Безопасность платформы

Для обеспечения высокого уровня защищенности платформы VK Cloud используются меры и практики безопасности, описанные ниже.

Дополнительная информация размещена на странице Безопасность облака.

Отслеживание и противодействие атакам

Security Operations Center (SOC VK) обеспечивает мониторинг VK Cloud, анализирует события безопасности серверов VK Cloud и выявляет аномалии с использованием системы класса SIEM (Security Information and Event Management). Также работают следующие механизмы:

Антифрод

Антифрод VK Cloud — комплекс мер безопасности и правил, направленных на фильтрацию автоматических регистраций ботов и пользователей, а также на предотвращение потенциальных атак на ресурсы платформы VK Cloud.

При активации сервисов VK Cloud может потребоваться подтвердить данные пользователя. В этом случае воспользуйтесь одним из предложенных способов верификации личности:

- **Привязка банковской карты.** Привяжите карту и, при необходимости, произведите оплату сервисов VK Cloud.
- **Карточка компании (для юридических лиц).** В сообщении приложите файл с реквизитами организации, от имени которой выполняется регистрация. Почтовый адрес должен указывать на наименование или иные реквизиты организации.
- **Обращение в техническую поддержку.** Создайте заявку на активацию учетной записи на портале службы технической поддержки. Категория заявки — учетная запись, группа — активация и доступ.

Отслеживание подозрительной активности

Пользователи интернета и автоматизированные сервисы вправе пожаловаться как вручную, так и автоматически на подозрительную активность, производящуюся с IP-адресов, принадлежащих VK Cloud. Например, подозрительная активность может включать в себя обращение к одной и той же веб-странице через короткие промежутки времени, множественные попытки подбора пароля и т. д.

Чтобы предоставлять пользователям бесперебойные сервисы, техническая поддержка VK Cloud оперативно реагирует на подобные жалобы.

Пользователю VK Cloud будет направлено предупреждение о наличии жалобы на подозрительную активность с IP-адреса, входящего в его проект. При отсутствии ответа в течение одних суток, IP-адрес может быть отсоединен от виртуальной машины и удален из проекта для устранения подозрительной активности.

Подозрительная активность может быть связана с получением злоумышленником несанкционированного доступа к виртуальной машине пользователя. Чтобы уменьшить риск возникновения подобной ситуации, соблюдайте правила безопасности:

- не устанавливайте простые пароли для учетных записей;
- не предоставляйте неконтролируемый доступ к ресурсам проекта;
- внимательно относитесь к скачиваемым и устанавливаемым на виртуальную машину программным средствам;
- проверяйте виртуальные машины на наличие вредоносного программного обеспечения или кода.

Проведение проверок безопасности

Внешние проверки проводятся не реже одного раза в год с участием внешнего подрядчика. Проверка проводится в том числе по модели внутреннего нарушителя.
Также VK Cloud проводит собственные аудиты информационной безопасности и участвует в программах Bug Bounty по поиску уязвимостей:

- Standoff 365.
- Bug Bounty Ru.
- BI.ZONE Bug Bounty.

Это позволяет максимально быстро выявлять и устранять уязвимости в VK Cloud.

Применение принципов безопасной разработки при построении платформы

- Обучение по информационной безопасности для разработчиков платформы.
- Интеграция и автоматизация инструментов и практик безопасности на всех этапах жизненного цикла разработки и эксплуатации (DevSecOps).
- Архитектурное ревью и аудит безопасности каждого сервиса.

Обеспечение соответствия требованиям 94-V и PCI DSS

Информация о соответствии требованиям 94-V приведена в соответствующем разделе.

Информация о сертификации PCI DSS доступна в разделе Сертификаты, лицензии и аттестаты.

Применение лучших отраслевых практик

- Изоляция сегментов и сервисов VK Cloud друг от друга с помощью файервола.
- Разграничение доступа к ресурсам VK Cloud с помощью ролевой модели на уровне Identity and Access Management (IAM).
- Наличие доступа к платформе только у ограниченного круга администраторов VK Cloud с обязательной аутентификацией. Для доступа используются доверенные и защищенные хосты (jump hosts).
- Разделение ответственности за безопасность между VK Cloud и пользователем (подробнее на странице Безопасность облака).