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 InCountry's data residency-as-a-service platform**

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

оборудование которой располагается в ЦОД сервис-провайдеров ООО «Яндекс.Облако» и ООО «Селектел».

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 InCountry's data residency-as-a-service platform 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:

3-й уровень защищенности ПДн.

Краткое описание защитных мер, исполнение которых позволит выполнить требования законодательства РФ по защите персональных данных в ИСПДн InCountry's data residency-as-a-service platform приведено в Приложении 1.

Схема декларирования соответствия **на основании собственных доказательств**

В InCountry, inc приняты организационные и технические меры, обеспечивающие соответствие ИСПДн InCountry's data residency-as-a-service platform требованиям №152-ФЗ «О персональных данных» и его подзаконных актов

Дата подписания **08.09.2020**

М.П.

(Подпись)

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, которые выполняются для достижения УЗ-3 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 google На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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 пользователей. Пользователи, которым больше не требуется доступ, отключаются или удаляются. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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» Средства аутентификации, такие как пароли и ключи, хранятся безопасным способом. Утраченные или скомпрометированные средства аутентификации подлежат незамедлительной замене. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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» и ООО «Селектел».
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 google.

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
		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 отменяется, когда он больше не нужен. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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» и ООО «Селектел».
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» и ООО «Селектел».
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 Linux и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	Требование по ограничению неуспешных попыток входа в ИСПДн установлено документом «InCountry Password Protection Standard».

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
		Блокировка учетных записей пользователей должно осуществляется после 5 неуспешных попыток входа в информационную систему. Используются встроенные механизмы ОС и прикладного ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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 Password Protection 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» и ООО «Селектел».
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» и ООО «Селектел».
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 документом «Wireless Standard».
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	Использование мобильных устройств контролируется и регулируется документом «Mobile Device Standard».
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Договор с ООО «Яндекс.Облако», Договор с ООО «Селектел»
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	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
		Opsgenie – платформу управления инцидентами. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Документами «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» и ООО «Селектел».
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» и ООО «Селектел».
РСБ.7	Защита информации о событиях безопасности	Все события безопасности защищены от несанкционированного доступа и модификации. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
Антивирусная защита (АВЗ)		
АВЗ.1	Реализация антивирусной защиты	Используется антивирусное ПО. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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» и ООО «Селектел».
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» и ООО «Селектел».
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».

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
		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» и ООО «Селектел».
АН3.3	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» и ООО «Селектел».
АН3.4	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» и ООО «Селектел».
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» и ООО «Селектел».
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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	Выполняется ООО «Яндекс.Облако» и ООО «Селектел»

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
	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	Выполняется ООО «Яндекс.Облако» и ООО «Селектел»
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	Удаленный доступ пользователей к ИСПДн осуществляется с использованием средства защиты информации при передаче по каналам связи. При передаче информации по внешним каналам используется шифрование.
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	Использование беспроводного устройства контролируется и регулируется документом «Wireless Standard»
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 «nCountry Change Management Standard». Только Operations Team имеет право вносить изменения в производственные системы. На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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 «nCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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 обеспечение 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 «nCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».
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

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Защитные меры, которые выполняются для достижения УЗ-3 в ИСПДн
		документом «nCountry Change Management Standard». На уровне платформы виртуализации – выполняется ООО «Яндекс.Облако» и ООО «Селектел».