Безопасный ЦОД. Свой/чужой или общий?

Андрей ШПАКОВ,
ведущий инженер,
ООО «С-Терра СиЭсПи»

Для того чтобы в ЦОДах можно было обрабатывать и хранить конфиденциальную информацию с соблюдением требований законодательства и обеспечением необходимой защиты, в них должны применяться сертифицированные отечественные продукты. Такие, как предлагает, в частности, компания «С-Терра СиЭсПи».

Деятельность крупных компаний сегодня уже невозможно представить без задействования собственных или сторонних центров обработки данных. Постепенно и менее крупные заказчики стали доверять свои данные сторонним организациям. Каковы же основные критерии доверия к ЦОДу в России и за ее пределами? Во-первых, это имя центра обработки данных. Во-вторых – пул крупных заказчиков с успешным бизнесом, которые пользуются услугами данного сервис-провайдера. Эти два фактора формируют репутацию поставщика услуг ЦОДа. Часто учитывается еще один параметр – наличие общепризнанных сертификатов ЦОДа. В этих случаях почти всегда подразумевается сертификация Tier I–IV от Uptime Institute. Сертификат Tier III (доступность 99,982%) от данной организации стал практически обязательным атрибутом серьезного сервис-провайдера, претендующего на внимание крупных заказчиков. В настоящее время Uptime Institute предлагает сертификацию дизайн-проекта центра обработки данных, сертификацию построенной площадки и сертификацию процессов эксплуатации ЦОДа. При этом все проверки, необходимые для выдачи сертификатов, проводятся только силами сотрудников компании Uptime Institute.

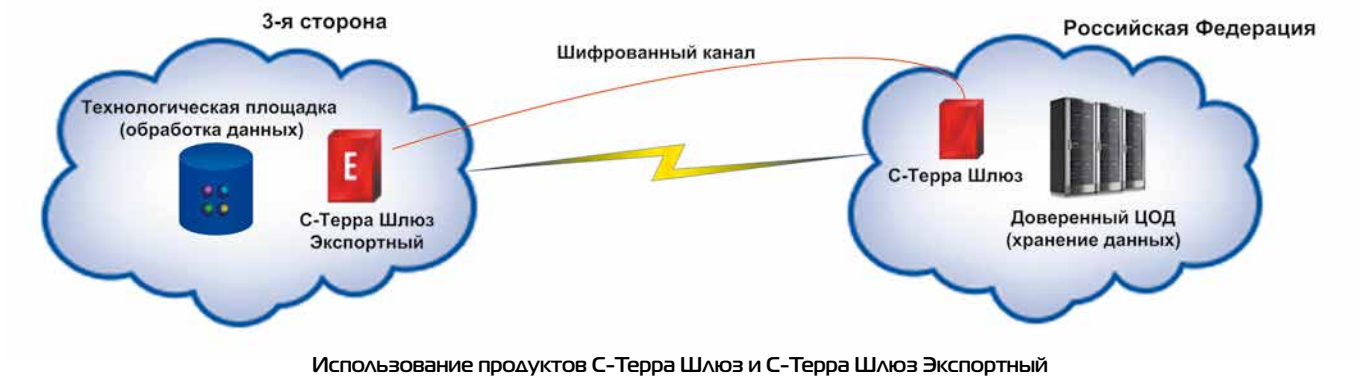
Детальная проверка проекта, его реализации и дальнейшей эксплуатации объекта – действительно эффективная мера для создания отказоустойчивого ЦОДа. Однако нужно отметить, что вся критически важная информация об устройстве такой площадки хранится в базе данных частной компании (Uptime Institute), имеющей штаб-квартиру в Нью-Йорке. А, как показало «дело Сноудена», термин «приватность» сегодня потерял свое былое значение. Кроме того, существуют угрозы нарушения целостности информации и ее перехвата при передаче. Соответственно, одной сертификации ЦОДа недостаточно. Вне зависимости от его местоположения необходимо применять и другие механизмы обеспечения безопасности. Из числа технических решений таковыми являются средства криптографической защиты информации при доступе, хранении и передаче.

Безопасный высокопроизводительный доступ

Уже сейчас некоторые провайдеры предлагают своим клиентам услугу защищенного доступа к данным. Обычно для этого используются западные VPN-продукты в виде виртуальных машин. Это дает провайдерам возможность экономить пул IP-адресов, оперативно предоставлять VPN-сервис клиентам и гибко распределять ресурсы. Причем в плане лицензирования провайдеры могут прибегнуть к арендной модели – платить производителю только за то ПО, которым воспользовался клиент. Однако такой подход не позволяет выполнить требования российского законодательства (например, по защите персональных данных), так как западные средства защиты не сертифицированы отечественным регулятором в области криптографии – ФСБ России. Для организации легитимной защиты необходимо применение сертифицированных отечественных продуктов. Такие продукты существуют в виде виртуальных машин с поддержкой всех актуальных гипервизоров. Ярким примером является С-Терра Виртуальный Шлюз. Его уже используют крупнейшие провайдеры нашей страны для предоставления своим клиентам доступа к облачным сервисам. Продукт сертифицирован ФСБ России по классам КС1 и МЭ4, а также ФСТЭК России по классу МЭ3.

На государственном уровне проблема сохранения конфиденциальности данных, находящихся за рубежом, уже решается в рамках мер по обеспечению информационной безопасности страны. В частности, принят Федеральный закон от 21.07.2014 № 242-ФЗ, который вступает в силу с 1 сентября 2015 г. и обязывает хранить персональные данные граждан РФ на территории России. Закон вполне логичен – ведь из-за внешних факторов (вспомним западные санкции) может быть нарушена работа ИТ-систем крупнейших компаний – резидентов РФ, а это сильнейший удар по клиентам и бизнесу в целом. Вместе с тем необходимость соответствовать требованиям закона ставит две новые задачи – для переноса данных нужно подобрать подходящий ЦОД на территории России и обеспечить защиту данных при их миграции. Решение второй задачи найдено компанией «С-Терра СиЭсПи» несколько лет назад, и его надежность и эффективность уже доказаны практикой.

Многие компании предпочитают хранить данные в России, а обрабатывать по-прежнему за ее пределами.



Использование продуктов С-Терра Шлюз и С-Терра Шлюз Экспортный

В этом случае для выполнения требований законодательства канал связи между объектами необходимо защитить. А это означает использование сертифицированных VPN-решений с шифрованием по криптоалгоритмам, соответствующим российским ГОСТам и разрешенным к вывозу за рубеж. Именно такой продукт есть в линейке компании «С-Терра СиЭсПи» – это С-Терра Шлюз Экспортный. Данный программно-аппаратный комплекс представляет собой экспортный вариант продукта С-Терра Шлюз, допускающий его использование как на территории РФ, так и за ее пределами. Он применим как в рамках концепции «хранение в РФ, обработка за границей», так и для защиты данных во время их миграции из заграничного хранилища в ЦОД, расположенный на территории нашей страны (см. рисунок). Продукт сертифицирован ФСБ России по классу КС1.

Сочетание производительного VPN-оборудования для защиты высокоскоростных каналов связи с низкой задержкой и кадров большого размера (Jumbo Frame) позволяет передавать данные на впечатляющей скорости до 7,5 Гбит/с. Следует отметить, что организации, обрабатывающей данные на технологической площадке, не обязательно создавать полноценную инфраструктуру для пользования VPN-шлюзом. Если площадка представляет собой несколько ноутбуков или серверов, достаточно установить программный комплекс С-Терра Клиент (также в экспортном исполнении) либо С-Терра Виртуальный Шлюз.

Шлюзы безопасности С-Терра способны защитить не только стандартный трафик, но и взаимодействие с системами хранения данных по протоколу iSCSI. При использовании технологии Jumbo Frame с одной пары шлюзов можно передать до 1500 Гбайт/ч. Среда передачи данных не обязательно должна быть ограничена Ethernet, это может быть и Fibre Channel (FCIP). Все вышеупомянутые сценарии могут быть реализованы не только на физическом оборудовании, но и в виртуальной среде, что позволяет встраивать средства криптографической защиты информации напрямую в инфраструктуру ЦОДа. На внутренних испытаниях с одного ядра процессора Intel Xeon E5-2643v3 при использовании гипервизора VMware ESXi 5.5 с технологией SR-IOV производительность решения достигала 300 Мбит/с. Если же заказчику потребуется перенести большой объем данных в короткие сроки, группы шлюзов можно развернуть в целые криптофермы.

Безопасность трансграничного обмена

В современных условиях глобализации все чаще требуется межгосударственное информационное взаимодействие, безопасность которого должна обеспечиваться по стандартам сотрудничающих стран. В этих случаях у государственных органов и коммерческих организаций возникает необходимость создания трансграничной доверенной среды. Компания «С-Терра СиЭсПи» имеет опыт защиты такого взаимодействия на своем оборудовании для внутренних ведомств Российской Федерации и Республики Беларусь. Компанией разработан сценарий, который позволяет создать единые центры хранения и обмена ресурсами для союзных государств. В его основе лежит использование С-Терра Шлюз Экспортный и BEL VPN Gate с белорусской криптографией.

Если заказчик обладает возможностью создать свой центр обработки данных, то перед ним почти всегда стоит задача построения катастрофоустойчивого решения – и, соответственно, задача репликации данных. Для таких случаев компания «С-Терра СиЭсПи» предлагает сценарии защиты высокоскоростных каналов связи на канальном и сетевом уровнях. Масштабируемость решения позволяет с помощью как аппаратных, так и виртуальных решений защищать каналы данных с пропускной способностью более 10 Гбит/с.

Безусловно, для владельцев конфиденциальной информации ее сохранность в ЦОДе – самая важная характеристика. Использование средств шифрования на основе национальных криптографических алгоритмов, в частности VPN-продуктов С-Терра, позволяет выполнить требования современного законодательства (ФЗ-152, ФЗ-242 и др.), обеспечить высокую производительность и надежно защитить данные при их передаче между участниками информационного обмена, в том числе трансграничного.