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 №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 Data Residency-as-a-Service» в отношении Сервисов, прописанных в Приложении 1,**

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

размещенных в ЦОД сервис-провайдера ООО «Яндекс.Облако», на момент проведения оценки соответствия были выполнены все необходимые меры для нейтрализации актуальных угроз безопасности ПДн.

По результатам моделирования угроз, выполненных в виде формализованной оценки рисков, были признаны актуальными угрозы третьего типа и неактуальными угрозы первого и второго типа.
Установлено соответствие ИСПДн «Платформа Data Residency-as-a-Service» 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 ИСПДн обеспечивается:**1-й уровень защищенности ПДн.**
Краткое описание защитных мер, исполнение которых позволит выполнить требования законодательства РФ к первому уровню защищенности персональных данных в ИСПДн «Платформа Data Residency-as-a-Service» приведено в Приложении 2.

Схема декларирования соответствия **на основании собственных доказательств**
В Инкантри, Инк приняты организационные и технические меры, обеспечивающие соответствие ИСПДн «Платформа Data Residency-as-a-Service» требованиям №152-ФЗ «О персональных данных» и его подзаконных актов.

Дата подписания **06.08.2021**

М.П.

(Подпись)

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

(Инициалы, фамилия)

Приложение 1. Список сервисов в области аудита системы защиты ИСПДн «Платформа Data Residency-as-a-Service»

1. REST API and Software Development Kit (SDK)
2. Border
3. Data Residency for Salesforce

Приложение 2. Оценка реализации требований по защите персональных данных

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-1 в ИСПДн
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)		
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	Идентификация и аутентификация пользователей в ИСПДн осуществляется по паре логин/пароль. Осуществляется проверка подлинности при помощи MFA. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	На уровне физического оборудования платформы виртуализации – выполняется ООО «Яндекс.Облако».
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Порядок управления учетными записями пользователей установлен документом «InCountry Identity & Access Management Standard». Создание, присвоение и уничтожение учетных записей пользователей осуществляется на основании соответствующих заявок. Всем пользователям присваиваются уникальные идентификаторы. Учётные записи пользователей, к которым больше не требуется доступ, отключаются или удаляются. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Управление средствами аутентификации осуществляется в соответствии с документами «InCountry Identity & Access Management Standard» и «InCountry Password Protection Standard». Используется безопасное хранение для средств аутентификации, таких как пароли и ключи. Утраченные или скомпрометированные средства аутентификации подлежат незамедлительной замене. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	В ИСПДн Компании осуществляется маскирование данных аутентификации при их вводе. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Идентификация и аутентификация внешних пользователей в ИСПДн осуществляется по паре логин/пароль. Осуществляется проверка подлинности при помощи MFA. Используются встроенные механизмы ОС и прикладного ПО.

Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Порядок управления учетными записями пользователей установлен документом «InCountry Identity & Access Management Standard». Всем пользователям предоставляется доступ к системам и информации на основе заявок, и доступ аннулируется, когда он больше не нужен. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Правила и методы разграничения доступа в Компании установлены документом «InCountry Identity & Access Management Standard». В Компании используется разграничение доступа на основе ролей. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	В Компании используются средства межсетевого экранирования.
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Доступ к ИСПДн осуществляется в соответствие с документом «InCountry Identity & Access Management Standard». Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	В соответствии с документом «InCountry Identity & Access Management Standard» пользователю назначаются права, минимально необходимые для выполнения должностных обязанностей. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Требование по ограничению неуспешных попыток входа в ИСПДн установлено документом «InCountry Identity & Access Management Standard». Блокировка учетных записей пользователей осуществляется после 5 неуспешных попыток входа в информационную систему. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».

УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу	Требование по блокированию сеанса доступа в ИСПДн установлено документом «InCountry Identity & Access Management Standard». Сеансы пользователя ограничены по времени и прекращаются после установленного времени бездействия или по запросу пользователя. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Все действия пользователя в корпоративных системах требуют предварительной аутентификации пользователя. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Удаленный доступ пользователей к ИСПДн осуществляется с использованием средства защиты информации при передаче по каналам связи.
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	Использование беспроводного устройства контролируется и регулируется такими документами, как «InCountry Corporate Device Security Standard» и «Acceptable Use Policy».
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Использование мобильных устройств контролируется и регулируется такими документами, как «InCountry Corporate Device Security Standard» и «BYOD Policy».
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Регулируется взаимодействие пользователей с информационными системами внешних организаций. Только одобренные внешние системы могут использоваться для обработки или хранения непубличных корпоративных данных. Договор с ООО «Яндекс.Облако».
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	На уровне физического оборудования платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Выполняется согласование состава устанавливаемых пакетов при обновлении ПО. В рамках релиза невозможно установить версию пакета, кроме согласованной. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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 платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗНИ.2	Управление доступом к машинным носителям персональных данных	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».

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 платформы виртуализации – выполняется ООО «Яндекс.Облако».
Регистрация событий безопасности (РСБ)		
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Перечень событий безопасности, подлежащих регистрации в ИСПДн, а также сроки хранения журналов аудита событий установлены документом «Logging and Monitoring Standard». Ведение журнала событий безопасности настроено для всех систем в рабочей среде. Zabbix, Threat Stack, ElastAlert генерируют оповещения по инцидентам и направляют их в Opsgenie – платформу управления инцидентами. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Документом «Logging and Monitoring Standard» определен состав информации о регистрируемых событиях безопасности в ИСПДн. Все журналы событий безопасности содержат такую информацию, как время, идентификатор пользователя и описание события. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Требования по сбору и хранению информации о событиях информационной безопасности в ИСПДн установлены документом «Deletion and Retention Policy». Сбор и хранение информации о событиях информационной безопасности осуществляется на уровне ОС, ППО, СУБД и СЗИ. Zabbix, Threat Stack, ElastAlert генерируют оповещения по инцидентам и направляют их в Opsgenie – платформу управления инцидентами. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Применяется SIEM. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
РСБ.7	Защита информации о событиях безопасности	Все события безопасности защищены от несанкционированного доступа и модификации. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Используется антивирусное ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Используется антивирусное ПО. Антивирусные базы регулярно обновляются. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».

Обнаружение вторжений (СОВ)		
СОВ.1	Обнаружение вторжений	Применяется HIDS Threat Stack. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
СОВ.2	Обновление базы решающих правил	
Контроль (анализ) защищенности персональных данных (АНЗ)		
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	Осуществляется регулярное сканирование уязвимостей. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Контроль установки обновлений прикладного ПО, системного ПО и СЗИ в Компании осуществляется в соответствии с документом «InCountry Change Management Standard». Осуществляется регулярное сканирование уязвимостей. Все изменения в производственных системах проходят через формальный процесс управления изменениями, который включает проверку и повторное тестирование. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется в соответствии с документом «InCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Контроль состава технических средств, программного обеспечения и средств защиты информации осуществляется в соответствии с документом «InCountry Change Management Standard». В производственных системах устанавливается только одобренное программное обеспечение. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	Настроены парольные политики. Проводится периодический аудит ИБ. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
Обеспечение целостности информационной системы и персональных данных (ОЦЛ)		
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Применяются средства контроля целостности на виртуальных серверах Платформы. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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 Платформы не входит функционал по обмену электронной почтой.

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	Осуществляется автоматизированный мониторинг работоспособности Платформы. Выполняется резервное копирование, при необходимости данные восстанавливаются из резервных копий. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Все сотрудники, имеющие доступ к данным клиентов (включая администраторов), проходят проверку подлинности с помощью MFA. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Всем пользователям предоставляется доступ к системам и информации по мере необходимости, и доступ отменяется, когда в нем больше нет необходимости. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Ведение журнала событий безопасности настроено для всех систем в производственной среде. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Для производственных систем реализована антивирусная защита. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	У каждого клиента есть выделенное отдельное пространство для хранения его данных (например, отдельный сервер или экземпляр БД). На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».

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	Выполняется ООО «Яндекс.Облако».
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Выполняется ООО «Яндекс.Облако».
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Пользователи не обладают административными привилегиями в рамках Платформы. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Удаленный доступ пользователей к ИСПДн осуществляется с использованием средства защиты информации при передаче по каналам связи. При передаче информации по внешним каналам она защищена от раскрытия и не передается в открытом виде. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	Удаленный доступ пользователей к ИСПДн осуществляется с использованием средства защиты информации при передаче по каналам связи. При передаче информации по внешним каналам она защищена от раскрытия и не передается в открытом виде. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	Права пользователей Платформы ограничены. Применяются средства контроля целостности на виртуальных серверах Платформы. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Осуществляется сегментирование и фильтрация траффика внутри сети. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Использование беспроводного устройства контролируется и регулируется документом «InCountry Corporate Device Security Standard».

Выявление инцидентов и реагирование на них (ИНЦ)		
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Управление инцидентами ИБ осуществляется в соответствии с документами: «Data Breach Notification Policy», «Security Incident Classification Matrix», «Security Incident Communication Plan», «Security Incident Response Plan». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	
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	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных, осуществляется в соответствии с документом «InCountry Change Management Standard». Только Operations Team имеет право вносить изменения в производственные системы. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных	Управление изменениями конфигурации информационной системы и системы защиты персональных данных осуществляется в соответствии с документом «InCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
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	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на предмет обеспечения защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных, осуществляется в соответствии с документом «InCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных осуществляется в соответствии с документом «InCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако».