## Меры безопасности

Настоящий документ представляет собой положение о технических и организационных мерах, реализуемых Яндексом для защиты данных клиентов на Платформе «Яндекс.Облака».

### Организация информационной безопасности

Система управления информационной безопасностью

- Яндекс поддерживает систему управления информационной безопасностью, которая включает в себя принятие и применение внутренних политик и процедур, направленных на минимизацию рисков информационной безопасности для клиентских данных.

Ответственность за безопасность

- У Яндекса есть команда безопасности, ответственная за внедрение и мониторинг процедур безопасности.

Управление рисками

- У Яндекса есть программа управления рисками, которая включает в себя регулярную оценку рисков и выполнение планов обработки рисков.

### Безопасность человеческих ресурсов

Скрининг

- Яндекс проверяет и верифицирует информацию обо всех кандидатах на трудоустройство.

Обучение

- Яндекс требует от всех сотрудников и подрядчиков применять меры информационной безопасности в соответствии с установленными правилами и процедурами в компании.
- Яндекс проводит обучение сотрудников по вопросам надлежащего обращения с данными клиентов.

Прекращение или смена работы

- Яндекс определяет, доводит до сведения своих сотрудников и подрядчиков и добивается выполнения тех обязанностей по обеспечению информационной безопасности, которые остаются в силе после увольнения или смены места работы.

### Управление активами

Инвентарь активов

- У Яндекса есть инвентарь активов, который включает в себя данные о клиентах и произведенные сервисом данные.

Допустимое использование

- Яндекс документирует и реализует правила допустимого использования информации и активов, связанных с информацией и средствами обработки информации.

Возвращение активов

- Сотрудники Яндекса возвращают все организационные активы, находящиеся в их распоряжении, после прекращения трудового договора.

Классификация информации

- Яндекс классифицирует информацию с точки зрения требований законодательства, ценности, критичности и чувствительности к несанкционированному раскрытию или изменению.

Обращение с активами

- Яндекс разрабатывает и внедряет процедуры обращения с активами в соответствии с принятой схемой классификации информации.

**Управление доступом**

Политика управления доступом

- У Яндекса есть политика, которая гарантирует, что только авторизованные лица имеют доступ к объектам, защищенным зонам, а также вычислительным и сетевым ресурсам.

Доступ к сетям и системам

- Доступ к сетям и системам Яндекса предоставляется только уполномоченным сотрудникам.
- Руководство Яндекса обязано утверждать доступ каждого сотрудника ко всем объектам, защищенным зонам и вычислительным и сетевым ресурсам.
- Яндекс ограничивает права доступа каждого пользователя минимальным набором прав, необходимым для выполнения его работы, и только на необходимое время.
- Яндекс размещает все интерфейсы управления аппаратным обеспечением в сегрегированных сетях с ограниченным доступом авторизованного персонала.
- Яндекс предоставляет доступ к исходному коду только уполномоченным лицам в соответствии с политикой безопасности

Проверка прав доступа пользователей

- Яндекс ежегодно пересматривает все права доступа пользователей.

Отзыв или корректировка прав доступа

- Яндекс отзывает права доступа к информации и системам для всех сотрудников, прекращающих работу в компании, и корректирует — при изменениях круга их ответственности.

Качество паролей

- Яндекс обеспечивает качественные пароли в своих системах управления паролями. Проверки включают минимальную длину пароля, количество классов символов и максимальный срок действия.

Сегрегация в виртуальных вычислительных средах

- Яндекс обеспечивает разделение доступа между сетями разных клиентов, а также и между внутренней средой администрирования Яндекса и средой облачных вычислений Яндекса.
- Яндекс контролирует сетевые потоки данных с помощью автоматизированных систем (списки доступа на маршрутизаторах, динамический межсетевой экран, брандмауэр).

**Физическая безопасность и безопасность среды**

Физический периметр безопасности

- Яндекс определяет периметры безопасности и использует их для защиты мест, содержащих конфиденциальную или критическую информацию, а также средства обработки информации.

Контроль физического доступа

- У Яндекса есть надлежащие средства контроля физического доступа, которые позволяют гарантировать, что доступ разрешен только авторизованному персоналу.

Вспомогательные инженерные коммуникации

- Яндекс защищает оборудование от сбоев питания и других сбоев, вызванных сбоями в работе вспомогательных инженерных коммуникаций.

Защита оборудования вне служебных помещений

- Сотрудники Яндекса не могут вывозить оборудование, информацию или программное обеспечение за периметр компании без предварительного разрешения.
- Яндекс применяет меры безопасности к активам вне периметра компании с учетом различных рисков работы в таких условиях.

Безопасная утилизация или повторное использование оборудования

- Яндекс гарантирует, что любые конфиденциальные данные на носителях информации были удалены или надежно перезаписаны перед повторным использованием носителей. В случае непригодности носителей Яндекс надежно утилизирует их, следуя формальным процедурам.

**Безопасность данных и управление жизненным циклом информации**

Безопасность передачи данных

- Яндекс защищает всю информацию клиентов, которая передается по общедоступным сетям, с использованием протокола TLS.

Безопасность данных при хранении

- Яндекс шифрует все данные клиентов при хранении.

Безопасное удаление

- При освобождении ресурсов клиента эти ресурсы очищаются перед их передачей другому клиенту.

**Управление инцидентами**

Реагирование на инциденты и отчетность

- В Яндексе есть формальный процесс мониторинга, отчетности и реагирования для инцидентов безопасности, чтобы идентифицировать, регистрировать и надлежащим образом реагировать на известные или предполагаемые инциденты безопасности.
- В Яндексе есть процедуры для сообщения клиентам об инцидентах безопасности, которые влияют на данные клиентов, без неоправданных задержек.

**Разработка и обслуживание информационных систем**

Жизненный цикл разработки систем

- В Яндексе есть документированный жизненный цикл разработки систем, который регулирует разработку и развертывание систем и приложений.

Требования информационной безопасности

- Яндекс включает требования, связанные с информационной безопасностью, в требования к новым информационным системам и усовершенствованиям существующих информационных систем.

Процедуры контроля изменения системы

- Яндекс контролирует изменения в системах в рамках жизненного цикла разработки с помощью формальных процедур контроля изменений, которые включают в себя обзор архитектуры безопасности.
- Яндекс использует процесс экспертной оценки всего производственного кода своей облачной платформы, а сотрудник службы безопасности проверяет критическую функциональность перед ее выпуском.

Проектирование защищенных систем

- Яндекс применяет принципы проектирования защищенных систем к любым работам по внедрению информационных систем.

Тестирование информационной безопасности

- Яндекс проводит регулярное фаззинг-тестирование, тестирование на проникновение и сканирование уязвимостей, чтобы обнаруживать, смягчать и решать проблемы безопасности в облачной платформе.

Криптографические стандарты

- В Яндексе задокументирована политика, которая устанавливает минимальные криптографические стандарты, которым должны следовать все приложения, а также сетевые и вычислительные ресурсы.

Безопасная среда разработки

- Яндекс создает и надлежащим образом защищает среды для разработки и интеграции систем, во всем жизненном цикле разработки систем.
- Яндекс разделяет среды разработки, тестирования и продакшн-среду.
- У Яндекса есть процедуры, гарантирующие, что производственные данные никогда не реплицируются в средах разработки или тестирования.

Управление уязвимостями

- Яндекс выполняет регулярные сканирования уязвимостей предпроизводственных, открытых в интернет систем и сетевых устройств перед перемещением этих систем / устройств в производство.
- Яндекс устраняет все обнаруженные уязвимости до перехода этих систем в производство.

Управление исправлениями

- У Яндекса есть политика управления исправлениями, документирующая максимальное время между моментом поставки критического патча безопасности и моментом его применения.

## Непрерывность работы и аварийное восстановление

Избыточность

- Яндекс использует механизмы резервирования для всех критических сервисов.
- Яндекс работает в нескольких территориально распределенных дата-центрах, предназначенных для работы 24x7 и защищенных от различных угроз окружающей среды.
- Яндекс использует избыточность хранилищ данных, которая позволяет восстановить данные клиентов в случае выхода из строя оборудования.

Тесты

- Яндекс регулярно тестирует свои планы обеспечения непрерывности работы и аварийного восстановления.

## Обзор информационной безопасности

Самостоятельная оценка

- Яндекс регулярно проверяет свои информационные системы на соответствие политике и стандартам информационной безопасности компании.
- Яндекс оценивает и пересматривает свой подход к управлению и реализации информационной безопасности с запланированной регулярностью или при возникновении существенных изменений.