Яндекс Облако

Разверните ИТ-инфраструктуру на безопасной платформе Яндекс.Облако

Грамотный подход к разработке и проектированию архитектуры, соответствие индустриальным стандартам и законодательным требованиям, безопасность физической инфраструктуры и защита данных — приоритет Яндекс.Облака и ответственность перед клиентами платформы

4 причины, почему Яндекс.Облако — безопасная и надёжная платформа

1 Заботится о безопасности своих сервисов на этапах создания и эксплуатации

Безопасная разработка
Процесс безопасной разработки (Security Development Lifecycle, SDL) помогает нам идентифицировать риски и управлять ими с момента проектирования сервисов платформы и на протяжении всего срока эксплуатации. Внедрение SDL позволяет снизить количество и серьезность ошибок, приводящих к эксплуатируемым уязвимостям.

Многоуровневая защита
Безопасность Яндекс.Облака организована таким образом, что одной угрозе противостоит набор средств защиты на разных уровнях. Такой подход удорожает любую потенциальную атаку и позволяет оперативно выявлять и предотвращать несанкционированную деятельность злоумышленников.

2 Обеспечивает безопасность облачной инфраструктуры с разных сторон

Физическая безопасность, мониторинг, шифрование данных и надежный способ очистки, гарантирующий невозможность их восстановления — над всем этим успешно работают разные команды Яндекс.Облака

3 Разделяет ответственность за обеспечение безопасности

Безопасность систем, использующих облачные сервисы, требует разделения ответственности между клиентом — владельцем конечной системой и провайдером — владельцем облачной инфраструктуры, используемой конечной системой.

В зависимости от модели облачных сервисов, используемой клиентской системой (IaaS, PaaS), данное разделение меняется.

4 причины, почему Яндекс.Облако — безопасная и надёжная платформа

4 Соответствует требованиям ФЗ-152 и индустриальных стандартов

ФЗ-152

Платформа Яндекс.Облако соответствует требованиям федерального закона № 152-ФЗ «О персональных данных». Для сервисов Яндекс.Облака выполнены меры по защите персональных данных согласно Постановлению № 1119 и 21 приказу ФСТЭК в соответствии с требованиями к 3-му уровню защищённости (УЗ-3).

GDPR

Общий регламент о защите данных (General Data Protection Regulation, GDPR) регулирует сбор и обработку персональных данных (ПД) физических лиц, находящихся в Европейской экономической зоне. Он призван усилить защиту ПД и сделать прозрачными их сбор, хранение и обработку. Яндекс.Облако выполняет ключевые требования GDPR

Стандарты ISO

Яндекс.Облако заботится о том, чтобы обеспечить безопасность систем и данных, которые клиенты размещают на платформе. Поэтому построили систему управления информационной безопасностью (СУИБ) в соответствии с высокими требованиями стандартов международной организации по стандартизации (ISO).

Аудит СУИБ Яндекс.Облака проводила международная команда аудиторов компании BSI. По результатам аудита платформа получила сертификаты соответствия стандартам ISO 27001, ISO 27017 и ISO 27018.

PCI DSS

Содержит набор требований для защиты данных держателей карт. Требования обязательны и распространяются на все компании, обрабатывающие данные платёжных систем Visa, MasterCard, American Express, JCB, МИР и др.

Соответствие облачной инфраструктуры требованиями PCI DSS не только позволяет клиентам использовать облачные сервисы для обработки данных платежных карт, но и подтверждает высокий уровень безопасности, обеспечиваемый провайдером.

На данный момент все зоны доступности Яндекс.Облака имеют сертификат соответствия требованиям PCI DSS v3.2.1 в части физической безопасности.

Посмотреть сертификаты и заключения

Полезные ссылки

- Подробнее о соответствии требованиям и безопасности Яндекс.Облака на сайте
- Международные стандарты безопасности в Яндекс.Облаке, вебинар, февраль 2020 (35 минут)
- Защита персональных данных в Яндекс.Облаке и соответствие ФЗ-152, вебинар, февраль 2020 (12 минут)
- Ключевые аспекты безопасности Облака — Евгений Сидоров и Андрей Иванов, вебинар, январь 2020 (58 минут)