



ООО «Селектел»
196006, Санкт-Петербург,
ул. Цветочная, д. 21, литера А

ТЕЛ./ФАКС +7 (812) 667-80-36 / 677-80-86

ИНН / ОГРН 7842393933 / 1089847357126

E-MAIL office@selectel.ru

САЙТ selectel.ru

Информационная система «VMware DaaS»

Акт оценки эффективности
принимаемых мер
по обеспечению безопасности
персональных данных
для 1-го уровня защищенности

1. ООО «Селектел» проведена оценка эффективности принимаемых мер и соответствия информационной системы «VMware DaaS» требованиям по обеспечению безопасности персональных данных, определенным в Требованиях к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и в Составе и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.
2. Технические средства информационной системы «VMware DaaS» располагаются по адресу: г. Москва, ул. Берзарина, д. 36, стр. 3.
3. Оценка эффективности принимаемых мер проведена в форме испытаний реализованных мер по обеспечению безопасности информационной системы «VMware DaaS».
4. По результатам проведения оценки эффективности принимаемых мер и соответствия информационной системы защиты требованиям по обеспечению безопасности персональных данных установлено, что информационная система «VMware DaaS» соответствует требованиям к составу и содержанию мер по обеспечению безопасности персональных данных для 1-го уровня защищенности персональных данных, а также обеспечивает защиту от актуальных угроз безопасности информации.
5. Результаты оценки действуют в течение 3 (трех) лет. При изменении структурно-функциональных характеристик информационной системы «VMware DaaS», условий ее эксплуатации, изменения требований, на соответствие которым проводилась оценка, появлении новых актуальных угроз безопасности информации проводится повторная оценка.
6. Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «VMware DaaS» и размещаемых на ее базе информационных систем, выполнение требований законодательства – совместная ответственность ООО «Селектел» и клиентов. Разграничение зон ответственности приведено в Приложении 1.
7. Перечень мер, на соответствие которым проводилась оценка, приведен в Приложении 2. Также указанное приложение содержит сведения о мерах, которые необходимо реализовать в клиентских информационных системах, размещаемых на базе информационной системы «VMware DaaS», для обеспечения безопасности персональных данных 1-го уровня защищенности.

Заместитель генерального директора по
разработке и эксплуатации продуктов



С.А. Пимков

31 мая 2024 г.

Разграничение зон ответственности в части обеспечения безопасности

Информационная система «VMware DaaS»

Информационная система «VMware DaaS» представляет собой распределенную вычислительную инфраструктуру, состоящую из набора инфраструктурных сервисов, предназначенную для размещения изолированных виртуальных рабочих столов (Virtual Desktop Infrastructure, VDI), используемых в том числе для обработки персональных данных до 1-го уровня защищенности включительно.

Обеспечение безопасности информации, обрабатываемой с использованием информационной системы «VMware DaaS», а также выполнение требований законодательства – совместная ответственность ООО «Селектел» и клиентов.

Разграничение ответственности между ООО «Селектел» и клиентами при пользовании сервисом «VMware DaaS» реализуется следующим образом:

1. ООО «Селектел» в общем случае отвечает за обеспечение информационной безопасности служебной инфраструктуры информационной системы «VMware DaaS» – обеспечивает физическую безопасность и отказоустойчивость оборудования, сетевую безопасность служебных сетей, безопасность платформы виртуализации и служебных серверов.
2. Клиент отвечает за обеспечение безопасности обрабатываемых на базе информационной системы «VMware DaaS» данных – обеспечивает безопасность виртуальных рабочих столов (включая операционные системы и приложения), организует управление доступом к обрабатываемым данным.

Схематично разграничение зон ответственности между ООО «Селектел» и клиентом представлено на схеме ниже (рисунок 1).



Рисунок 1 – Разграничение зон ответственности между ООО «Селектел» и клиентом

Приложение 2

Выполнение мер по обеспечению безопасности информации

Информационная система «VMware DaaS»

Выполнение мер, необходимых для обеспечения безопасности персональных данных 1-го уровня защищенности, а также для защиты от актуальных угроз безопасности, осуществляется за счет использования штатного функционала системного и прикладного программного обеспечения, входящего в состав информационной системы «VMware DaaS», а также применяемых средств защиты информации и комплекса организационных мер.

Перечень реализуемых ООО «Селектел» мер, сформированный с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, и Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21, приведен в таблице ниже. Кроме того, указанная таблица содержит перечень мер, которые необходимо реализовать в клиентских информационных системах, размещаемых на базе информационной системы «VMware DaaS», для обеспечения безопасности персональных данных 1-го уровня защищенности.

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками	Реализуется на уровне сетевого оборудования, служебных серверов и платформы виртуализации (далее при совместном упоминании - служебная инфраструктура)	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
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	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	Не применимо, т.к. внешние пользователи служебной инфраструктуры отсутствуют	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами объекта информатизации	Реализуется для служебных сетей	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование объекта информатизации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование объекта информатизации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.6	Ограничение неуспешных попыток входа в объект информатизации (доступа к объекту информатизации)	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.10	Блокирование сеанса доступа в объект информатизации после установленного времени бездействия (неактивности) пользователя или по его запросу	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
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	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
РСБ.7	Защита информации о событиях безопасности	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АВЗ.1	Реализация антивирусной защиты	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Реализуется на уровне служебных серверов	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
COB.1	Обнаружение вторжений	Реализуется на уровне служебной сети и служебных серверов	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
COB.2	Обновление базы решающих правил	Реализуется на уровне служебной сети и служебных серверов	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АНЗ.1	Выявление, анализ уязвимостей объекта информатизации и оперативное устранение вновь выявленных уязвимостей	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Реализуется на уровне служебной инфраструктуры	Не применимо, т.к. технические средства не входят в зону ответственности клиента
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Реализуется на уровне платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	Реализуется на уровне служебных серверов и платформы виртуализации	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей	Реализуется на уровне служебной сети	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента
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 объекта информатизации, в помещения и сооружения, в которых они установлены	Реализуется на уровне технических средств	Не применимо, т.к. технические средства не входят в зону ответственности клиента

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
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	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	Реализуется на уровне служебной сети	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных
ИНЦ.5	Принятие мер по устранению последствий инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	Реализуется в отношении инцидентов, возникающих на уровне дата-центра, служебных сетей и инфраструктуры	Необходимо реализовать в отношении инцидентов, возникающих на уровне клиентских приложений и данных
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Обозначение меры	Описание меры	Реализация ООО «Селектел»	Реализация клиентом
УКФ.2	Управление изменениями конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации объекта информатизации и системы защиты информации на обеспечение защиты информации и согласование изменений в конфигурации объекта информатизации с должностным лицом (работником), ответственным за обеспечение безопасности информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений
УКФ.4	Документирование информации (данных) об изменениях в конфигурации объекта информатизации и системы защиты информации	Реализуется на уровне служебной инфраструктуры	Необходимо реализовать на уровне операционной системы виртуального рабочего стола и на уровне клиентских приложений

Лист регистрации изменений

Номер редакции	Дата	Описание
1	31 мая 2024 г.	Исходный документ