Заключение о соответствии системы защиты персональных данных требованиям №152-ФЗ «О персональных данных»

ООО «Кард Секьюрити»

(Наименование организации-изготовителя, фамилия, имя, отчество индивидуального предпринимателя, принявших декларацию о соответствии)

(адрес, телефон, факс)

Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации №3099 от 22 ноября 2016

в лице **генерального директора Иванова Александра Юрьевича**

(Фамилия, имя, отчество руководителя организации, от имени которой принимается декларация)

заявляет, что **в результате проведенного аудита системы защиты персональных данных ИСПДн «Платформа «Яндекс.Облако» в составе следующих Сервисов:**

1. **Сервис Облачных вычислений / Yandex Compute Cloud**
2. **Сервис Магазин облачных приложений / Yandex Cloud Marketplace**
3. **Сервис для управления сетевыми балансировщиками нагрузки / Yandex Load Balancer**
4. **Сервис Управления для PostreSQL / Yandex Managed Service for PostgreSQL**
5. **Сервис Управления для MongoDB / Yandex Managed Service for MongoDB**
6. **Сервис Управления для ClickHouse / Yandex Managed Service for ClickHouse**
7. **Сервис Управления для Redis™ / Yandex Managed Service for Redis™**
8. **Сервис Управления для MySQL® / Yandex Managed Service for MySQL®**
9. **Сервис Управления данными Data Proc / Yandex Data Proc**
10. **Сервис по управлению облачными ресурсами / Yandex Resource Manager**
11. **Сервис по управлению доступом к облачным ресурсам / Yandex Identity and Access Management**
12. **Сервис речевых технологий / Yandex SpeechKit**
13. **Сервис машинного перевода / Yandex Translate**
14. **Сервис Виртуальное частное облако / Yandex Virtual Private Cloud**
15. **Сервис Объектного хранилища / Yandex Object Storage**

(Наименование, тип, марка продукции, на которую распространяется декларация, код ОК 005-93 и (или) ТН ВЭД СНГ)

а также инфраструктуры на основе которой они работают, состоящей из технических и программных средств, включая биллинговую систему (Биллинг).

По результатам моделирования угроз были признаны актуальными угрозы третьего типа и неактуальными угрозы первого и второго типа. На момент проведения оценки соответствия были выполнены все необходимые меры для нейтрализации актуальных угроз безопасности ПДн.

Установлено соответствие указанных ИСПДн требованиям

1. **№152-ФЗ «О персональных данных» от 27 июля 2006 г.**
2. **«Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации № 1119 от 01.11.2012 г.**
3. **«Состав и содержание технических и организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный Приказом ФСТЭК № 21 от 18.02.2013 г.**

(Обозначение нормативных документов, соответствие которым подтверждено данной декларацией с указанием пунктов, содержащих требования для данной продукции)

а также в данных ИСПДн обеспечивается: **3-й уровень защищенности ПДн**

Краткое описание встроенных защитных механизмов Платформы «Яндекс.Облако» и защитных мер, выполнение которых позволит клиентам выполнить требования законодательства РФ к третьему уровню защищенности персональных данных, приведено в Приложении 1.

Схема декларирования соответствия **на основании собственных доказательств**

В ООО «Яндекс.Облако» приняты организационные и технические меры, обеспечивающие соответствие ИСПДн «Платформа «Яндекс.Облако» требованиям №152-ФЗ «О персональных данных» и его подзаконных актов

Дата подписания **22.02.2019**

М.П.

(Подпись)

генеральный директор ООО «КардСек», Иванов А.Ю.

(Инициалы, фамилия)

Приложение 1. Разделение ответственности за защиту персональных данных

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 3
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации		
ИАФ.5	Защита обратной связи при вводе аутентификационной информации		
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	На уровне доступа к сервисам Платформы, предоставляемым клиентам	На уровне клиентских виртуальных машин
Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа		
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	Управление сетевым доступом на уровне: • физического оборудования Платформы; • сервисных/служебных сетей Платформы; • ограничение доступа между сегментами сетей различных клиентов Платформы; • ограничение доступа из клиентских сетей в сервисную/служебную сеть.	Управление сетевым доступом: • между сегментами клиентской виртуальной сети; • сетевого доступа к клиентской виртуальной сети из-за ее пределов.
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование	На уровне: • физического оборудования	На уровне клиентских виртуальных машин

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 3
	информационной системы	Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы		
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)		
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	На уровне доступа: • пользователей к сервисам Платформы; • административного доступа к физическим и виртуальным сервисным/служебным системным компонентам.	На уровне удаленного доступа к клиентским виртуальным серверам.
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Не применяется	Не применяется
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Не применяется	Не применяется
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	На уровне сервисных/служебных системных компонентов.	При организации такого взаимодействия с клиентскими виртуальными машинами
Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Физические носители информации, применяемые в рамках Платформы	Не применимо
Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	На уровне: • сервисных/служебных системных компонентов; • сервисов Платформы, в том числе клиентских	На уровне клиентских виртуальных серверов и используемого на них программного обеспечения и средств защиты информации.
РСБ.2	Определение состава и содержания информации о событиях безопасности,		

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 3
	подлежащих регистрации	действий по использованию сервисов.	
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		
РСБ.7	Защита информации о событиях безопасности		
Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Не применимо, так как используются ОС, не подверженные вирусному заражению, а также отсутствует доступ из клиентских сетей в сервисные/служебные.	На уровне клиентских виртуальных машин
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		
Контроль (анализ) защищенности персональных данных (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	На уровне сервисных/служебных виртуальных и физических системных компонентов	На уровне клиентских виртуальных машин
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		
Защита среды виртуализации (ЗСВ)			
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	На уровне: • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	Не применимо
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин		На уровне клиентских виртуальных машин
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Не применимо, так как используются ОС, не подверженные вирусному заражению, а также отсутствует доступ из клиентских сетей в сервисные/служебные.	На уровне клиентских виртуальных машин
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты	Управление сетевым	На уровне сегментов

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 3
	(сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	доступом на уровне: • сервисных/служебных сетей Платформы; • ограничение доступа между сегментами сетей различных клиентов Платформы.	сети клиента
Защита технических средств (ЗТС)			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	На уровне обеспечения физической безопасности ЦОД	Не применимо
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Не применяется в ЦОД для отображения ПДн	Не применимо
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	На уровне ЦОД	Не применимо
Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	На уровне каналов: • используемых для доступа администраторов к системным компонентам Платформы; • используемых для доступа пользователей и администраторов к консоли управления средой виртуализации; • между ЦОД.	На уровне каналов связи, установленным клиентом для доступа к его виртуальным машинам.
Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных	На уровне клиентской виртуальной инфраструктуры
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты		

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 3
	персональных данных	серверов Платформы и прочих виртуальных устройств; • Программного обеспечения Платформы.	
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		