Политика информационной безопасности

Цель политики

Настоящая политика уточняет требования политик информационной безопасности компаний, входящих в группу VK (далее — VK) применительно к управлению и обеспечению информационной безопасностью (далее — ИБ) при предоставлении облачных услуг VK Cloud.

Область действия политики

Применимость: VK Cloud
Применимо начиная с: 01.09.2023

Управление и обеспечение ИБ при предоставлении сервисов VK Cloud

Разделение ответственности в области ИБ

- Обязанности и ответственность в области ИБ при использовании облачных услуг разделяются между VK Cloud и потребителями облачных услуг (далее — клиент). Описание границ разделения ответственности поддерживается в актуальном состоянии в рамках публичной документации, доступной для потенциальных и действующих клиентов VK Cloud.

Коммуникация с клиентами

- VK Cloud обеспечивает своевременное информирование клиентов о статусе работы сервисов, сбоях и изменениях, которые могут на них повлиять. Подобное уведомление проводится через раздел Статус работы сервисов на сайте VK Cloud, а также для повышения оперативности в специальном Telegram-канале.

Сообщения о нарушениях ИБ

- Эффективное взаимодействие между VK Cloud и клиентами при нарушениях ИБ является важным фактором минимизации возможных последствий инцидентов ИБ.
  В VK внедрен и постоянно совершенствуется процесс управления инцидентами ИБ.

- VK Cloud предоставляет своим клиентам механизмы сообщения о событиях и инцидентах ИБ. VK Cloud обязуется уведомлять пользователей об инцидентах, повлиявших на них.
  При необходимости расследования инцидентов VK Cloud гарантирует обеспечение взаимодействия с клиентами, предоставление необходимой информации.

ИБ при разработке и внедрении облачных сервисов

- Разработка и внедрение облачных сервисов VK Cloud выполняется с учетом требования по ИБ.

- Требования по ИБ для облачных сервисов VK Cloud формируются на основе анализа безопасности архитектуры разрабатываемых и внедряемых сервисов и лучших практик в области ИБ.

- По результатам разработки проводится всестороннее тестирование разработанных сервисов или изменений в них, включая контроль реализации требований
  ИБ и безопасности кода.

- Для продуктовых команд и команд разработки проводятся тренинги и повышение осведомленности по безопасной разработке.

Риски от уполномоченных инсайдеров, управление доступом

- VK Cloud учитывает риск несанкционированного доступа уполномоченных инсайдеров к клиентским данным и принимает меры по его минимизации. VK Cloud строго контролирует доступ к хранилищам и базам данных.
- Внедрена политика управления доступом сотрудников VK Cloud и контрагентов, события ИБ регистрируются и отслеживаются, методы аутентификации регламентированы. Только авторизованные работники VK или подрядчиков VK получают доступ к ресурсам VK Cloud, исходя из принципа наименьших привилегий.
- Учетные записи и их права пересматриваются для минимизации рисков ИБ, связанных с накоплением избыточных прав, осуществлением несанкционированного доступа и неправомерного использования информационных ресурсов VK Cloud.
- Доступ к данным клиентов строго ограничен и предоставляется только тем работникам, которым этот доступ требуется для осуществляется должностных обязанностей. Со всеми работниками подписывается соглашение о конфиденциальности, проводится регулярное обучение и повышение осведомленности в области ИБ.

Управление жизненным циклом и доступом клиентов

- Началом жизненного цикла клиента является создание учетной записи в платформе VK Cloud. В дальнейшем, управление правами доступа пользователей клиента осуществляется самим клиентом, включая, заведение пользователей, настройку уровня доступа, двухфакторной аутентификации и т.д.
- VK Cloud осуществляет поддержку своих клиентов на всех этапах их жизненного цикла в рамках технической поддержки.
- Удаление данных клиента осуществляется либо при удалении учетной записи в платформе VK Cloud, либо при отключении клиента в случае неуплаты за предоставляемые сервисы.

Безопасность виртуализации

- VK Cloud уделяет внимание обеспечению безопасности виртуализации. Для этого VK Cloud обеспечивает контроль и управление доступом к виртуальной инфраструктуре, защиту от несанкционированного доступа к виртуальной инфраструктуре, защиту от сетевых атак, управляет уязвимостями.

Изоляция клиентов облачных сервисов

- Инфраструктурные ресурсы VK Cloud запущены на специально выделенных физических серверах, не используемых для работы среды виртуализации. Доступ из клиентских сетей в сервисные сети невозможен.
- Виртуальная среда клиента VK Cloud изолирована от других клиентов. Осуществляется управление информационными потоками на уровне клиентских виртуальных машин.
- Изоляция между клиентами обеспечивается: на уровне сети, на уровне гипервизора и на уровне приложения. При создании виртуальной машины клиент самостоятельно осуществляет настройку правил межсетевого экранирования или выбирает предлагаемый сетевой профиль.