МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЕДИНАЯ ЦИФРОВАЯ ПЛАТФОРМА РОССИЙСКОЙ ФЕДЕРАЦИИ «ГОСТЕХ» ДЛЯ СОЗДАНИЯ, РАЗВИТИЯ И ЭКСПЛУАТАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРЕДЪЯВЛЕНИЮ ТРЕБОВАНИЙ К ПОСТАВЩИКАМ ВЫЧИСЛИТЕЛЬНОЙ ИНФРАСТРУКТУРЫ И ОБЛАЧНЫХ ПЛАТФОРМ В ЧАСТИ ИСПОЛЬЗУЕМЫХ ИМИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Москва
2022

Содержание

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Используемые в настоящем документе термины и основные понятия в области автоматизированных систем определены в ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

Также в тексте настоящего документа используются следующие термины и сокращения:

Сокращение/Термин	Значение/Определение
ТЗКИ	Техническая защита конфиденциальной информации
ИСПДн	Информационная система персональных данных
ИТ	Информационная технология
API	Прикладной программный интерфейс
L3VPN	Тип виртуальной частной сети, в которой для передачи данных на сетевом уровне используются метки MPLS
Persistent Volumes	Часть хранилища в кластере, выделенная администратором
Cinder	Служба блочного хранилища для предоставления конечным пользователям соответствующих ресурсов хранения
ИБ	Информационная безопасность
ПАК ЗИ	Программно-аппаратный комплекс защиты информации
ПО	Программное обеспечение
ПУ	Подсистема управления
ПХД	Подсистема хранения данных
ПВС	Подсистема вычислительной сети
ПВР	Подсистема вычислительных ресурсов

Сокращение/Термин	Значение/Определение
ПЗИ	Подсистема защиты информации
ЦОД	Центр обработки данных
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю
Заказчик	Государственные органы, обеспечивающие создание, развитие, эксплуатацию ГИС на ЕЦП «ГосТех» и (или) использование цифровых продуктов цифровой экосистемы «ГосТех»
Контейнер	Готовый к запуску пакет программного обеспечения, содержащий все необходимое для запуска: исполняемый образ приложения и системные библиотеки, а также значения по умолчанию для существенных параметров запуска
Контейнерная оркестрация	Автоматизация и управление жизненным циклом контейнеров
Облачная платформа	Набор технологических решений, обеспечивающих предоставление вычислительных ресурсов, ресурсов хранения и сеть передачи данных, возможности гибкого управления и масштабирования за счет применения технологий виртуализации физической инфраструктуры
Сервис, Продукт	Программное обеспечение, реализующее функциональные потребности, предназначенное для функционирования в отдельном процессе и взаимодействующее с другими сервисами и сторонними приложениями с использованием стандартизированных интерфейсов. Сервисы могут быть написаны на разных языках программирования и использовать разные технологии хранения данных
Поставщик вычислительной инфраструктуры и облачных платформ	Юридическое лицо или индивидуальный предприниматель, предоставляющие вычислительную инфраструктуру, облачные платформы на ЕЦП «ГосТех»
ГИС	Государственная информационная система

2. ОБЩИЕ ПОЛОЖЕНИЯ

В настоящих методических рекомендациях перечислены основные требования к поставщикам вычислительной инфраструктуры и облачных платформ, предназначенных для формирования доверенной облачной инфраструктуры, обеспечивающей создание и эксплуатацию государственных информационных систем, создаваемых на ЕЦП «ГосТех», в части используемых ими информационных технологий и технологий обеспечения информационной безопасности.

Методические рекомендации предназначены для изучения Заказчиками ГИС, создаваемых на ЕЦП «ГосТех» и используются при формировании технических заданий на оказание услуг по предоставлению вычислительной инфраструктуры и облачных платформ применительно к конкретной ГИС Заказчика.

3. ТРЕБОВАНИЯ К ПОСТАВЩИКАМ ВЫЧИСЛИТЕЛЬНОЙ ИНФРАСТРУКТУРЫ И ОБЛАЧНЫХ ПЛАТФОРМ В ЧАСТИ ИСПОЛЬЗУЕМЫХ ИМИ ТЕХНОЛОГИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Требования к лицензированию

В соответствии с подпунктом «е» пункта 4 постановления Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» Поставщик должен иметь лицензию на деятельность по ТЗКИ, включающую разрешение на осуществление следующих видов деятельности:

услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации) – в целях организации работ по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации Заказчика.

В соответствии с пунктами 1 и 4 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного постановлением Правительства Российской Федерации от 16.04.2012 № 313 (далее – Положение), Поставщик должен иметь лицензию, включающую разрешение на осуществление видов деятельности,

соответствующих пунктам 11, 12, 13, 14, 15, 20, 22, 23, 25, 28 приложения к Положению:

изготовление с использованием шифровальных (криптографических) средств изделий, предназначенных для подтверждения прав (полномочий) доступа к информации и (или) оборудованию в информационных и телекоммуникационных системах;

монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;

монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;

работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

передача защищенных с использованием шифровальных (криптографических) средств информационных систем;

передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей;

изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

В тех случаях, когда Поставщик одновременно оказывает услуги по предоставлению вычислительной инфраструктуры и (или) облачных

платформ и услуги связи, в соответствии со статьей 29 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», Поставщик должен иметь лицензию на осуществление деятельности в области оказания услуг связи.

Применительно к ЕЦП «ГосТех» Заказчикам может быть необходимо оказание услуг связи, которые предусмотрены пунктами 13, 14 и 16 приложения № 1 к Положению о лицензировании деятельности в области оказания услуг связи, утвержденному постановлением Правительства Российской Федерации от 30.12.2020 № 2385:

услуги связи по предоставлению каналов связи;

услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;

телематические услуги связи.

3.2. Требования регуляторов в области информационной безопасности

В соответствии с пунктом 14.2 приказа ФСТЭК России от 11.02.2013 № 17 класс защищенности информационно-телекоммуникационной инфраструктуры центра обработки данных должен быть не ниже класса защищенности информационной системы, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных.

В соответствии с пунктом 17.6 приказа ФСТЭК России от 11.02.2013 № 17 в случае, если информационная система создается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных уполномоченного лица, такая инфраструктура центра обработки данных должна быть аттестована на соответствие требованиям, предусмотренным этим приказом.

В соответствии с пунктом 26 приказа ФСТЭК России от 11.02.2013 № 17 предъявляются следующие требования к используемым в инфраструктуре Поставщика средствам защиты информации:

- в информационных системах 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

- в информационных системах 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

- в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

В информационных системах 1 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В информационных системах 2 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В информационных системах 3 класса защищенности применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

В соответствии с пунктом 26.1 приказа ФСТЭК России от 11.02.2013 № 17 при проектировании вновь создаваемых или модернизируемых информационных систем, имеющих доступ к информационно-телекоммуникационной сети «Интернет», должны выбираться маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

Постановлением Правительства Российской Федерации от 16.11.2015 № 1236 введен запрет на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

Постановлением Правительства Российской Федерации от 30.04.2020 № 616 введен запрет на допуск промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд.

В целях обеспечения защиты обрабатываемых в ГИС на ЕЦП «ГосТех» персональных данных к инфраструктуре Поставщика необходимо предъявить требования по безопасности информации для информационных систем персональных данных в соответствии с установленным уровнем защищенности персональных данных. При этом необходимо учитывать, что уровень защищенности персональных данных не может быть выше класса защищенности, установленного для размещаемой на инфраструктуре ГИС.

В соответствии с пунктом 16 постановления Правительства Российской Федерации от 01.11.2012 № 1119 при обработке в ГИС на ЕЦП «ГосТех» требуется наличие структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

3.3. Требования к резервированию и катастрофоустойчивости

Технологическая платформа ЕЦП «ГосТех» должна развертываться исключительно на геораспределенной инфраструктуре. Для обеспечения возможности построения геораспределенной инфраструктуры у Поставщика должно быть не менее 3 (трех) территориально разнесенных ЦОД, 2 (два) из которых должны быть разнесены между собой на расстояние не менее 20 км. Третий (резервный) ЦОД должен быть отнесен от остальных ЦОД на расстояние не менее 100 км для обеспечения георезервирования.

Каналы связи между ЦОД Поставщика должны быть защищены средствами, реализующими алгоритмы криптографического преобразования информации, прошедшими проверку соответствия в форме сертификации.

Инфраструктура Поставщика должна обеспечивать бесперебойное функционирование и сохранность информации, обрабатываемой на вычислительных и технологических ресурсах, в следующих аварийных ситуациях:

- полное отключение электроэнергии;
- нарушение функционирования или выход из строя каналов связи;
- полный или частичный отказ технических средств, включая, в том числе сбои и отказы накопителей на жестких магнитных дисках;
- сбой в функционировании общего и (или) специального программного обеспечения.

В целях обеспечения надлежащего уровня надежности и отказоустойчивости Поставщиком должны обеспечиваться:

- необходимый уровень резервирования технических средств инфраструктуры, достаточный в случае отказа основных технических средств, для функционирования ИС в полном объеме с возможностью автоматического переключения на резервные технические средства;
- возможность организации автоматического и ручного резервного копирования данных с вычислительных и телекоммуникационных средств и общесистемного программного обеспечения, включая возможность проверки целостности резервных копий;
- автоматическое выявление недоступности или снижения показателей производительности;
- автоматическое оповещение технических служб и обслуживающего персонала о сбоях в работе технических средств, а также о снижении качества работы выделенных ресурсов и служб.
- резервирование каналов передачи информации, средств обеспечения функционирования вычислительной инфраструктуры.

Резервирование каналов передачи информации включает:

- резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к вычислительной инфраструктуре;

- наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) вычислительной инфраструктуры планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления.

Резервирование средств обеспечения функционирования вычислительной инфраструктуры включает:

- использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента информационной системы (технического средства, устройства) в случае отключения основного источника питания;

- использование долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения сегментом информационной системы (техническим средством, устройством) установленных функциональных (задач);

- определение перечня энергозависимых технических средств, которым необходимо обеспечить наличие резервных источников питания (кратковременных и долговременных).

3.4. Иные требования

ЦОД Поставщика должен по крайней мере соответствовать следующим основным требованиям, предъявляемым к центрам обработки данных:

– возможность обслуживания без остановки оборудования;

– присутствие в дежурной смене не менее 1 квалифицированного сотрудника в режиме 24x7;

– надлежащие разрешения и допуск у персонала в соответствии с требованиями государственных нормативных документов;

– работающий посменно персонал с надлежащей квалификацией для определенных операций смены, выполняемых в индивидуальном порядке или сменной бригадой;

– интегрированный подход к управлению эксплуатацией, охватывающий все аспекты работы центра обработки данных (эксплуатация, ИТ, ИБ);

– целевая доступность оказываемых услуг не менее 99,982 %;

– наличие комплексной системы автоматического пожаротушения, включающей системы раннего оповещения, противодымной вентиляции, установки газового пожаротушения;

– основная система сигнализации должна быть выполнена на основе адресно-аналогового оборудования;

– резервирование всех элементов инфраструктуры, оказывающих влияние на доступность оказываемых услуг;

– наличие двух полностью независимых источников бесперебойного питания, включая дизельно-генераторную систему;

– наличие круглосуточной физической охраны, комбинированного контроля доступа и удаленного видеонаблюдения;

– использование промышленных систем охлаждения и кондиционирования с резервированием, а также систем контроля температурно–влажностного режима в серверных залах;

– периодические проверки отказоустойчивости и работоспособности всех элементов инфраструктуры, включая резервные;

– наличие нескольких независимых энерговводов не ниже 2 категории;

– распределенное резервирование каналов связи.

Поставщик должен обеспечить мониторинг предоставляемых вычислительных ресурсов и ресурсов хранения данных. Мониторинг предоставляемых вычислительных ресурсов и ресурсов хранения данных должен обеспечиваться средствами системы мониторинга информационно-технологической инфраструктуры Поставщика.

Должны быть предоставлены основной и резервные каналы связи для организации подключения между ЦОД на 3 (третьем) уровне модели OSI.

Каналы L3VPN должны быть организованы в соответствии с требованиями по защите информации. Все применяемые средства криптографической защиты информации должны соответствовать требованиям ФСБ России.

Поставщик должен обеспечивать контроль и анализ защищенности инфраструктуры с использованием специализированных средств по выявлению уязвимостей в используемом ПО и его некорректной конфигурации, влияющей на уровень защищенности, с устранением выявленных уязвимостей и (или) недостатков.

3.5. Требования для оператора связи к режиму доступа

В соответствии с пунктом 5 приказа Мининформсвязи Российской Федерации от 09.01.2008 № 1 Поставщиком должны обеспечиваться следующие мероприятия по защите от доступа со стороны физических лиц, не имеющих на это право:

- оснащение сооружений связи, в которых размещаются узлы связи, техническими средствами защиты, включая охранную сигнализацию;
- наличие ограждений, исключающих случайный проход физических лиц и въезд транспорта на охраняемую территорию;
- организация контрольно-пропускного режима как на охраняемой территории, так и внутри сооружений связи;
- оборудование распределительных кабельных шкафов запирающими устройствами и датчиками охранной сигнализации о несанкционированном доступе;
- регистрация и последующий контроль действий обслуживающего персонала в процессе эксплуатации узлов связи в соответствии с установленным порядком доступа к средствам и линиям связи.

В соответствии с пунктом 12 этого же приказа Мининформсвязи Российской Федерации события, связанные с несанкционированным доступом к сетям связи и передаваемой посредством их информации, регистрируются документально и заверяются подписью должностного лица, зарегистрировавшего это событие.

В соответствии с пунктом 3 приказа Минкомсвязи России от 04.04.2016 № 135 сторонняя организация обязана ежеквартально представлять оператору связи сведения об иностранных организациях и иностранных гражданах, привлекаемых к оказанию услуг связи.

В соответствии с пунктом 5 этого же приказа Минкомсвязи России оператор связи ежеквартально направляет в территориальный орган ФСБ России имеющиеся сведения об иностранных организациях и иностранных гражданах (лицах без гражданства), привлекаемых к оказанию услуг и (или) выполнению работ, связанных с эксплуатацией и (или) управлением его сетью связи.

В соответствии с пунктом 8 этого же приказа Минкомсвязи России оператор связи хранит в течение трех лет информацию о всех действиях со средствами связи, выполненных обслуживающим персоналом оператора связи или привлеченными лицами в процессе эксплуатации и (или) управления сетью связи как с рабочих мест, так и с использованием удаленного доступа.

4. ТРЕБОВАНИЯ К ПОСТАВЩИКАМ ВЫЧИСЛИТЕЛЬНОЙ ИНФРАСТРУКТУРЫ И ОБЛАЧНЫХ ПЛАТФОРМ В ЧАСТИ ИСПОЛЬЗУЕМЫХ ИМИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

4.1. Общие требования

В соответствии со Стандартом по управлению динамической инфраструктурой единой цифровой платформы «ГосТех», утвержденным протоколом заочного голосования членов президиума Правительственной Комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 08.12.2022 №54, облачная платформа Поставщика должна быть сертифицирована ФСТЭК России, а также все каналы связи, выходящие за пределы контролируемой зоны, должны быть защищены средствами криптографической защиты информации, прошедшими установленным порядком процедуру оценки соответствия требованиям ФСБ России, класс которых определен в модели угроз безопасности информации.

Поставщик в рамках предоставления облачных платформ должен также предоставить общесистемное и прикладное программное обеспечение, в том числе ПО платформы виртуализации, а также ПО или ПАК ЗИ (и, при необходимости, право на его использование).

Использование указанного ПО должно быть разрешено лицензиаром на всей территории Российской Федерации. Условия использования ПО указываются в соответствующем лицензионном (пользовательском) соглашении правообладателя соответствующего ПО.

Программное обеспечение (ПО) с открытым исходным кодом, в случае его использования в составе облачной платформы, должно быть размещено в национальном репозитории открытого кода (с момента ввода репозитория в эксплуатацию) и доступно для Поставщиков облачной платформы.

При этом Поставщиком облачной платформы должны выполняться следующие требования:

- ПО, предполагаемое к использованию в составе облачной платформы, должно быть размещено в локальном репозитории Поставщика, защищенном от внешнего воздействия, в котором осуществляется анализ компонентов на наличие известных уязвимостей, проводится контроль целостности, а также антивирусный и контекстный контроль содержимого;
- сборка компонентов облачной платформы должна проводиться в локальном и изолированном сборщике;

- Поставщик также осуществляет анализ компонентов на наличие известных уязвимостей, функциональное тестирование, антивирусный и контекстный контроль. При этом в составе облачной платформы должны отсутствовать компоненты с лицензиями, ограничивающими их использование на платформе «ГосТех»;

- должно осуществляться документирование процесса поддержки жизненного цикла ПО, в том числе процедуры поставки, идентификация мер безопасности, поддержка производства, процедуры приемки и автоматизации.

Вместе с тем Поставщик обязан предоставить документацию, подтверждающую применение технологий разработки безопасного программного обеспечения (в соответствии с ГОСТ Р 56939-2016) и соблюдения требований к компонентам доверия к безопасности (в соответствии с ГОСТ Р ИСО/МЭК 15308-3-2013), а также согласованные ФСТЭК России и ФСБ России модели угроз и нарушителя безопасности информации.

Поставщик обязан:

1) предоставить вычислительные ресурсы, управляемые ПО из единого реестра российских программ для электронных вычислительных машин и баз данных, отнесённого к классу «Средства обеспечения облачных и распределенных вычислений, средства виртуализации и системам хранения данных»;

2) предоставить Заказчику доступ к необходимой информации (копиям журналов регистрации событий) и иные необходимые полномочия, требуемые Заказчику для выявления инцидентов в отношении ИС Заказчика, размещаемых в ЦОД Поставщика, и реагирование на них;

3) предоставить Заказчику возможность контроля (мониторинга) на уровне инфраструктуры за обеспечением уровня защищенности информации, содержащейся в ГИС на ЕЦП «ГосТех»;

4) обеспечить мониторинг и устранение технических сбоев при предоставлении Сервисов;

5) осуществлять мониторинг производительности Сервисов;

6) вести журнал сбоев в Сервисах с фиксацией времени обнаружения сбоя и времени, затраченного на восстановление Сервисов;

7) обеспечить мониторинг и устранение технических сбоев инфраструктуры (в том числе, но не ограничиваясь, серверов, ПХД, сетевого оборудования, систем виртуализации) при предоставлении Сервисов;

8) обеспечить автоматическое оповещение (по электронной почте) уполномоченных лиц Заказчика в случае наступления нештатной ситуации (сбои

оборудования, каналов связи, системного ПО, и прочее).

4.2. Требования к архитектуре облачной платформы Поставщика

В состав облачной платформы Поставщика должны входить следующие подсистемы:

- подсистема управления (ПУ);
- подсистема вычислительных ресурсов (ПВР);
- подсистема хранения данных (ПХД);
- подсистемы вычислительной сети (ПВС);
- подсистема защиты информации (ПЗИ).

Облачная платформа должна строиться на базе программного обеспечения собственной разработки Поставщика, включенного в единый реестр российских программ для электронных вычислительных машин и баз данных, либо на базе ПО с открытым исходным кодом. Специалисты, выполняющие работы по поддержке облачной платформы, должны обладать необходимой квалификацией работы с операционными системами семейства Linux.

4.2.1. Требования к ПУ

ПУ должна предоставлять графический пользовательский интерфейс, позволяющий взаимодействовать со всеми остальными подсистемами, предоставлять доступ к прикладному программному интерфейсу (API).

ПУ должна обладать:

- панелью, позволяющей оперативно управлять сервисами посредством пользовательского интерфейса;
- расширенной панелью управления, предоставляющей доступ к расширенным настройкам и функционалу для технических специалистов посредством пользовательского интерфейса;
- прикладным программным интерфейсом.

ПУ должна обеспечивать выполнение следующих функций:

- предоставление пользовательского интерфейса;
- аутентификация и авторизация пользователей, в том числе, на базе ролевой модели;
- двухфакторная аутентификация пользователей;
- поддержка возможности управления несколькими инсталляциями Платформы в рамках одной учетной записи администратора;

- запуск вычислительных ресурсов с предустановленными на этих вычислительных ресурсах шаблонов прикладного ПО и различных ОС.

4.2.2. Требования к ПВР

ПВР должна обеспечивать управление гипервизорами, жизненным циклом виртуальных машин (ВМ).

ПВР должна обеспечивать выполнение следующих функций:

- создание, конфигурирование и удаление ВМ;
- создание и управление кластерами контейнерной оркестрации;
- создание и управление кластерами больших данных;
- перемещение ВМ между серверами виртуализации и между ЦОД Поставщика с простоем (downtime) не более 10 (десяти) минут;
- подключение и отключение томов ПХД к ВМ;
- отслеживание ресурсных квот для ВМ (групп ВМ);
- стандартизация ВМ;
- предоставление API;
- возможность управления инфраструктурой из специализированных программных средств, включая: инструменты описания серверной инфраструктуры в виде кода, инструменты написания сценариев автоматизации управления инфраструктурой, инструменты управления кластером контейнеров Linux;
- взаимодействие со смежными системами (компонентами).

Средства оркестрации должны поддерживать следующую функциональность:

- создание кластеров как посредством веб-интерфейса, так и с помощью REST API;
- встроенный Cinder Persistent Volume Provisioner;
- хранение Persistent Volumes на ПХД или же SDS для увеличения отказоустойчивости;
- интеграция с Load Balancer с поддержкой Proxy Protocol;
- предустановленный Ingress Controller, интегрированный с Load Balancer;
- масштабирование количества узлов (node) кластера с помощью API и веб-интерфейса;
- обновление версию кластера с помощью веб-интерфейса и REST-API (поддержка как минорных, так и мажорных обновлений);
- поддержка режима развертывания master и node-серверов в нескольких зонах доступности с гарантированным распределением ВМ между ними для обеспечения высокой доступности;

- поддержка horizontal pod autoscaler;
- предустановленный docker registry;
- создание конфигурации multi-master (3, 5, 7 мастеров);
- доступ к API-серверу через Load Balancer в режиме multi-master;
- интеграция с системой резервного копирования в S3-совместимое объектное хранилище, поддержка резервного копирования кластера целиком, или конкретного namespace, поддержка резервирования данных на persistent volumes;
- поддержка RWX persistent volumes, наличие встроенного сервиса, предоставляющего высокодоступные RWX-хранилища, подключаемые по протоколу NFS;
- поддержка создания кластера в частной сети;
- возможность организации VPN-соединения между кластером системы и инфраструктурой Заказчика;
- поддержка CRUD-операций для кластеров посредством REST API и веб-интерфейса;
- интегрированная система мониторинга;
- поддержка Istio service mesh и объединения кластеров в единую сущность;
- поддержка Calico v3 network driver;
- поддержка нулевой тарификации за RAM и CPU для остановленных ВМ;
- предустановленный CoreDNS.

4.2.3. Требования к ПХД

ПХД должна обеспечивать управление и интеграцию аппаратных и программных систем хранения данных, а также должна предоставлять ресурсы хранения данных по запросу других подсистем.

ПХД должна обеспечивать выполнение следующих функций:

- автоматическая репликация данных в не менее, чем 2 (два) ЦОД;
- создание, конфигурирование и удаление логических дисков;
- создание снимков;
- создание, хранение и удаление образов;
- отслеживание ресурсных квот;

ПХД должна обеспечивать работу следующих типов хранения данных:

- S3-совместимое (API) объектное хранилище;
- блочное и файловое хранилище.

4.2.4. Требования к ПВС

ПВС должна обеспечивать управление пулом сетевых ресурсов (сети, виртуальные сети, пулы IP-адресов, маршрутизаторы, сетевые сервисы и др.), создавать виртуальные сетевые элементы по запросу других подсистем.

ПВС должна обеспечивать выполнение следующих функций:

- управление пулами IP-адресов;
- управление IP-адресами (создание, освобождение) в рамках выбранной сети, доступной для региона, в котором работает ВМ;
- создание защищенного периметра сети передачи данных;
- создание, конфигурирование и удаление виртуальных маршрутизаторов, балансировщиков нагрузки, сетей и подсетей.

4.2.5. Требования к ПЗИ

ПЗИ должна включать функции, направленные на реализацию мер защиты информации, предусмотренных Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17.

При этом функциональные компоненты ПЗИ должны быть сертифицированы ФСТЭК России и ФСБ России по требованиям безопасности информации.