Приложение 5 - "Требования к внешнему хостингу данных"

Данные требования применимы к хостингу всех приложений и данных **ВТ** классов **"Конфиденциально"** или **"Строго конфиденциально"** на любом объекте, который не находиться в собственности или под управлением ВТ. Это включает, помимо прочего, Облачные службы, при которых а) передаваемые данные защищены от перехвата, как правило - с использованием протокола шифрования, а также б) данные ВТ зашифрованы при хранении в рамках облачной службы.

К Конфиденциальным приложениям и данным, хостинг которых осуществляется за пределами ВТ, применимы следующие условия:

- Центр обработки данных должен иметь действующий сертификат ISO 27001 (или сертификат/ сертификаты, демонстрирующий эквивалентные средства контроля) по управлению безопасностью, или должен соответствовать Требованиям безопасности сертификации ISO 27001 или политикам безопасности, соответствующим ISO 27001 и/или работать над получением сертификата ISO 27001 в сроки, согласованные с ВТ;
- Передаваемые данные должны быть защищены устойчивым шифрованием с целью защиты данных ВТ между точкой выхода из ВТ и границей Центра обработки данных (как правило - балансировщиком нагрузки и расшифровывающим устройством, расположенным за межсетевым экраном на границе Центра обработки данных);
- Инженеры Центра обработки данных, имеющие физический доступ к серверам, не должны иметь логического доступа к производственной среде, а администраторы с логическим доступом к системам, не должны иметь физического доступа к Центру обработки данных.
- Весь логический доступ должен контролироваться системой обеспечения безопасности учетных записей с целью обеспечения контроля управления паролями и реализации соответствующего процесса предоставления разрешений для проверки идентификационных данных запрашивающего лица, например, CyberArk.
- Применительно к привилегированному доступу (включая, помимо прочего, управление базами данных), управление паролями должно быть привязано к срокам и, во всех возможных случаях, должны быть реализованы дополнительные ограничения на исходный IP-адрес.
- Любой привилегированный доступ, (например, со стороны Администраторов баз данных, группы безопасности доступа и т.п.) к системам, на которых осуществляется обработка Информации ВТ, должен отвечать требованиям, предусмотренным Приложением 1 - "Классификация информации".
- Для удаленного доступа, необходимо использовать виртуальную частную сеть в сочетании с основанной на ролях двухфакторной аутентификацией; кроме того, весь удаленный привилегированный доступ третьих сторон может получать доступ к системам, в которых осуществляется передача или хранение данных ВТ, только из той же страны, что и Центр обработки данных или из страны или с территории, которая обеспечивает достаточный уровень защиты для данных ВТ;
- Необходимо реализовать процессы управления криптографическими ключами полного жизненного цикла, которые соответствуют передовым методикам отрасли;
- Любой физический доступ к зонам или оборудованию, где осуществляется хранение или обработка Информации ВТ, должен иметь проверяемый процесс, например, процесс запроса на внесение изменений, чтобы гарантировать предоставление доступа только на минимально необходимый период, т.е. бессрочный доступ не допускается;
- Резервные хранилища данных за пределами объекта должны шифроваться в соответствии с требованиями, предусмотренными Приложением 1;
- Необходимо располагать средствами контроля для минимизации, выявления и предотвращения неразрешенного доступа. Средства контроля должны предусматривать создание аудиторского следа с использованием принципа "Кто, Что, Откуда, Когда".
- "Кто" - какой пользователь, например, идентификатор учетной записи пользователя;
- "Что" - к какому активу он получал доступ, например, данные;
- "Откуда" он получал доступ к активу, например, IP-адрес; а также

- "Когда" - например, отметка времени.
- Сведения обо всем физическом и логическом доступе должны фиксироваться в журнале, а файлы журнала - сохраняться в течение 1 года (минимум);
- В случае нарушения, когда имеет место утечка, хищение или видоизменение данных ВТ, необходимо располагать процессом для того, чтобы в разумный период времени оповестить ВТ с достаточной степенью детализации;

При наличии Строго конфиденциальной информации дополнительно применяются следующие условия:

- Центр обработки данных должен пройти проверку системы безопасности на объекте;
- Серверы приложений, базы данных и т.п. должны размещаться на выделенной инфраструктуре без других арендаторов, а их хостинг - осуществляться в отдельной стойке с защищенным корпусом. В случае если данное требование не может быть выполнено, Департамент ВТ по оценке рисков должен получить заверения, демонстрирующие достаточную изоляцию данных ВТ от данных других клиентов, использующих ту же самую среду, что гарантирует, что Администраторы баз данных не могут иметь логического доступа к копиям данных клиента, а также не могут просматривать данные клиента в объединенном виде. Таблицы и строки баз данных не должны отражать вид одной копии данных клиента.
- Необходимо располагать процессами, гарантирующими безопасное удаление Строго конфиденциальных данных в конце их жизненного цикла в облаке; Стирание/удаление на всех устройствах хранения, содержащих Строго конфиденциальные данные, должно осуществляться в соответствии с указаниями, предусмотренными Приложением 1;