Приложение 1. Разделение ответственности за защиту персональных данных

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
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	Управление сетевым доступом на уровне: • физического оборудования Платформы; • сервисных/служебных сетей Платформы;	Управление сетевым доступом: • между сегментами клиентской виртуальной сети;

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
	системы, а также между информационными системами	• ограничение доступа между сегментами сетей различных клиентов Платформы; • ограничение доступа из клиентских сетей в сервисную/служебную сеть.	• сетевого доступа к клиентской 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

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	На уровне сервисных/служебных системных компонентов	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
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
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)			
АВЗ.1	Реализация антивирусной защиты	Не применимо, потому что защищенный сегмент содержит только серверы. Операционная система, используемая на серверах,	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
АВЗ.2	Обновление базы данных признаков вредоносных		

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
	компьютерных программ (вирусов)	практически не подвержена вирусному заражению. На серверах нет прямого доступа в Интернет.	
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)			
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 и клиентских Docker-контейнеров
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	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 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	На уровне клиентских почтовых серверов
Обеспечение доступности персональных данных (ОДТ)			

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	На уровне: • физического оборудования Платформы; • сервисных/служебных серверов Платформы и прочих виртуальных устройств. Выполняется автоматизированная репликация данных в облачном 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.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 Облака
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 инфраструктуре	Не применимо, так как в защищаемом контуре расположены исключительно серверные мощности, используются ОС практически не подверженные вирусному заражению, отсутствует прямой доступ в интернет.	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной	Управление сетевым доступом на уровне:	На уровне сегментов сети клиента

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
	инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	• сервисных/служебных сетей Платформы; • ограничение доступа между сегментами сетей различных клиентов Платформы.	
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 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	На уровне: • физического оборудования Платформы;	На уровне клиентских виртуальных машин и клиентских Docker-контейнеров

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
	изменению в процессе обработки персональных данных	• сервисных/служебных серверов Платформы и прочих виртуальных устройств.	
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 ООО «Нубес» или его подрядчиков	Из числа 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
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 ООО «Нубес» или его подрядчиков	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: • 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;	На уровне клиентской виртуальной инфраструктуры и клиентских Docker-контейнеров
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		

Источник требования	Содержание мер по обеспечению безопасности персональных данных	Встроенные защитные механизмы Платформы ООО «Виртуальные инфраструктуры»	Защитные меры, которые должны выполнить клиенты для достижения УЗ - 2
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	• Программного обеспечения Платформы.	
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		

Дата подписания **20.04.2025**

М.П.

(Подпись)

Исполнительный директор ООО «Кард Сек», И.С.Антонов

(Инициалы, фамилия)