

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 сервиса «Yandex BareMetal», размещенной на следующих площадках:

- 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 сервиса «Yandex BareMetal» 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 сервисе «Yandex BareMetal» обеспечивается:

1-й уровень защищенности ПДн

Краткое описание встроенных защитных механизмов сервиса «Yandex BareMetal» и защитных мер, выполнение которых позволит клиентам выполнить требования законодательства РФ к первому 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 сервиса «Yandex BareMetal» требованиям №152-ФЗ «О персональных данных» и его подзаконных актов

Дата подписания

13.10.2025



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

Приложение 1. Разделение ответственности за защиту персональных данных

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	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	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	Не применяется
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов		На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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)		
Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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 Сервиса; • сервисных/служебных сетей Сервиса; • ограничение доступа между сегментами сетей различных клиентов Сервиса; • ограничение доступа из клиентских сетей в	Управление сетевым доступом: • между сегментами клиентской виртуальной сети; • сетевого доступа к клиентской виртуальной сети из-за ее пределов.

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
		сервисную/служебную сеть.	
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети		
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)	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	При организации такого взаимодействия с разворачиваемой инфраструктурой, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	На уровне сервисных/служебных системных компонентов	Не применяется
Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том	Неприменимо: Выполнение указанного	На уровне разворачиваемой инфраструктуры,

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов		
Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.1	Учет машинных носителей персональных данных	На уровне физических носителей информации, применяемых в рамках Сервиса.	Не применимо
ЗНИ.2	Управление доступом к машинным носителям персональных данных	На уровне физических носителей информации, применяемых в рамках Сервиса.	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 Сервиса.	Не применимо
Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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)			
АВЗ.1	Реализация антивирусной защиты	Не применимо, потому что Компания несет ответственность за обеспечение физической и сетевой безопасности Сервиса и не имеет возможности управлять средствами защиты на уровне клиентских серверов	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)		
Обнаружение вторжений (ОВВ)			
ОВВ.1	Обнаружение вторжений	На уровне:	На уровне клиентских

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
СОВ.2	Обновление базы решающих правил	- сервисов вычислительной среды; - сервисных/служебных серверов Сервиса и прочих физических устройств; - сетевого оборудования.	сегментов сети
Контроль (анализ) защищенности персональных данных (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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		
АНЗ.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	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)	Не применимо, так как в состав Сервиса не входит функционал по обмену электронной почтой	На уровне клиентских почтовых серверов
Обеспечение доступности персональных данных (ОДТ)			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие	На уровне: физического оборудования	На уровне ИСПДн клиента резервное копирование и восстановление

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	мер по восстановлению отказавших средств и их тестирование	Сервиса; • сервисных/служебных серверов Сервиса и прочих физических устройств.	персональных данных осуществляется клиентом.
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных		На уровне ОС физических серверов Сервиса и инфраструктуры клиента резервное копирование данных осуществляется клиентом с помощью платформенных инструментов.
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	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин		
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных		
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций		
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		
Защита технических средств (ЗТС)			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации,	На уровне обеспечения физической безопасности ЦОД	Не применимо

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
	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		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Не применяется в ЦОД для отображения ПДн	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	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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 связи, установленным клиентом для доступа к разворачиваемой инфраструктуре, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		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 разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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)			

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры на уровне сервиса Yandex BareMetal	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 1
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Неприменимо: Выполнение указанного требования осуществляется при помощи функционала аттестованной среды облачных вычислений «Яндекс.Облако», имеющей аттестат соответствия № Л024-00107-00/00580503.00099.2023	Из числа работников клиентской организации или ее подрядчиков
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов		На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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 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 разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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 Сервиса; • сервисных/служебных серверов Сервиса и прочих физических устройств; • Программного обеспечения Сервиса.	На уровне разворачиваемой инфраструктуры, включающей ОС, СУБД, ППО, средства виртуализации и механизмы сетевой безопасности
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		