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

ООО «Кард Сек»

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

Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации
№Л024-00107-00/00583151 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 отношении Сервисов, прописанных в Приложении 1**, размещенных в ЦОД:

- ООО «Яндекс» по адресу г. Мытищи, ул. Силикатная, д.19;
- ООО «Яндекс ДЦ Владимир» по адресу г. Владимир, ул Поисковая (мкр. Энергетик), д. 1;
- ООО «Яндекс ДЦ» по адресу ул. Пушкина, д.21, г. Сасово;
- ООО «Яндекс ДЦ Калуга» по адресу г. Калуга, 1-й Автомобильный проезд, д. 8

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

Также установлено соответствие **ИСПДн «Платформа «Яндекс.Облако»** 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)

В **ИСПДн «Платформа «Яндекс.Облако»** обеспечивается: **1-й уровень защищенности ПДн**

Краткое описание встроенных защитных механизмов **ИСПДн «Платформа «Яндекс.Облако»** и защитных мер, выполнение которых позволит клиентам выполнить требования законодательства РФ к первому уровню защищенности персональных данных, приведено в Приложении 2.

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 **03.10.2024**

М.П.

(Подпись)

генеральный директор ООО «Кард Сек», Иванов А.Ю.
(Инициалы, фамилия)

Приложение 1. Список сервисов в области аудита системы защиты ИСПДн «Платформа «Яндекс.Облако»

1. Yandex Identity and Access Management (IAM);
2. Yandex Cloud Organization;
3. Yandex Resource Manager;
4. Yandex Compute Cloud;
5. Yandex Virtual Private Cloud;
6. Yandex Network Load Balancer;
7. Yandex Object Storage;
8. Yandex Billing
9. Yandex API Gateway
10. Yandex Managed Service for: (PostgreSQL, MySQL®, MongoDB, ClickHouse, Redis™, Apache Kafka®, GreenPlum®, ElasticSearch);
11. Yandex Data Processing;
12. Yandex Container Registry;
13. Yandex Cloud Functions;
14. Yandex IoT Core;
15. Yandex Managed Service for Kubernetes;
16. Yandex DataLens;
17. Yandex Cloud Marketplace;
18. Yandex Message Queue;
19. Yandex Database;
20. Yandex SpeechKit;
21. Yandex Translate;
22. Yandex DataSphere;
23. Yandex Application Load Balancer;
24. Yandex DataTransfer;
25. Yandex Vision OCR;
26. Yandex Audit Trails;
27. Yandex SpeechSense;
28. Yandex Foundation Models.
29. Smart Web Security (SWS).
30. SmartCaptcha.
31. Managed Service for Open Search (Open Search).

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

Дата подписания **03.10.2024**

М.П.

(Подпись)

генеральный директор ООО «Кард Сек», Иванов А.Ю.

(Инициалы, фамилия)

Приложение 2. 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 - 1
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 и клиентских Docker-контейнеров
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	На уровне физического оборудования Платформы	Не применяется
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
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 и клиентских Docker-контейнеров
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 и клиентских Docker-контейнеров
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	Управление сетевым доступом: • между сегментами клиентской виртуальной сети; • сетевого доступа к клиентской

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
		сетей Платформы; • ограничение доступа между сегментами сетей различных клиентов Платформы; • ограничение доступа из клиентских сетей в сервисную/служебную сеть.	виртуальной сети из-за ее пределов.
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
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 и клиентским Docker-контейнерам
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 и клиентскими Docker-контейнерами
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	На уровне сервисных/служебных	Не применяется

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
		системных компонентов	
Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.1	Учет машинных носителей персональных данных	На уровне физических носителей информации, применяемых в рамках Платформы.	Не применимо
ЗНИ.2	Управление доступом к машинным носителям персональных данных	На уровне физических носителей информации, применяемых в рамках Платформы.	Не применимо
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	На уровне физических носителей информации, применяемых 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 действий по использованию сервисов.	На уровне клиентских виртуальных серверов и Docker-контейнеров, а также используемого на них программного обеспечения и средств защиты информации.
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации		
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения		
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них		
РСБ.7	Защита информации о событиях безопасности		
Антивирусная защита (АВЗ)			

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
АВ3.1	Реализация антивирусной защиты	Не применимо, потому что защищенный сегмент содержит только серверы. Операционная система, используемая на серверах, практически не подвержена вирусному заражению. На серверах нет прямого доступа в Интернет и используется HIDS.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		
Обнаружение вторжений (СОВ)			
СОВ.1	Обнаружение вторжений	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских сегментов сети
СОВ.2	Обновление базы решающих правил		
Контроль (анализ) защищенности персональных данных (АНЗ)			
АН3.1	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 и клиентских Docker-контейнеров
АН3.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации		
АН3.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		
АН3.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		
АН3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе		
Обеспечение целостности информационной системы и персональных данных (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную	Не применимо, так как в состав Платформы не	На уровне клиентских

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	входит функционал по обмену электронной почтой	почтовых серверов
Обеспечение доступности персональных данных (ОДТ)			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств. выполняется автоматизированная репликация данных в платформенном хранилище.	На уровне ИСПДн клиента резервное копирование и восстановление персональных данных осуществляется клиентом. На уровне клиентских виртуальных машин и контейнеров Docker резервное копирование данных осуществляется клиентом с помощью платформенных инструментов.
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных		
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала		
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 и клиентских Docker-контейнеров
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	На уровне: • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	Реализовано на уровне архитектуры Платформы
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	На уровне: • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	На уровне: • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной	Не применимо, так как в защищаемом контуре	На уровне клиентских виртуальных машин и

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	инфраструктуре	расположены исключительно серверные мощности, используются ОС практически не подверженные вирусному заражению, отсутствует прямой доступ в интернет, а также на хостах применяется HIDS.	клиентских Docker-контейнеров
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Управление сетевым доступом на уровне: • сервисных/служебных сетей Платформы; • ограничение доступа между сегментами сетей различных клиентов Платформы.	На уровне сегментов 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.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и	На уровне каналов:	На уровне каналов связи, установленным клиентом

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	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	• используемых для доступа администраторов к системным компонентам Платформы; • используемых для доступа пользователей и администраторов к консоли управления средой виртуализации; • между ЦОД.	для доступа к его виртуальным машинам и Docker-контейнерам.
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	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 сегментов сети клиента
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	На уровне сервисных/служебных сегментов сети.	На уровне сегментов виртуальной сети клиента
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Не применимо	Не применимо
Выявление инцидентов и реагирование на них (ИНЦ)			
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Из числа работников Яндекс.Облако или его подрядчиков	Из числе работников клиентской организации или ее подрядчиков
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы «Яндекс.Облако»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Из числа работников Яндекс.Облако или его подрядчиков	Из числе работников клиентской организации или ее подрядчиков
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	На уровне: • физического оборудования Платформы; • средств управления средой виртуализации; • сервисных/служебных серверов Платформы и прочих виртуальных устройств; • сервисов Платформы.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ИНЦ.5	Принятие мер по устранению последствий инцидентов		
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов		
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 серверов Платформы и прочих виртуальных устройств; • Программного обеспечения Платформы.	На уровне клиентской виртуальной инфраструктуры и клиентских Docker-контейнеров
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		
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		