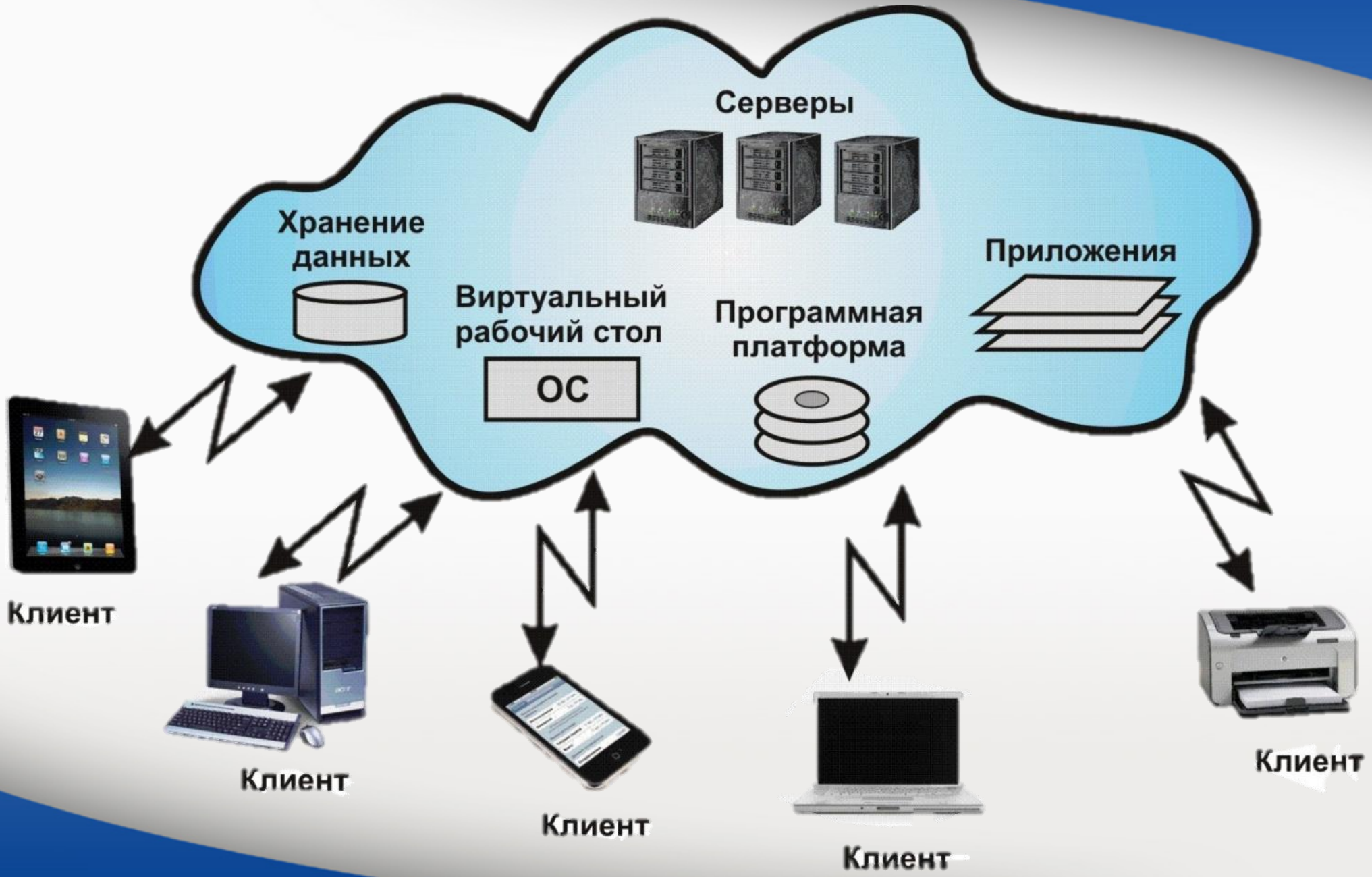
Средства защиты данных в облачных системах

Облачные системы

Это технологии обработки данных, в которых компьютерные ресурсы предоставляются Интернет - пользователю как онлайн - сервис. Слово « облако » здесь присутствует как метафора, олицетворяющая сложную инфраструктуру, скрывающую за собой все технические детали.


Серверы
Хранение данных
Виртуальный рабочий стол
ОС
Программная платформа
Приложения
Клиент
Клиент
Клиент
Клиент
Клиент

Облачные вычисления

Это вычислительная модель, обеспечивающая быстрый, простой и удобный сетевой доступ к пулу вычислительных ресурсов (сеть, сервера, диски, приложения и сервисы) по требованию, причем такой доступ требует минимального привлечения администраторов или сервис провайдеров.

Одним из основных достоинств "Облачных технологий" является безопасность ("облачные" сервисы имеют высокую безопасность при должном ее обеспечении, однако при халатном отношении эффект может быть полностью противоположным).

На сегодняшний день наиболее популярны пять метода защиты информации в "Облачных технологиях":

1) Шифрование;
2) Защита данных при передаче;
3) Аутентификация;
4) Изоляция пользователей;
5) Резервирование.

Сохранность данных. Шифрование.

Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в ЦОД (Центр обработки данных – совокупность серверов, размещенных на одной площадке с целью повышения эффективности и защищенности), а также в случае отсутствия необходимости, безвозвратно удалять.

При шифровании данных всегда возникает вопрос о ключах. Их хранение на облачном сервере нецелесообразно, поскольку каждый, кто имеет доступ к облачным серверам или шаблонам, мог бы получить доступ к ключу, а значит, и к расшифрованным данным. Набор пароля при запуске системы, как это принято в локальных решениях для шифрования данных, затруднен в связи с отсутствием настоящей консоли, однако идея неплоха. Физический ввод ключа заменяется запросом, который облачный сервер отправляет внешнему источнику — серверу управления ключами (Key Management Server, KMS).

Решающим фактором для обеспечения безопасности такого решения является раздельная эксплуатация облачного сервера и сервера управления ключами (см. Рисунок 1): если оба размещены у (одного и того же) провайдера облачных сервисов, то вся информация снова оказывается собранной в одном месте. Хорошей альтернативой является установка сервера KMS в локальном ЦОД или в качестве внешней услуги у другого сервис-провайдера.

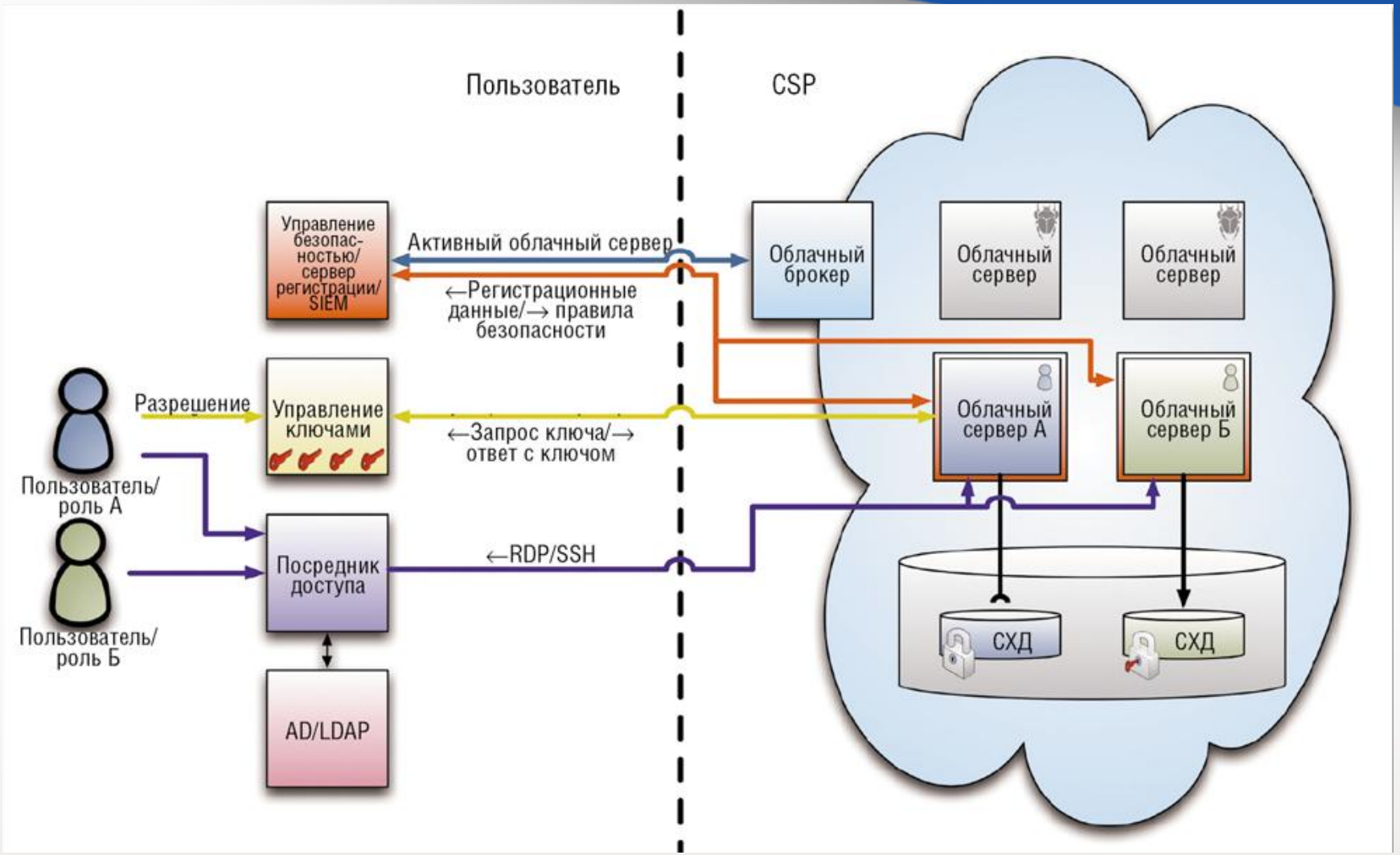


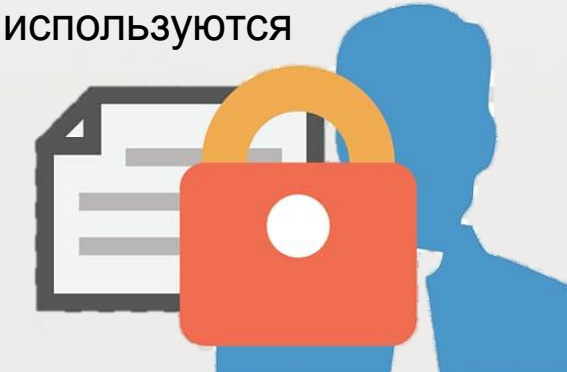
Рис. 1.
Схема взаимодействия пользователя, сервера управления ключами и облачного сервера

Защита данных при передаче.

Для безопасной обработки данных обязательным условием является их шифруемая передача. В целях защиты данных в публичном облаке используется туннель виртуальной частной сети (VPN), связывающей клиента и сервер для получения публичных облачных услуг. VPN-туннель способствует безопасным соединениям и позволяет использовать единое имя и пароль для доступа к разным облачным ресурсам. В качестве средства передачи данных в публичных облаках VPN - соединение использует общедоступные ресурсы, такие как Интернет. Процесс основан на режимах доступа с шифрованием при помощи двух ключей на базе протокола Secure Sockets Layer (SSL).

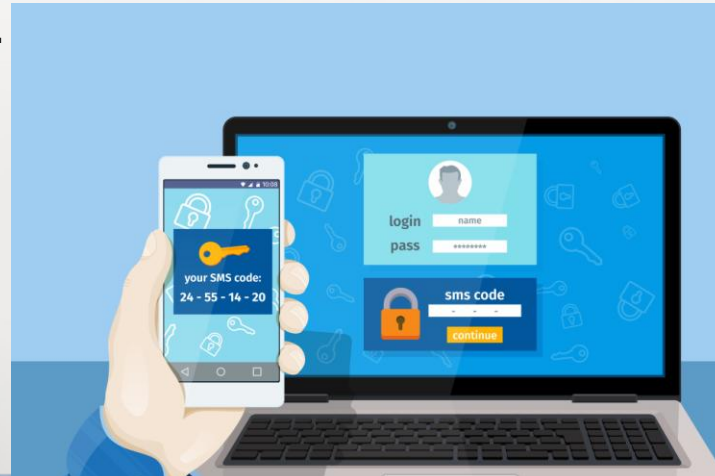
Большинство протоколов SSL и VPN в качестве опции поддерживают использование цифровых сертификатов для аутентификации, посредством которых проверяется идентификационная информация другой стороны, причем еще до начала передачи данных. Такие цифровые сертификаты могут храниться на виртуальных жестких дисках в зашифрованном виде, и используются они только после того, как сервер управления ключами проверит идентификационную информацию и целостность системы. Следовательно, такая цепочка взаимозависимостей позволит передавать данные только тем облачным серверам, которые прошли предварительную проверку.

Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения в них, даже в случае доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами.



Аутентификация

Аутентификация — защита паролем. Для обеспечения более высокой надежности, часто прибегают к таким средствам, как токены (электронный ключ для доступа к чему-либо) и сертификаты. Наиболее простой и достаточно надежный метод аутентификации — это технология одноразовых паролей (One Time password, OTP). Такие пароли могут генерироваться либо специальными программами, либо дополнительными устройствами, либо сервисами, с пересылкой пользователю по SMS. Основное отличие облачной инфраструктуры заключается в большой масштабируемости и более широкой географической распределенности. На первый план выходит использование для получения одноразовых паролей мобильных гаджетов, которые сегодня есть практически у каждого. В самом простом случае одноразовый пароль будет сгенерирован специальным сервером аутентификации и выслан в SMS на мобильный телефон пользователя после ввода правильного статического пароля на страницу доступа к облачному сервису. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать протокол LDAP (Lightweight Directory Access Protocol) и язык программирования SAML (Security Assertion Markup Language).



Изоляция пользователей

Использование индивидуальной виртуальной машины и виртуальной сети.

Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счет изменения кода в единой программной среде. Этот подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющем получить доступ к данным. В случае возможной ошибки в коде пользователь может получить доступ к информации другого пользователя. В последнее время такие инциденты часто имели место.

Резервное копирование данных

Приложения, которые работают в облаке, защищены только в определенной степени. Периодически появляются истории, как тот или иной ненадежный облачный провайдер стер виртуальные машины или файлы в хранилище. Для полной защиты данных, которые генерируются облачными приложениями, потребуется резервное копирование в дата-центр (ЦОД) заказчика или в другое облако.

В сценариях с малым масштабом пользователи могут копировать файлы, например, из Office 365 на локальный том или на внешний диск. Но это ручной процесс, который может быть ненадежным и его сложно масштабировать.

Для больших файлов и более крупных приложений такие сценарии очень редки. Предприятия, использующие облако по модели IaaS, могут пользоваться интерфейсами прикладных систем (API), которые предоставляют облачные провайдеры, для разработки собственного программного обеспечения для резервного копирования, или сторонним программным обеспечением для резервного копирования на локальные серверы, в сетевое хранилище (NAS) или в свой ЦОД.

Резервное копирование из облака в облако обещает дать бизнесу несколько преимуществ по сравнению с локальными резервными копиями, включая более низкие затраты на инфраструктуру, более быстрое резервное копирование и восстановление, а также большую гибкость.

В рамках услуги облачного резервного копирования пользователи получают возможность резервирования важных данных (файлов, баз, конфигураций операционных систем) в облако. Для этого они устанавливают специальные агенты для резервирования данных требуемых приложений. Наличие агентов позволяет гарантировать целостность данных в резервной копии, а сама передача резервируемых данных осуществляется через интернет по VPN-каналам.

Спасибо за внимание