

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего профессионального образования
«Уральский федеральный университет
имени первого Президента России Б.Н.Ельцина»

418/03

ПРИКАЗ
Екатеринбург

04.06.2015.

О вводе в промышленную эксплуатацию сервиса предоставления вычислительных ресурсов

В связи с успешным завершением этапа опытно-промышленной эксплуатации сервиса предоставления вычислительных ресурсов, реализованного в рамках проекта 4.1.2.4-14 «Внедрение системы управления виртуальной вычислительной инфраструктурой на базе технологий Local Cloud» мероприятия 4.1 «Модернизация ИТ-инфраструктуры» Программы развития УрФУ,

ПРИКАЗЫВАЮ:

1. Ввести в промышленную эксплуатацию сервис предоставления вычислительных ресурсов в Уральском федеральном университете с 08 июня 2015 года.
2. Ввести в действие утвержденное Положение об использовании сервиса предоставления вычислительных ресурсов на основе технологий частного облака Уральского федерального университета имени первого Президента России Б.Н. Ельцина (Приложение 1) с 08 июня 2015 года.
3. Ввести в действие утвержденный Регламент предоставления вычислительных ресурсов на основе технологий частного облака Уральского федерального университета имени первого Президента России Б.Н. Ельцина (Приложение 2) с 08 июня 2015 года.
4. Директору по информационным технологиям Богданович И.А. в срок до 11 июня 2015 года:
 - 4.1. организовать техническое сопровождение и обслуживание указанного сервиса.
 - 4.2. подготовить обоснование необходимых затрат на лицензионное и техническое обеспечение сервиса предоставления вычислительных ресурсов к началу процесса формирования бюджета 2016 года.
5. Контроль за исполнением приказа возложить на проректора по экономике и стратегическому развитию Сандлера Д. Г.

Ректор



В.А. Кокшаров

Исполнитель:
И.С. Заложных

Приложение 1

к приказу ректора

от 04.06.2015. № 418/03

УТВЕРЖДАЮ

Ректор

Уральского федерального университета
имени первого Президента России

Б.Н. Ельцина


В.А. Кокшаров

03» июня 2015 года



ПОЛОЖЕНИЕ

**об использовании сервиса предоставления вычислительных ресурсов на
основе технологий частного облака Уральского федерального университета
имени первого Президента России Б.Н. Ельцина**

Екатеринбург, 2015г.

Содержание

1. Термины и сокращения.....	3
2. Основные положения.....	4
3. Возможности и особенности сервиса предоставления вычислительных ресурсов....	5
4. Порядок предоставления сервиса	6
5. Качество предоставления сервиса (SLA).....	7
6. Пул вычислительных ресурсов	8
7. Права и обязанности пользователей сервиса	8
8. Порядок ввода в действие, внесения изменений и информирования.....	10

1. Термины и сокращения

В настоящем Положении используются следующие основные понятия и сокращения:

УрФУ	Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
ДИТ	Дирекция информационных технологий УрФУ
УИБ	Управление информационной безопасности УрФУ
ПО	Программное обеспечение
ОС	Операционная система
Гостевая ОС	Операционная система, устанавливаемая на виртуальную машину
AT.URFU.RU AD Единый каталог	Единый каталог пользователей и информационных ресурсов УрФУ, построенный на базе технологии Microsoft™ Active Directory. Включает в себя домен Active Directory «at.urfu.ru», лес Active Directory «at.urfu.ru», DNS-зону «at.urfu.ru» дочерние DNS-зоны в зоне «at.urfu.ru», а также несколько обратных DNS-зон.
Корпоративная почта	Набор из почтовых систем для пересылки и хранения электронной почты, обслуживающий почтовые домены «urfu.ru», «usu.ru» и «ustu.ru» и сопровождаемый отделом базовых сервисов.
Подразделение	Структурное подразделение университета, соответствующее принятой организационно-штатной структуре университета. В качестве Подразделения могут выступать управление, центр, отдел, институт, департамент, кафедра, лаборатория, сектор и иные организационные единицы.
Общедоступные сетевые сервисы	Сервисы, которые обеспечивают подключение клиентов к сети (DHCP), службе каталогов, разрешению адресов (система доменных имён, англ. DNS)
Аутентификация	Процедура проверки подлинности пользователя путём сравнения введённого им пароля с паролем в базе данных пользователей.
Авторизация	Предоставление пользователю прав доступа к информационным ресурсам и прав на выполнение определённых действий в каталоге.
ПО	Программное обеспечение.
Вредоносное ПО	ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности или доступности информации.
Учетная запись	Учетная запись пользователя в едином каталоге пользователей AT.URFU.RU. Включает Имя учётной записи, Пароль и ряд других атрибутов.
Облачные вычисления	Возможность получения необходимых вычислительных мощностей по запросу из сети, при этом пользователю не важны детали реализации этого механизма, и он получает из этого "облака" все

	необходимое.
Виртуализация	Абстракция вычислительных ресурсов и предоставление пользователю системы, которая "инкапсулирует" (скрывает в себе) собственную реализацию.
Local Cloud, Частное облако	Физически или логически выделенный пул вычислительных ресурсов с возможностью создания различных конфигураций ИТ-инфраструктуры. Реализация модели облачных вычислений на имеющихся у университета компьютерных ресурсах.
Вычислительные ресурсы	Набор из объема оперативной памяти, места на диске, процессорных ядер, сетевого адаптера, а также иного программно-аппаратного обеспечения, формирующих аппаратное обеспечение сервера.
Пул вычислительных ресурсов	Группа унифицированного, однородного и однотипного коммуникационного и серверного оборудования, поддерживаемая ДИТ и размещенная в ЦОДах или серверных помещениях УрФУ, из которого выделяются вычислительные ресурсы по запросу подразделений в рамках сервиса предоставления вычислительных ресурсов.
Вычислительные мощности	Набор серверного оборудования и систем хранения данных, из которых составляется пул вычислительных ресурсов.
Корпоративная сеть	Корпоративная сеть УрФУ, включающая в себя коммуникационное аппаратное и коммуникационное программное обеспечение.
Администратор приложения	Администратор приложения – представитель Заказчика, выполняющий определённые функции согласно данному положению.

2. Основные положения

2.1 Целью настоящего Положения является описание сервиса предоставления вычислительных ресурсов на основе технологий «Local Cloud», порядка предоставления сервиса, прав и обязанностей пользователей, а также уровней обслуживания для пользователей данной услуги.

2.2 УрФУ проводит единую централизованную политику по управлению вычислительными ресурсами. Для обеспечения высокой надежности информационных сервисов подразделениям следует размещать вычислительные ресурсы в пуле вычислительных ресурсов УрФУ.

2.3 «Local Cloud» – это группа высокопроизводительных серверов, систем хранения данных и сетевого оборудования, размещенных в ЦОДах или серверных помещениях ДИТ и работающих как единая система для предоставления высокой доступности сервисов и приложений конечным пользователям. Облачная платформа УрФУ характеризуется высокой надежностью, производительностью и гибким масштабированием, что достигается путем дублирования всех критически важных для работы компонентов и за счет распределения нагрузки между узлами (серверами) кластера.

2.4 Сервис предоставления вычислительных ресурсов, именуемый также в дальнейшем «Хостинг», предоставляется дирекцией информационных технологий подразделениям, сотрудникам или преподавателям УрФУ, именуемым в дальнейшем «Пользователь».

2.5 Сервис предоставления вычислительных ресурсов (хостинга) обеспечивает возможность размещения информационных систем и сервисов с целью обеспечения учебного процесса, научных исследований, международного сотрудничества и иной образовательной или административной деятельности университета.

2.6 Сервис предоставления вычислительных ресурсов осуществляется посредством предоставления Пользователю физических серверов и виртуальных машин, управляемых средствами портала самообслуживания.

2.7 В развитие настоящего Положения могут создаваться обязательные для исполнения пользователями сервиса технологические регламенты и иные технические условия, прочие частные регламенты, инструкции и нормы регулирования по использованию сервиса предоставления вычислительных ресурсов в особых случаях.

3. Возможности и особенности сервиса предоставления вычислительных ресурсов

3.1 Достоинством использования настоящего сервиса для Пользователя является высокая доступность серверов, возможность создания и восстановления мгновенных снимков виртуальных машин, возможность масштабирования (увеличение объема оперативной памяти и жесткого диска, а также числа вычислительных ядер) при возрастании потребностей прикладной системы.

3.2 Пользователь имеет возможность управлять сервером (включить, выключить, перезагрузить, оперативно восстанавливать работу сервера и прикладной системы), а также предоставить доступ к серверу другому пользователю.

3.3 Высокая доступность ресурсов «частного облака» обеспечивается в случае сбоя одного из серверов или выхода из строя части коммутационного оборудования за счет перемещения служб или приложений между узлами облака. Для пользователей сервиса кластер выглядит как единое целое, и его неполадки могут выразиться в кратковременном снижении производительности или недоступности какого-либо ресурса на время от нескольких секунд до нескольких минут.

3.4 Пользователь может оперативно получать необходимые вычислительные ресурсы без необходимости администрировать и поддерживать инфраструктуру (ЦОД, серверные помещения, системы кондиционирования и охлаждения, систему бесперебойного питания, сетевую инфраструктуру, физические сервера и гипервизоры). Пользователь при использовании сервиса продолжает администрировать ОС и прикладные сервисы.

3.5 Сервис предоставления вычислительных ресурсов интегрирован с иными базовыми сервисами корпоративной сети УрФУ: сервис доступа в корпоративную сеть, сервисы единого каталога пользователей, почтовая система, сервис предоставления сетевых настроек DHCP, сервис регистрации разрешения имен DNS, сервис инфраструктуры открытых ключей PKI, сервис точного времени NTP, сервис обновления ПО Microsoft WSUS и сервис активации и управлению ключами KMS.

3.6 Для получения доступа ко всем возможностям сервиса предоставления вычислительных ресурсов персональные компьютеры и сервера пользователей и подразделений должны иметь адресацию согласно «Положению об использовании адресации интернет протокола версии 4 в сети Уральского федерального университета имени первого Президента России Б.Н. Ельцина».

3.7 Доступ к ряду возможностей хостинга для пользователей, компьютеров, серверов или иных устройств, не имеющих адресацию согласно указанному выше Положению, может быть ограничен или невозможен.

3.8 Для получения доступа ко всем возможностям хостинга персональные компьютеры пользователей и подразделений должны быть присоединены к домену AT.URFU.RU, а подразделение должно иметь назначенного Администратора подразделения в едином каталоге пользователей, выполняющего функции администрирования компьютеров и раздела подразделения в едином каталоге пользователей, в соответствии с «Регламентом администрирования единого каталога пользователей Active Directory AT.URFU.RU».

3.9 Доступ к ряду возможностей хостинга для пользователей с компьютеров и устройств, не присоединенных к домену «AT.URFU.RU», может быть ограничен или невозможен.

4. Порядок предоставления сервиса

4.1 Руководитель подразделения, запрашивающего сервис предоставления вычислительных мощностей должен назначить Администратора приложения, согласно форме, описанной в Регламенте предоставления вычислительных ресурсов.

4.2 Сервис хостинга при отсутствии назначенного Администратора приложений не предоставляется.

4.3 Для получения ресурсов и виртуальных серверов в «частном облаке» УрФУ институтам и структурным подразделениям университета необходимо заполнить мотивированную Заявку в форме служебной записки на имя директора по информационным технологиям на предоставление сервиса согласно регламенту предоставления вычислительных ресурсов.

4.4 Предоставление вычислительных ресурсов Пользователю осуществляется после согласования с ДИТ параметров и объемов предоставляемых вычислительных ресурсов, согласования с УИБ целей использования предоставляемых вычислительных ресурсов, а также содержания и целевой группы потребителей информационных ресурсов, на основании решения, принятого директором по информационным технологиям.

4.5 Предоставление вычислительных ресурсов осуществляется только при наличии достаточного объема свободных и незарезервированных ресурсов в пуле вычислительных ресурсов, сопровождаемых Дирекцией ИТ. Предоставление вычислительных ресурсов осуществляется только для обеспечения выполнения основной деятельности УрФУ, не связанной с обработкой персональных данных, информацией ограниченного распространения или сведениями, составляющими коммерческую тайну.

4.6 По факту исполнения полученной Заявки ДИТ оповещает Администратора приложений о готовности использования выделенных вычислительных ресурсов и предоставляет ему необходимую информацию и реквизиты для использования сервиса.

4.7 Администратор приложений самостоятельно создает необходимые ему виртуальные машины (при необходимости используя предоставленные шаблоны) с согласованными параметрами.

4.8 Администратор приложений при необходимости самостоятельно настраивает ОС на аппаратном или виртуализованном аппаратном обеспечении внутри предоставленных ему вычислительных ресурсов.

4.9 На одной виртуальной машине допускается размещение не более одного сервиса или не более одной информационной системы.

4.10 ДИТ осуществляет консультирование Администратора приложений.

4.11 ДИТ оставляет за собой право отказать в предоставлении сервиса хостинга Пользователю в случае невозможности выделения вычислительных ресурсов запрошенного объема.

4.12 УИБ/ДИТ оставляет за собой право отказать в предоставлении сервиса хостинга Пользователю в случае, если размещаемые данные содержат информацию ограниченного распространения.

5. Качество предоставления сервиса (SLA)

5.1 Часы работы: работоспособность сервиса обеспечивается 24 часа в сутки 7 дней в неделю 365 дней в году, за исключением случаев проведения запланированных профилактических работ на инфраструктуре пула вычислительных ресурсов.

5.2 Инфраструктура сервиса может работать в основном и аварийном режимах.

5.3 В основном режиме сервис предоставляется согласно настоящему соглашению о качестве обслуживания. В аварийном режиме возможны отклонения от соглашения о качестве обслуживания. В этом случае производительность виртуальных машин и предоставляемые Заказчику вычислительные ресурсы могут быть ограничены, при этом Дирекция ИТ осуществляет обязательное информирование Заказчика об отклонениях в качестве предоставлении сервиса.

5.4 Управление изменениями. ДИТ использует структурированный подход для управления изменениями в инфраструктуре Хостинга с помощью механизмов формального запроса и утверждения изменений. Любое изменение может принадлежать к одной из двух категорий: Запланированное, Аварийное.

5.5 Плановое техническое обслуживание. Запланированные периоды обслуживания позволяют ДИТ выполнять необходимые административные действия и процедуры с инфраструктурой хостинга (связанные с ограничением работы сервиса и предоставленных вычислительных ресурсов), а также проводить модернизацию сервиса.

5.6 В отдельных случаях при использовании подразделением нестандартных решений по согласованию с ДИТ пользователям сервиса могут предоставляться иные соглашения о качестве обслуживания коммуникационной и вычислительных компонент.

5.7 Проведение плановых и внеплановых работ сопровождается обязательным со стороны Дирекции ИТ информированием Заказчика.

6. Пул вычислительных ресурсов

6.1 Основой инфраструктуры сервиса предоставления вычислительных ресурсов выступает пул вычислительных ресурсов.

6.2 Пул вычислительных ресурсов состоит из аппаратной составляющей (вычислительные мощности) и программной составляющей с централизованным управлением и интеграцией всех компонентов.

6.3 В аппаратную часть пула вычислительных ресурсов входят:

- Унифицированные и однотипные вычислительные узлы;
- Аппаратные компоненты, управляющие вычислительными узлами;
- Системы хранения данных;
- Коммуникационное оборудование;
- Межсетевые экраны.

6.4 В программную часть пула вычислительных ресурсов входят:

- Гипервизоры;
- Сервера для управления, мониторинга хостинга и резервного копирования вычислительных ресурсов и инфраструктуры пула вычислительных ресурсов;
- Сервера для предоставления доступа к сервису предоставления вычислительных ресурсов, в том числе к порталу самообслуживания;
- Коммуникационное ПО для передачи данных и средства по его управлению;
- Базовые основные сервисы УрФУ: корпоративная сеть, единый каталог пользователей, почтовая система, сервис предоставления сетевых настроек DHCP, сервис регистрации разрешения имен DNS, сервис инфраструктуры открытых ключей PKI, сервис точного времени NTP, сервис обновления ПО Microsoft WSUS и сервис активации, управления ключами KMS и сервисы аутентификации RADIUS и TACACS+.

6.5 Пул вычислительных ресурсов размещается в ЦОДах или серверных помещениях ДИТ УрФУ.

6.6 ДИТ обеспечивает унифицированность, однородность, централизованное управление и однотипность сетевого и серверного оборудования, составляющего пул вычислительных ресурсов.

7. Права и обязанности пользователей сервиса

7.1 Пользователи сервиса предоставления вычислительных ресурсов (Администраторы приложений) имеют следующие права:

- Использовать учетную запись для доступа к выделенным вычислительным ресурсам;
- Использовать портал самообслуживания для управления выделенными вычислительными ресурсами;
- Обращаться за справочной информацией и консультацией к запросам специалистам ДИТ и службу технической поддержки.

7.2 Пользователи сервиса предоставления вычислительных ресурсов обязаны:

- Ознакомиться с настоящим положением до начала работы;

- При использовании выделенных вычислительных ресурсов выполнять все утвержденные правила и регламенты информационной безопасности, касающихся использования информационных систем университета;
- Нести полную ответственность за все действия, выполняемые ими при использовании выделенных вычислительных ресурсов;
- Исключить возможность неосторожного причинения вреда (действием или бездействием) инфраструктуре сервиса хостинга;
- Соблюдать требования законодательства РФ;
- Использовать лицензионное ПО, средства антивирусной защиты;
- Использовать выделенные вычислительные ресурсы исключительно в целях реализации функций своего структурного подразделения.

Администратор приложений должен своевременно обновлять ПО (включая утилиты поддержки виртуализации внутри гостевой ОС), в том числе по запросам специалистов ДИТ.

7.3 Пользователям сервиса предоставления вычислительных ресурсов запрещается:

- Использовать выделенные вычислительные ресурсы не по указанному в Заявке назначению;
- Использовать вредоносное ПО (за исключением использования подобного ПО в специальных лабораториях в целях выполнения учебной программы);
- Осуществлять несанкционированный доступ к информационным системам, сервисам и ресурсам университета;
- Предпринимать попытки взлома механизмов безопасности сервиса хостинга, а также любых информационных систем, сервисов и ресурсов университета;
- Использовать выделенные вычислительные ресурсы для размещения ИСПДн и иных прикладных систем, хранящих и обрабатывающих персональные или конфиденциальные данные без дополнительного согласования с ДИТ и Управлением информационной безопасности УрФУ.

7.4 Пользователь сервиса несет ответственность:

- за информацию, размещенную на предоставленных вычислительных ресурсах,
- за несвоевременное резервное копирование виртуального или физического сервера;
- за актуальность предоставленной в Заявке информации;
- за утрату данных на виртуальных или физических серверах вследствие сбоя системного или прикладного программного обеспечения.

7.5 В случае нарушения пользователем данного Положения доступ пользователя к сервису предоставления вычислительных ресурсов может быть ограничен ДИТ с последующим применением дисциплинарных, административных или иных мер, а процесс предоставления услуги Заказчику прекращен.

7.6 В случае возникновения опасности причинения ущерба другим пользователям или сервисам информационной инфраструктуры университета доступ пользователя к сервису хостинга может быть ограничен, а процесс предоставления услуги Заказчику прекращен.

8. Порядок ввода в действие, внесения изменений и информирования

8.1 Настоящее Положение об использовании сервиса предоставления вычислительных ресурсов на основе технологий частного облака Уральского федерального университета имени первого Президента России Б.Н. Ельцина вводится в действие приказом ректора.

8.2 Изменения в настоящее Положение могут быть инициированы сотрудниками Дирекции информационных технологий, в рамках исполнения своих обязанностей по данному Положению или иным принятым в УрФУ порядком для внесения изменений в руководящие документы. Измененная редакция положения согласуется с Управлением информационной безопасности и утверждается приказом Ректора.

8.3 Утвержденная Ректором редакция Положения публикуется в специальном разделе портала УрФУ.

8.4 Требования текущего варианта Положения с момента опубликования на портале УрФУ являются обязательными для всех пользователей (в том числе студентов, сотрудников) информационной инфраструктуры университета.

Приложение 2

к приказу ректора

от 04.06.2015 № 418/03

УТВЕРЖДАЮ



Ректор
Уральского федерального университета
имени первого Президента России
Б.Н. Ельцина


В.А. Кокшаров

«03» июня 2015 года

РЕГЛАМЕНТ

предоставления вычислительных ресурсов на основе технологий частного облака

Уральского федерального университета имени первого

Президента России Б.Н. Ельцина

Екатеринбург, 2015г.

Содержание

1. Термины и сокращения	3
2. Общие положения	5
3. Администраторы	6
4. Обязанности администраторов	7
5. Администраторы приложений	9
6. Сетевые администраторы	14
7. Инфраструктурные администраторы	16
8. Администраторы аудита	18
9. Администраторы мониторинга	19
10. Функции инженерного отдела по сопровождению сервиса	20
11. Зоны ответственности	20
12. Соглашение об уровне обслуживания	23
13. Инфраструктура пула вычислительных ресурсов	27
14. Пул вычислительных ресурсов	29
15. Порядок предоставления сервиса хостинга	30
16. Порядок диагностики и решения проблем	33
17. Параметры предоставляемых вычислительных ресурсов	35
18. Сетевая связность вычислительных ресурсов	36
19. Сетевая адресация вычислительных ресурсов	36
Приложение №1 Форма заявки на выделение вычислительных ресурсов	40

1. Термины и сокращения

УрФУ	Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
ДИТ, Дирекция ИТ, Дирекция информационных технологий	Дирекция информационных технологий УрФУ
УИТИ	Управление информационно-телекоммуникационной инфраструктуры ДИТ
УПП	Управление поддержки пользователей ДИТ
Отдел базовых сервисов, ОБС	Отдел базовых сервисов в УИТИ ДИТ
Инженерный отдел	Отдел развития и эксплуатации инженерной инфраструктуры и центров обработки данных УИТИ ДИТ
Отдел мониторинга	Отдел мониторинга единой сети передачи данных УИТИ ДИТ
Сетевой отдел	Отдел развития и эксплуатации единой сети передачи данных в УИТИ ДИТ
УИБ	Управление информационной безопасности
ПО	Программное обеспечение
ОС	Операционная система
Единый каталог, АД, AD, Active Directory, AT.URFU.RU	Каталог объектов Microsoft Active Directory. Включает в себя домен Active Directory «at.urfu.ru», лес Active Directory «at.urfu.ru», DNS-зону «at.urfu.ru» дочерние DNS-зоны в зоне «at.urfu.ru» и несколько обратных DNS-зон.
Корпоративная почта	Инфраструктура из почтовых систем для пересылки электронной почты, обслуживающая почтовый домен «urfu.ru» и поддерживаемая отделом базовых сервисов, а также почтовый ящик в почтовых системах УрФУ.
Подразделение	Структурное подразделение УрФУ соответствующее принятой организационно-штатной структуре университета. В качестве Подразделения могут выступать управление, центр, отдел, институт, департамент, кафедра, лаборатория, сектор и т.п.
Вредоносное ПО	ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности или доступности информации.
Учетная запись	Учетная запись пользователя или администратора в едином каталоге пользователей AT.URFU.RU. Включает Имя учётной записи (логин), Пароль и ряд других атрибутов.
Вычислительные ресурсы	Набор из объема оперативной памяти, места на диске, процессорных ядер, сетевого адаптера, а также иного программно-аппаратного обеспечения, формирующих аппаратное обеспечение сервера.
Пул вычислительных	Группа унифицированного, однородного, централизованно-управляемого и однотипного коммуникационного и серверного оборудования,

ресурсов УИТИ, пул вычислительных ресурсов	поддерживаемая УИТИ, из которого выделяются вычислительные ресурсы по запросу подразделений в рамках сервиса предоставления вычислительных ресурсов.
Инфраструктура пула вычислительных ресурсов	Пул вычислительных ресурсов УИТИ, а также набор серверов, гипервизоров, ОС, виртуальных машин, базовых сервисов и иного ПО, размещенного в пуле вычислительных ресурсов, обеспечивающего возможность предоставления сервиса хостинга.
Вычислительные мощности	Набор серверного оборудования и систем хранения данных, из которых составляется пул вычислительных ресурсов.
Виртуальная машина, VM	Один из типов предоставляемого вычислительного ресурса; виртуальный сервер, развернутый на поддерживаемых гипервизорах в пуле вычислительных ресурсов.
Шаблон виртуальной машины	Заранее заданный набор технических характеристик виртуальной машины и/или настроек операционной системы.
Хостинг	Предоставлению вычислительных ресурсов, а также сервис по предоставлению вычислительных ресурсов из пула вычислительных ресурсов УИТИ.
Частное облако	Физически или логически выделенный пул вычислительных ресурсов с возможностью создания различных конфигураций ИТ-инфраструктуры. Реализация модели облачных вычислений на имеющихся у университета компьютерных ресурсах.
Корпоративная сеть	Корпоративная сеть УрФУ, поддерживаемая отделом развития и эксплуатации единой сети передачи данных УИТИ, включающая в себя коммуникационное аппаратное и коммуникационное программное обеспечение.
Портал	Веб-интерфейс « https://vm.urfu.ru/ », либо иной, используемый администраторами виртуальных машин и администраторами приложений, для управления предоставленными им вычислительными ресурсами и данными в них (включая ОС и приложения).
Стандарт IP-адресации, положение об IP-адресации	Положение об использовании адресации интернет протокола версии 4 в сети Уральского федерального университета имени первого Президента России Б.Н. Ельцина.
DHCP	Протокол динамической конфигурации хоста (англ. Dynamic Host Configuration Protocol,) – сетевой протокол, позволяющий компьютерам автоматически получать IP адрес и другие параметры, необходимые для работы в сети.
DNS	Domain Name System (Система доменных имен)

2. Общие положения

- 2.1 Целью настоящего Регламента является описание порядка предоставления (аренды) вычислительных ресурсов на основе технологий «Local Cloud», прав и обязанностей пользователей, а также уровней обслуживания для пользователей данной услуги.
- 2.2 Сервис предоставления вычислительных ресурсов, именуемый также в дальнейшем «Хостинг», предоставляется дирекцией информационных технологий подразделениям, сотрудникам или преподавателям УрФУ, именуемым в дальнейшем «Пользователь».
- 2.3 Регламент определяет общие правила использования сервиса Хостинга для всех пользователей и администраторов информационной инфраструктуры УрФУ.
- 2.4 Хостинг предоставляется для размещения информационных систем и сервисов с целью обеспечения учебного процесса, научных исследований, международного сотрудничества и иной образовательной или административной деятельности университета.
- 2.5 Сервис Хостинга интегрирован с основными базовыми сервисами УрФУ: доступ в корпоративную сеть и интернет, сервисы единого каталога пользователей, корпоративная почтовая система, сервис предоставления сетевых настроек DHCP, сервис регистрации разрешения имен DNS, сервис инфраструктуры открытых ключей PKI, сервис точного времени NTP, сервис обновления ПО Microsoft WSUS и сервис активации и управления ключами KMS.
- 2.6 Сервис Хостинга эксплуатируется в соответствии с дизайном, техно-рабочей и нормативной документацией по перечисленным основным базовыми сервисам УрФУ.
- 2.7 УрФУ проводит единую централизованную политику по управлению вычислительными ресурсами. Для обеспечения высокой надежности информационных сервисов подразделениям следует размещать вычислительные ресурсы в пуле вычислительных ресурсов УрФУ. Размещение приложений, информационных систем и сервисов вне пула вычислительных ресурсов осуществляется в исключительных случаях по согласованию с начальником УИТИ ДИТ при невозможности работы размещаемого сервиса в пулах вычислительных ресурсов.
- 2.8 Из пула вычислительных ресурсов предполагается выделение любых вычислительных ресурсов в виде виртуальных машин. Предоставление вычислительных ресурсов на физических серверах осуществляется в исключительных случаях по согласованию с начальником УИТИ ДИТ при невозможности работы размещаемого сервиса в виртуализированной среде.
- 2.9 Инфраструктура Пула вычислительных ресурсов поддерживается ДИТ.

- 2.10 Инфраструктура хостинга обеспечивает инфраструктуру для централизованного управления и обслуживания серверов и сервисов подразделений, а также реализации ряда корпоративных сетевых сервисов, таких как файловые сервисы, единый каталог пользователей, почтовые сервисы, сервисы печати, сервисы лицензирования, сервисы аутентификации RADIUS и TACACS+, и иные базовые сервисы корпоративной сети.
- 2.11 Серверы, системы хранения и другие подсистемы пула вычислительных ресурсов сопровождаются Отделом базовых сервисов УИТИ ДИТ.
- 2.12 Корпоративная сеть, используемая пулом вычислительных ресурсов, поддерживается отделом развития и эксплуатации единой сети передачи данных УИТИ ДИТ.
- 2.13 В развитие данного регламента могут создаваться обязательные для исполнения пользователями и администраторами технологические регламенты и иные технические условия и требования к хостингу, прочие частные регламенты и нормы регулирования по использованию сервиса Хостинга в специальных случаях.
- 2.14 ДИТ может приостановить оказание сервиса Хостинга, если Пользователь не выполняет обязанности и требований настоящего регламента.
- 2.15 ДИТ может приостановить оказание Хостинга любому Пользователю по предписанию УИБ о невозможности предоставления Хостинга по соображениям безопасности.
- 2.16 ДИТ может принимать решение о приостановке оказания сервиса Хостинга, блокирования или запрета использования ПО Пользователя в случае, если эксплуатация такого программного обеспечения приводит или может привести к аварийным ситуациям, нарушению требований системы безопасности
- 2.17 ДИТ оставляет за собой право отказать в предоставлении услуг или прекратить предоставляемые услуги любому Пользователю по своему усмотрению.

3. Администраторы

- 3.1. Администраторы – это пользователи информационной структуры университета, ответственные за проведение технических работ по администрированию инфраструктуры хостинга, предоставленных вычислительных ресурсов и конечных приложений, и назначенные соответствии с требованиями, описанными в данном регламенте.
- 3.2. Администраторы должны придерживаться настоящего регламента для решения задач администрирования и все свои действия выполнять строго по инструкциям,

- регламентам или задокументированным процедурам (при наличии инструкций или задокументированных процедур для решения конкретной задачи администрирования).
- 3.3. Администраторы должны ознакомиться с существующими документами, а в дальнейшем получать изменения и новые документы и своевременно изучать их.
- 3.4. Администраторы своими действиями не должны нарушать структуру и дизайн хостинга, описанные в техно-рабочей документации.
- 3.5. После назначения администратор обязан выполнять свои функции в рамках назначенных ему ролей, а также процедур и инструкций. Администратору запрещается выполнять административные действия с инфраструктурой хостинга вне назначенных ему ролей, функций, задокументированных процедур или инструкций. В данном регламенте предусмотрено, что только один тип администраторов может выполнять заданную функцию.
- 3.6. Все администраторы хостинга подразделяются на следующие категории:
- Инфраструктурные администраторы,
 - Администраторы приложений,
 - Сетевые администраторы,
 - Администраторы мониторинга,
 - Администраторы аудита.
- 3.7. Один пользователь может принадлежать нескольким категориям администраторов, если он удовлетворяет требованиям каждой категории и назначен на каждую в соответствии с настоящим регламентом.
- 3.8. Все администраторы должны иметь соответствующую квалификацию, необходимую для выполнения задач в категории, на которую он был назначен.

4. Обязанности администраторов

- 4.1 Администраторы приложений должны использовать только единую диспетчерскую службу ДИТ для взаимодействия с другими администраторами.
- 4.2 Инфраструктурные администраторы, сетевые администраторы и администраторы аудита должны использовать корпоративную почту или единую диспетчерскую службу ДИТ для взаимодействия с другими администраторами. В случаях аварийных ситуаций им разрешается использование мобильных телефонов для коммуникаций с остальными администраторами.

- 4.3 При отсутствии реакции, инфраструктурные администраторы могут сократить или полностью прекратить оказание услуги хостинга подразделению.
- 4.4 Администраторам запрещена передача журнала безопасности или его части подразделениям, либо сторонним организациям, если это не предусмотрено законодательством РФ.
- 4.5 После утверждения или обновления регламента администрирования сервиса предоставления вычислительных ресурсов, администраторы должны ознакомиться с настоящим регламентом до начала работы.
- 4.6 Администраторы должны использовать для работы с инфраструктурой хостинга только свою персональную учетную запись, а также хранить в тайне и не допускать компрометации соответствующий ей пароль. При компрометации пароля немедленно его изменить и сообщить об этом в единую диспетчерскую службу ДИТ.
- 4.7 Администраторы несут полную ответственность за все действия, выполняемые ими при доступе к инфраструктуре хостинга.
- 4.8 Администратор несет полную ответственность за все действия, произведенные в сервисе хостинга, совершенные от его имени его учетной записи.
- 4.9 Администраторы должны использовать лицензионное ПО, средства антивирусной защиты.
- 4.10 Администраторам запрещается:
- Осуществлять доступ сервисам хостинга с использованием чужих атрибутов доступа (логин и пароль) или воспользовавшись чужим сеансом;
 - Препятствовать работе сервиса или инфраструктуры хостинга;
 - Использовать, публиковать и передавать информацию, содержащие вредоносное ПО и вирусы, либо их компоненты (за исключением использования подобного ПО в специальных лабораториях в целях выполнения учебной программы);
 - Осуществлять несанкционированный доступ к сервисам;
 - Предпринимать попытки взлома механизмов безопасности хостинга;
 - Использовать системы электронной почты для массовой рассылки нежелательных сообщений (спама).
- 4.11 В случае нарушения администратором регламента администрирования сервиса предоставления вычислительных ресурсов доступ администратора к ряду сервисов может быть ограничен с последующим применением дисциплинарных, административных или иных мер, а предоставление сервиса хостинга подразделению может быть прекращено.

5. Администраторы приложений

- 5.1 Администратор приложения – представитель Пользователя, выполняющий определённые функции согласно данному положению.
- 5.2 Администраторы приложений должны использовать предоставленные вычислительные ресурсы только для тех задач, для которых данные вычислительные ресурсы были выделены.
- 5.3 Администраторы приложений должны управлять предоставленными вычислительными ресурсами через портал, средствами удаленного администрирования серверов, а также по иным регламентам и инструкциям инфраструктурных администраторов.
- 5.4 Администраторы приложений должны самостоятельно с помощью портала или по инструкциям инфраструктурных администраторов выполнять создание виртуальных машин и иные операции на предоставленных вычислительных ресурсах с использованием соответствующей инструкций, в том числе:
- Запуск, перезапуск и остановка вычислительного ресурса;
 - Создание, возврат и удаление снимков виртуальной машины с параметрами и требованиями, описанными в соответствующей инструкции;
 - Монтирование загрузочных ISO-образов для восстановления или установки ОС внутри предоставленных вычислительных ресурсов.
- 5.5 Администраторы приложений на предоставленных им вычислительных ресурсах полностью и самостоятельно осуществляют администрирование и управляют всеми данными, конфигурациями и процессами (при наличии дополнительных регламентами, положений и инструкция, в соответствии с ними), в том числе:
- Операционной системой и ее настройками, в том числе процессом установки операционной системы;
 - Контролем доступа к ОС и приложениями;
 - Средствами удаленного администрирования сервера (в том числе серверами протоколов SSH, RDP, PowerShell и иными);
 - Загрузчиком операционной системы;
 - Драйверами устройств;
 - Утилитами поддержки виртуализации;
 - Файловыми системами и разделами жестких дисков;

- Сетевыми настройками (в том числе адресами DNS-серверов, NTP-серверов и WINS-серверов);
- DHCP-клиентом;
- Системным ПО;
- Прикладным ПО;
- Приложениями;
- Базами данных и СУБД;
- Сервисами и информационными системами;
- Антивирусом и персональным межсетевым экраном;
- Средствами удаленного администрирования сервера, производимого через сетевые интерфейсы сервера;
- Иными ресурсами и данными, размещенными внутри предоставленных вычислительных ресурсов.

5.6 Администраторы приложений самостоятельно обеспечивают и восстанавливают работоспособность, а также обеспечивают наличие перечисленных выше компонентов.

5.7 Если администратор приложений не управляет перечисленными выше компонентами, то сервис хостинга (или его часть) для данного администратора приложений или подразделения приостанавливается, а через 14 дней предоставленные вычислительные ресурсы отзываются.

5.8 Настройки некоторых из перечисленных выше компонентов дополнительно должны быть согласованы с инфраструктурными администраторами, сетевыми администраторами или администраторами аудита. Это относится к компонентам, непосредственно взаимодействующими с внешней средой (аппаратное обеспечение) по отношению к предоставленному вычислительному ресурсу. Сюда входят сетевые настройки (в том числе IP-адреса) и топология подключения к сети, драйвера устройств, утилиты поддержки виртуализации и методы публикации приложений в корпоративной сети или сети Интернет.

5.9 Администраторам приложений запрещается самовольно без согласования с инфраструктурными или сетевыми администраторами назначать сетевые настройки (в том числе IP-адрес и MAC-адрес).

5.10 Администраторы приложений должны обеспечить подключение клиентов к серверам с помощью DNS-имен или с помощью других технологий, позволяющих оперативно изменять IP-адрес сервера.

- 5.11 При необходимости коммуникаций между серверами администраторы приложений должны обеспечивать такое взаимодействие с использованием DNS-имён в качестве имен серверов.
- 5.12 Администраторы приложений должны обеспечить себе возможность управления операционной системой средствами удаленного администрирования сервера из корпоративной сети и не препятствовать его работе (отключать средства управления, назначать некорректные сетевые настройки, отключать сети, запрещать возможность через межсетевые экраны).
- 5.13 Администраторы приложений должны самостоятельно обрабатывать заявки пользователей по использованию сервиса, размещенного в пуле вычислительных ресурсов.
- 5.14 Администраторы приложений должны исключить возможность неосторожного причинения вреда (действием или бездействием) инфраструктуре хостинга.
- 5.15 Администраторам приложений запрещается использовать средства администрирования (в т. ч. ошибки и уязвимости в ПО) для получения доступа к ресурсам, доступ к которым им явно не предоставлен.
- 5.16 Администраторы приложений могут делегировать свои полномочия полностью или их часть на виртуальные машины иным Администраторам приложений.
- 5.17 Администраторы приложений могут делегировать некоторые из своих полномочий на предоставленные вычислительные ресурсы иным администраторам подразделений, пользователям или подразделениям.
- 5.18 Делегирование возможно только при письменном согласии пользователя, администратора или подразделения с возлагаемыми на него задачами.
- 5.19 Делегирование осуществляется администратором приложений самостоятельно.
- 5.20 Администраторы приложений в рамках данного регламента не могут делегировать свои полномочия иным типам администраторов (инфраструктурным администраторам, администраторам аудита или сетевым администраторам), сервисным администраторам единого каталога пользователей, а также подразделениями в составе ДИТ. Администраторам приложений запрещаются такие действия.
- 5.21 Администратор сервера и администратор виртуальных машин являются частными случаями администратора приложений согласно данному регламенту.
- 5.22 Администратор приложения должен на предоставленных ему вычислительных ресурсах:
- Управлять паролями, учетными записями и восстанавливать пароли;

- Не изменять сетевые настройки без согласования с инфраструктурными или сетевыми администраторами;
- Своевременно устанавливать обновления безопасности на ОС;
- Своевременно устанавливать и обновлять актуальные версии драйверов, утилит для виртуализации, а также установить и использовать антивирус с последними доступными базами;
- Своевременно выключать, удалять виртуальную машину при завершении цикла работ, а также освобождать иные предоставленные вычислительные ресурсы с уведомлением инфраструктурных администраторов.
- Оперативно устранять проблемы внутри ОС, если они влияют на пул вычислительных ресурсов, в том числе обнаруживать и восстанавливать «зависшие» приложения.
- Обеспечить наличие не менее 5% свободного дискового пространства на всех предоставленных вычислительных ресурсах. В дополнение к этому на каждом логическом разделе размером более гигабайта обеспечить не менее 512 мегабайт свободного места.
- Обеспечить возможность резервного копирования виртуальной машины инфраструктурой пула вычислительных ресурсов.
- Обеспечить защиту развернутой операционной системы и иного развернутого ПО на предоставленных вычислительных ресурсах, а также данных на уровне приложения и данных на уровне ОС в соответствии с законодательством РФ, нормативными актами УрФУ и требованиями развернутого ПО.

5.23 Администраторам приложений запрещается фальсификация сетевых адресов (включая IP-адрес и MAC-адрес), а также других идентификационных данных, используемых в сетевых протоколах, при передаче данных в сети Интернет, без согласования с инфраструктурными и сетевыми администраторами.

5.24 Администраторам приложений запрещается использование вычислительных ресурсов хостинга в качестве маршрутизатора сетевого уровня, прокси-сервера (как TCP-прокси, так и HTTP-прокси, так и SOCKS-прокси и иные), сервера виртуальной частной сети (VPN), трансляции адресов (NAT) и иных сервисов предоставления доступа в корпоративную сеть, либо туннельных сервисов, а также устанавливать ПО для данных задач, без согласования с инфраструктурными и сетевыми администраторами.

- 5.25 Администратор приложений при наличии технической возможности должен обеспечить работоспособность технологий Dynamic DNS внутри ОС на предоставленных вычислительных ресурсах.
- 5.26 Администратор приложений при наличии технической возможности должен обеспечить подключение клиентов к предоставленному вычислительному ресурсу по DNS-имени.
- 5.27 Администратор приложений должен иметь не менее одной резервной копии операционной системы и не менее одной резервной копии информационной системы, размещенной в виртуальной машине, на серверной площадке в другом здании, либо на оборудовании, не связанном с пулом вычислительных ресурсов.
- 5.28 Администратор приложений должен самостоятельно своевременно создавать консистентные резервные копии хранимых данных, информационных систем, сервисов и приложений, размещенных в пуле вычислительных ресурсов, а также управлять созданными резервными копиями.
- 5.29 Администраторы приложений не должны создавать чрезмерную необоснованную нагрузку на пул вычислительных ресурсов и корпоративную сеть, а также организовать атаки (в том числе и DDOS-атаки).
- 5.30 Администраторы приложений должны бережно и экономно использовать предоставленные вычислительные ресурсы. При возможности оптимизации развернутых приложений, сервисов или информационных систем с целью сокращения потребления вычислительных ресурсов, они должны быть оптимизированы.
- 5.31 Для получения возможности воспользоваться вычислительными ресурсами из пула вычислительных ресурсов администратору приложения необходимо иметь почтовый ящик в почтовом домене «@urfu.ru», предоставить инфраструктурными администраторам обоснование необходимости доступа и сообщить имя административной учетной записи администратора подразделения в едином каталоге пользователей «AT.URFU.RU». При отсутствии административной учетной записи, допускается сообщение данных основной учетной записи, однако в этом случае часть возможностей может быть недоступна.
- 5.32 Администратор приложений должен указать мобильный телефон и контактный адрес электронной почты в едином каталоге пользователей для обеспечения возможности оперативной коммуникации в случае аварий.
- 5.33 При наличии уже выделенных вычислительных ресурсов из пула вычислительных ресурсов, инфраструктурные администраторы могут самостоятельно

без запросов предоставлять доступ администратору приложений данных вычислительных ресурсов к порталу и выделенным вычислительным ресурсам.

5.34 Администраторам приложений запрещено использовать предоставленные вычислительные ресурсы под задачи, отличающихся от согласованных с инфраструктурными администраторами.

5.35 Администраторам приложений запрещено размещать на предоставленных вычислительных ресурсах ИСПДн, персональные данные, сведения составляющие государственную тайну и иные виды конфиденциальной информации без согласования с управлением информационной безопасности УрФУ и инфраструктурными администраторами.

6. Сетевые администраторы

6.1 Сетевыми администраторами сервиса хостинга являются назначенные начальником УИТИ сотрудники отдела развития и эксплуатации единой сети передачи данных УИТИ, а также начальник отдела развития и эксплуатации единой сети передачи данных УИТИ.

6.2 Сетевые администраторы должны выполнять задачи администрирования корпоративной сети в соответствии с положением об использовании интернет протокола версии 4 в УрФУ, регламентом администрирования сервиса предоставления сетевых настроек DHCP и нормативными документами, и регламентами по сервису предоставления вычислительных ресурсов.

6.3 Сетевые администраторы обеспечивают работоспособность всех необходимых потоков сетевых коммуникаций для сервисов, размещенных в пуле вычислительных ресурсов, согласно техно-рабочей документации, с учетом действующей нормативной документации по корпоративной сети УрФУ и технических ограничений корпоративной сети.

6.4 Сетевые администраторы должны обеспечить возможность сетевых коммуникаций для всей инфраструктуры хостинга в соответствии с требованиями инфраструктурных компонентов хостинга, а также техно-рабочей документации по инфраструктуре хостинга, согласованной с начальником сетевого отдела УИТИ.

6.5 Сетевые администраторы осуществляют проектирование, внедрение, администрирование и диагностику всего сетевого коммуникационного оборудования и

всего ПО, либо их части, обеспечивающее коммуникации между компонентами пула вычислительных ресурсов, включая программные компоненты.

- 6.6 Сетевые администраторы должны согласовывать схему, топологию и архитектуру корпоративной сети, участвующую в передаче данных для пула вычислительных ресурсов, а также относящиеся нормативные документы и регламенты с инфраструктурными администраторами.
- 6.7 Сетевые администраторы обеспечивают предоставление, регистрацию и резервацию статических и динамических IP-адресов (получаемых с помощью сервиса предоставления сетевых настроек DHCP), используемых в пуле вычислительных ресурсов при наличии необходимости или обоснования в соответствии с регламентом администрирования сервиса предоставления сетевых настроек DHCP.
- 6.8 Сетевые администраторы обеспечивают настройку или перенастройку по запросу параметров доступа к сетевым сегментам на предоставленных администратору приложениях вычислительных ресурсов (настройку параметров подключения сетевых адаптеров со стороны коммуникационного оборудования и коммуникационного и управляющего ПО).
- 6.9 Сетевые администраторы обеспечивают возможность доступа к порталу и предоставленным вычислительным ресурсам изнутри корпоративной сети.
- 6.10 Сетевые администраторы организуют резервное копирование конфигурации коммуникационной инфраструктуры.
- 6.11 Сетевые администраторы должны согласовывать с инфраструктурными администраторами проводимые работы в корпоративной сети, уведомлять инфраструктурных администраторов об инцидентах, процессе и результатах их решения, если они могут повлиять на возможность сетевых коммуникаций компонентов пула вычислительных ресурсов и предоставленных вычислительных ресурсов.
- 6.12 Сетевые администраторы обеспечивают корректность заполнения информации о выделенных IP адресах виртуальным ресурсам и сетях инфраструктуры хостинга на портале: <http://ip.dit.urfu.ru>.
- 6.13 Сетевые администраторы должны уведомлять администраторов приложений о проводимых работах в корпоративной сети, если они могут повлиять на возможность сетевых коммуникаций, предоставленных администратору приложения вычислительных ресурсов.

7. Инфраструктурные администраторы

- 7.1 Инфраструктурные администраторы выполняют функции администрирования серверной инфраструктуры пула вычислительных ресурсов с целью обеспечения возможности предоставления вычислительных ресурсов для подразделений УрФУ в рамках имеющихся вычислительных мощностей.
- 7.2 Инфраструктурные администраторы обеспечивают функционирование сервиса хостинга и организуют предоставление вычислительных ресурсов администраторам приложений.
- 7.3 Только инфраструктурные администраторы имеют и могут иметь административный доступ (либо его аналог любого вида) к пулу вычислительных ресурсов и серверам управления пула вычислительных ресурсов (часть серверов инфраструктуры пула).
- 7.4 Только инфраструктурные администраторы могут иметь физический доступ к пулу вычислительных ресурсов и его инфраструктурным компонентам.
- 7.5 Инфраструктурные администраторы и только они осуществляют настройку и поддержку пула вычислительных ресурсов и его инфраструктуры, в которую входят следующие объекты и функции:
- Добавление, исключение и обновление компонентов пула вычислительных ресурсов и инфраструктурных компонентов хостинга. Определение возможности добавления устройства в пул;
 - Контроль целостности и мониторинг состояния и изменений хостинга;
 - Исправление ошибок, внесенных другими администраторами, при отсутствии возможности исправления этих ошибок самими администраторами;
 - Делегирование полномочий иным администраторам.
- 7.6 Инфраструктурные администраторы не могут делегировать полномочия управления перечисленными выше объектами не инфраструктурным администраторам и сервисным учетным записям, которыми управляют не сервисные администраторы единого каталога пользователей.
- 7.7 Инфраструктурные администраторы не осуществляют управление операционными системами и приложениями подразделений, размещенных на вычислительных ресурсах из пула вычислительных ресурсов. Выполнение таких действий сервисным администраторам запрещается.
- 7.8 Роль инфраструктурного администратора может назначаться только сотрудникам ОБС.
- 7.9 Роль инфраструктурного администратора может назначаться только сервисным администраторам единого каталога пользователей.

- 7.10 Инфраструктурные администраторы назначаются сервисным администратором единого каталога пользователей с соответствующей группой-ролью (согласно дизайну единого каталога пользователей) посредством включения сервисной административной учетной записи инфраструктурного администратора в соответствующую группу-роль (согласно дизайну единого каталога пользователей).
- 7.11 Инфраструктурные администраторы должны не менее чем за пять рабочих дней уведомлять других администраторов о планируемых изменениях в инфраструктуре хостинга посредством корпоративной почты, если эти изменения могут привести к неработоспособности сервиса хостинга или предоставленных вычислительных ресурсов.
- 7.12 Инфраструктурные администраторы уведомляют всех администраторов и УПП о глобальных изменениях структуры хостинга (также могут уведомлять об иных изменениях хостинга) посредством корпоративной почты.
- 7.13 Инфраструктурные администраторы организуют техническое обслуживание серверных компонентов пула вычислительных ресурсов.
- 7.14 Инфраструктурные администраторы обеспечивают разработку и регулярную актуализацию шаблонов виртуальных машин и аппаратных серверов.
- 7.15 Инфраструктурные администраторы обеспечивают администратору приложений возможность установки и настройки на предоставленных вычислительных ресурсах любой поддерживаемой ОС любой поддерживаемой версии, в том числе с помощью монтирования загрузочного ISO-образа с дистрибутивом администратора приложений.
- 7.16 Инфраструктурные администраторы отслеживают работоспособность виртуальной инфраструктуры и основных коммуникационных компонентов.
- 7.17 Инфраструктурные администраторы обеспечивают доступ к порталу администраторам приложений, в том числе доступ к консоли предоставленных вычислительных ресурсов изнутри корпоративной сети университета.
- 7.18 Инфраструктурные администраторы обеспечивают настройку системных параметров и масштабирование аппаратной части предоставленных вычислительных ресурсов при поступлении соответствующей заявки от администратора приложений, при наличии незарезервированных ресурсов, при условии отсутствия технической возможности выполнения данных действий иным администратором, в том числе:
- Изменение числа процессорных потоков;
 - Изменение выделенного объема для долгосрочного хранения данных виртуальной машины;

- Изменение выделенного объема оперативной памяти.
- 7.19 Виртуальные машины в пуле вычислительных ресурсов инфраструктурными администраторами создаются только при отсутствии технической возможности администратору приложений воспользоваться порталом.
- 7.20 Инфраструктурные администраторы обеспечивают резервное копирование инфраструктуры пула вычислительных ресурсов за исключением коммуникационной инфраструктуры и систем мониторинга.
- 7.21 Инфраструктурные администраторы могут заполнять информацию о выделенных IP адресах виртуальным ресурсам на портале: <http://ip.dit.urfu.ru>.
- 7.22 Инфраструктурные администраторы обеспечивают периодическое резервное копирование виртуальных машин размещенных в пуле вычислительных ресурсов с сохранностью ОС, но без гарантий сохранности и консистентности данных приложений внутри ОС, при наличии технической возможности.
- 7.23 Инфраструктурные администраторы планируют и организуют согласование регламентных, профилактических и иных видов работ, которые могут привести к временной неработоспособности сервиса.
- 7.24 Инфраструктурные администраторы обеспечивают возможность восстановления виртуальной машины по запросу администратора приложений.

8. Администраторы аудита

- 8.1 Администраторы аудита осуществляют аудит всех действий администраторов и пользователей сервиса, изменений структуры пула вычислительных ресурсов, аудит делегирования полномочий администраторам и сервисным учетным записям и аудит создания, изменения, связывания и удаления виртуальных машин.
- 8.2 Технически возможность аудита предоставляется посредством делегирования учетным записям администраторов аудита или сервисным учетным записям предназначенных для аудита следующих полномочий:
 - Просмотр настроек систем управления пулом вычислительных ресурсов;
 - Просмотр настроек коммуникационного оборудования и коммуникационного ПО;
 - Чтение журнала безопасности серверов инфраструктуры пула вычислительных ресурсов;
 - Чтения журналов аудита действий пользователей.

- 8.3 Администраторы аудита осуществляют копирование всего журнала безопасности с событиями аудита, либо необходимой его части.
- 8.4 Администраторы аудита не могут вносить изменения в пул вычислительных ресурсов, инфраструктуру и его параметры, в настройки виртуальных машин, а также осуществлять подключение к консоли виртуальных машин, посылать команды виртуальным машинам.
- 8.5 Роль администратора аудита может назначаться только сотрудниками отдела технической защиты информации управления информационной безопасности УрФУ.
- 8.6 Администратор аудита назначается распоряжением руководителя управления информационной безопасности УрФУ, согласованным с начальником УИТИ. Администратор аудита сервиса хостинга назначается по процедуре назначения администратора аудита единого каталога пользователей в соответствии регламентом администрирования единого каталога пользователей.

9. Администраторы мониторинга

- 9.1 Администраторами мониторинга сервиса хостинга являются назначенные начальником сотрудники отдела мониторинга единой сети передачи данных УИТИ, а также начальник отдела мониторинга единой сети передачи данных УИТИ.
- 9.2 Администраторы мониторинга развертывают и поддерживают системы мониторинга, сбора статистики и оповещений об инцидентах для инфраструктуры пула вычислительных ресурсов. Администраторы мониторинга также могут организовывать мониторинг предоставленных администраторам приложений вычислительных ресурсов.
- 9.3 Администраторы мониторинга организуют сбор и предоставление статистики по использованию инфраструктуры пула вычислительных ресурсов и ее отдельным компонентам.
- 9.4 Администраторы мониторинга совместно с сетевыми администраторами организуют сбор сетевой статистики и статистики посещений ресурсов в сети Интернет компонентов инфраструктуры пула вычислительных ресурсов и предоставленных вычислительных ресурсов, а также предоставляют статистику остальным администраторам по запросу.
- 9.5 Администраторы мониторинга в случае возникновения инцидентов организуют оповещение инфраструктурных и иных администраторов, на работу которых данные

инциденты могут произвести влияние, либо которым необходимо провести работы по решению проблемы.

9.6 Технически возможность мониторинга предоставляется посредством делегирования учетным записям администраторов мониторинга или сервисным учетным записям предназначенных для мониторинга возможности просмотра настроек, статистики и размещенных данных инфраструктуры пула вычислительных ресурсов.

9.7 Администраторы мониторинга не могут вносить изменения в пул вычислительных ресурсов, инфраструктуру и его параметры (за исключением систем мониторинга, сбора статистики и уведомления о инцидентах), в настройки виртуальных машин, а также осуществлять подключение к консоли виртуальных машин, посылать команды виртуальным машинам.

10. Функции инженерного отдела по сопровождению сервиса

10.1 Сотрудники инженерного отдела выполняют установку, перестановку и демонтаж оборудования в центрах обработки данных ДИТ, серверных помещениях ДИТ и коммуникационных узлах, а также выполняют профилактические работы на оборудовании в данных помещениях по запросам инфраструктурных администраторов.

10.2 Сотрудники инженерного отдела выполняют подключение соединений (как силовых, так и коммуникационных) внутри перечисленных помещений и между ними.

10.3 Сотрудники инженерного отдела в перечисленных помещениях для размещенного оборудования обеспечивают необходимые условия по электропитанию, охлаждению, уровню влажности и т.п. согласно требований к оборудованию и документации по данным помещениями.

10.4 Начальник инженерного отдела организует работы сотрудников инженерного отдела по решению указанных в данном разделе задач.

11. Зоны ответственности

11.1 Сервис хостинга не предполагает оказание Пользователю услуг по администрированию предоставленных вычислительных ресурсов, операционных систем и приложений, расположенных на выделенных ресурсах. Администрирование предоставленных вычислительных ресурсов осуществляется администратором приложения или другим представителем Пользователя.

- 11.2 При возникновении проблем в пуле вычислительных ресурсов, негативно влияющих на предоставленные вычислительные ресурсы и требующих для восстановления участия нескольких администраторов, администратор приложения выполняет восстановление программной части внутри предоставленных вычислительных ресурсов, администратор инфраструктуры выполняет восстановление аппаратной части или виртуализованной аппаратной части, а сетевой администратор восстанавливает сетевую связность до внешнего аппаратного или виртуализованного аппаратного интерфейса предоставленного вычислительного ресурса. Порядок диагностики инцидентов описан в разделе «Порядок предоставления сервиса хостинга».
- 11.3 Зона ответственности УИТИ по обеспечению надежной работы коммуникационной инфраструктуры пула вычислительных ресурсов физически находится между коннектором сетевого кабеля для клиентского компьютера, физического сервера или иного сетевого устройства подразделения, размещенного в корпоративной сети УрФУ; внешним сетевым интерфейсом предоставленного вычислительного ресурса; беспроводной точкой доступа; соединением с вышестоящим провайдером доступа УрФУ в Интернет. Для компонентов инфраструктуры (клиентский компьютер, виртуальная машина, вычислительный ресурс) размещаемых на границе ответственности, УИТИ разрабатывает регламенты и инструкции по подключению, использованию и диагностике соединения с коммуникационной инфраструктурой.
- 11.4 Зоной ответственности администратора приложений является драйвер физического или виртуального сетевого адаптера сервера или виртуальной машины, а также сетевые настройки данного сетевого адаптера и операционной системы.
- 11.5 Зоной ответственности отдела развития и эксплуатации инженерной инфраструктуры и центров обработки данных УИТИ являются все физические соединения (как коммуникационные, так и силовые) между компонентами инфраструктуры пула вычислительных ресурсов, в том числе между портами физических серверов и сетевым оборудованием.
- 11.6 Администрирование коммуникационных сетей для инфраструктуры пула вычислительных ресурсов осуществляется отделом развития и эксплуатации единой сети передачи данных УИТИ совместно с ОБС. Отдел развития и эксплуатации единой сети передачи данных УИТИ и ОБС организуют достаточный для оперативного выполнения диагностики доступ к физическим устройствам, к коммуникационному и

управляющему ПО, необходимому для работы коммуникационных сетей инфраструктуры пула вычислительных ресурсов.

- 11.7 Разграничение задач по администрированию сервиса предоставления сетевых настроек DHCP закрепляется в регламенте администрирования данного сервиса.
- 11.8 Внутренняя статистика использования вычислительных ресурсов при необходимости собирается, хранится и анализируется администратором приложений. Администраторы мониторинга могут помочь администратору приложений в ее сборе.
- 11.9 Если внесение изменений в конфигурацию вычислительных ресурсов технически возможно администратором приложений, то данные изменения производятся администратором приложений.
- 11.10 Серверами подразделений, не включенными в пул вычислительных ресурсов, управляют сотрудники или администраторы этих подразделений. Администраторы этих подразделений (а при их отсутствии - руководители) являются администраторами приложений для данных серверов и должны осуществлять все соответствующие функции на данных серверах, а также поддерживать аппаратную часть серверов. Поддержка УИТИ данных серверов осуществляется только в сетевой части до сетевого интерфейса сервера (только при условии размещения сервера в сети УрФУ) и в части инженерной инфраструктуры (только при условии размещения серверов в серверных помещениях ДИТ или ЦОД ДИТ). Доступ к консоли таких серверов не предоставляется. Администратор приложений должен самостоятельно обеспечить доступ к консоли через корпоративную сеть или выполнять работы в консоли физически находясь непосредственно около сервера.
- 11.11 В случаях исключения компонентов вычислительных мощностей из пула вычислительных ресурсов при размещении на таких компонентах виртуальных машин, они переносятся инфраструктурными администраторами. Если на данных компонентах предоставлены вычислительные мощности иного типа, то их перенос осуществляется администратором приложений за разумное время.
- 11.12 Инженерный отдел по запросам сервисных, сетевых администраторов и администраторов приложений устанавливает, перемещает и демонтирует оборудование в серверных помещениях и центрах обработки данных, подключает необходимые коммуникации (сети), обеспечивает бесперебойную подачу электроэнергии и охлаждение, а также по инструкциям нажимает аппаратные кнопки и переключатели на оборудовании.

11.13 Служба технической поддержки ДИТ организует регистрацию и маршрутизацию инцидентов, полученных от администраторов приложений.

12. Соглашение об уровне обслуживания

12.1 Управление изменениями. ДИТ использует структурированный подход для управления изменениями в инфраструктуре хостинга с помощью механизмов формального запроса и утверждения изменений. Любое изменение может принадлежать к одной из двух категорий: Запланированное и Аварийное.

12.2 Запланированные периоды обслуживания позволяют ДИТ выполнять необходимые административные действия и процедуры с инфраструктурой хостинга (связанные с ограничением работы сервиса и предоставленных вычислительных ресурсов), а также проводить его модернизацию.

12.3 Инженерный отдел, инфраструктурные и сетевые администраторы должны поддерживать работу хостинга режиме 24 часа в сутки, 7 дней в неделю и 365 дней в году без простоев, за исключением случаев проведения запланированных профилактических работ на инфраструктуре пула вычислительных ресурсов.

12.4 Инфраструктура хостинга может работать в двух режимах: основной и аварийный. При основном режиме сервис предоставляется согласно настоящему соглашению о качестве обслуживания. В аварийном режиме возможны отклонения от соглашения о качестве обслуживания.

12.5 Допускаются внеплановые (аварийные) простои в работе хостинга суммарно не более 96 часов в год.

12.6 Инфраструктурные и сетевые администраторы должны за 5 рабочих дней предупреждать администраторов приложений о запланированных профилактических работах на инфраструктуре хостинга, которые приведут или могут привести к неработоспособности сервиса хостинга и/или временному прекращению предоставления вычислительных ресурсов более чем на 2 минуты.

12.7 Для одного предоставленного вычислительного ресурса (в том числе виртуальной машины) максимальное число запланированных профилактических работ на инфраструктуре хостинга, произведенных не по инициативе администратора приложений, с остановкой предоставленных вычислительных ресурсов более чем на 2 минуты – 3 раза в месяц.

- 12.8 Администраторы приложений должны согласовать предложенное время проведения запланированных профилактических работ в диапазоне 2-х рабочих дней, следующих после 5-и рабочих дней с момента предупреждения инфраструктурам администраторам.
- 12.9 Если администратор приложений не согласовывает время запланированных профилактических работ в течении 2-х рабочих дней и не направляет мотивированный отказ, то профилактические работы могут быть проведены в произвольное время с уведомлением администратора приложений с помощью корпоративной почты.
- 12.10 Максимальное время одного простоя во время проведения запланированных профилактических работ зависит от объема данных в предоставленных вычислительных ресурсах. При объеме данные до 80 GB – до 5 часов. При объеме данных до 1 ТБ – до 24 часов. При объеме данных от 1 ТБ – 24 часа.
- 12.11 Допускается проведение профилактических работ на инфраструктуре хостинга в неограниченном объеме без уведомления администраторов приложений при условии отсутствия влияния на доступность и работоспособность предоставленных вычислительных ресурсов, либо если это влияние приведет к не более чем двукратному 2-х минутному перерыву в работе сервиса в течение одного рабочего дня.
- 12.12 При обеспечении высокой доступности вычислительного ресурса допускается остановка вычислительного ресурса с двухминутным перерывом перед перезапуском на той же площадке не чаще 3-х раз в неделю.
- 12.13 При отсутствии высокой доступности сервиса допускается остановка сервиса при поломках аппаратной части до момента восстановления сервиса, осуществляющемся в плановом режиме в рабочее время, либо отзыва вычислительных мощностей из пула вычислительных ресурсов с прекращением предоставления вычислительных ресурсов на данном оборудовании.
- 12.14 Помимо проведения запланированных профилактических работ, приостановка услуг для конкретного предоставленного вычислительного ресурса допускается в неограниченном объеме при выполнении заявок от администратора приложений (например, при изменении диска и иных). Приблизительное оценочное время, необходимое для выполнения заявки, при наличии информации сообщается администратору приложений и согласовывается с ним.
- 12.15 Все администраторы должны выполнять предписания инфраструктурных администраторов, связанных с восстановлением документированной структуры и дизайна сервиса хостинга в течение 3-х рабочих дней. При угрозах негативного

влияния на сервисы подразделений, данные изменения должны выполняться в приоритетном порядке.

12.16 В плановом непериприоритетном режиме в рабочее время ДИТ осуществляется восстановление:

- Зарезервированных компонентов инфраструктуры хостинга;
- Одного предоставленного вычислительного ресурса (сервера или виртуальной машины);
- Возможность использования портала.

12.17 В приоритетном порядке в рабочее время ДИТ осуществляется восстановление:

- Незарезервированных компонентов инфраструктуры хостинга в одном кампусе (согласно стандарту IP-адресации);
- Вышедших из строя всех частей зарезервированного компонента инфраструктуры хостинга в одном кампусе (согласно стандарту IP-адресации);
- Сетевых коммуникаций внутри одного кампуса (согласно стандарту IP-адресации);
- Восстановление систем управления инфраструктурой пула вычислительных ресурсов.

12.18 В наиболее приоритетном порядке ДИТ осуществляется восстановление:

- Вышедшей из строя всех частей зарезервированного компонента инфраструктуры хостинга при наличии проблем в нескольких кампусах;
- Сетевых коммуникаций между кампусами.

12.19 Для организации наиболее надежных сервисов администраторам приложений следует обеспечивать катастрофоустойчивость сервисов. Катастрофоустойчивость и высокая доступность должны обеспечиваться в соответствии с нормативной документацией, регламентами и инструкциями, разработанными инфраструктурными и сетевыми администраторами.

12.20 Сетевые администраторы осуществляют создание, настройку и документирование требуемых новых сегментов сетей для пула вычислительных ресурсов по заявке инфраструктурных администраторов в течение 3-х дней на всем коммуникационном оборудовании и всем коммуникационном и управляющем ПО.

12.21 Сетевые администраторы осуществляют настройку межсетевых экранов корпоративной сети в соответствии с требованиями сервисов с учетом действующей нормативной документации по корпоративной сети УрФУ в течение 3-х дней.

12.22 Заявки иного рода сетевыми администраторами должны обрабатываться и, при наличии технической возможности, решаться в течении 3-х дней.

- 12.23 Обеспечивается качество сетевой связности между предоставленными вычислительными ресурсами:
- Скорость связи до 50 мегабит. Более 50 мегабит и до 2 гигабит может предоставляться после согласования с УИТИ;
 - Потери не более 3 %;
 - Задержки не более 10 миллисекунд в среднем за 2 минуты;
 - Методика тестирования – согласно положению о КСПД УрФУ.
- 12.24 Обеспечивается качество сетевой связности между предоставленными вычислительными ресурсами и сетью до вышестоящих Интернет-провайдеров:
- Скорость связи до 10 мегабит. Более 10 мегабит может предоставляться после согласования с ДИТ;
 - Потери не более 3 %;
 - Методика тестирования – согласно положению о КСПД УрФУ.
- 12.25 При необходимости проведения профилактических работ на коммуникационном оборудовании, которые могут нарушить качество обслуживания сетевой связности, о таких работах уведомляются администраторы приложений не менее чем за 5 рабочих дней.
- 12.26 Инженерный отдел выполняет заявки инфраструктурных, сетевых администраторов в течении 10 рабочих дней.
- 12.27 По согласованию с ДИТ могут предоставляться иные соглашения о качестве обслуживания коммуникационной и вычислительных компонент. Такие соглашения могут повлечь дополнительные затраты подразделения на проектирование, внедрение и поддержку нестандартных решений.

13. Инфраструктура пула вычислительных ресурсов

13.1 Инфраструктура пула вычислительных ресурсов состоит из аппаратной составляющей (вычислительные мощности) и программной составляющей с централизованным управлением и интеграцией всех компонентов.

13.2 В аппаратную часть инфраструктуры пула вычислительных ресурсов входят и могут входить:

- Унифицированные и однотипные вычислительные узлы;
- Аппаратные компоненты, управляющие вычислительными узлами;
- Системы хранения данных;
- Коммуникационное оборудование;
- Межсетевые экраны.

13.3 Аппаратная часть должна удовлетворять техническим требованиям дизайна, иметь возможность интеграции с остальной инфраструктурой.

13.4 Системы хранения данных и вычислительные узлы в одном кампусе должны быть размещены в серверном помещении ДИТ с иными вычислительными мощностями пула вычислительных ресурсов.

13.5 В программную часть инфраструктуры пула вычислительных ресурсов входят:

- Гипервизоры;
- Сервера для управления, мониторинга хостинга и резервного копирования вычислительных ресурсов и инфраструктуры пула вычислительных ресурсов;
- Сервера для предоставления доступа к сервису предоставления вычислительных ресурсов, в том числе к порталу;
- Коммуникационное ПО для передачи данных и средства по его управлению;
- Основные сервисы УрФУ: корпоративная сеть, единый каталог пользователей, почтовая система, сервис предоставления сетевых настроек DHCP, сервис регистрации разрешения имен DNS, сервис инфраструктуры открытых ключей PKI, сервис точного времени NTP, сервис обновления ПО Microsoft WSUS и сервис активации, управления ключами KMS и сервисы аутентификации RADIUS и TACACS+;
- Системы мониторинга, сбора статистики и уведомления о инцидентах.

13.6 В сети инфраструктуры пула вычислительных ресурсов включаются все физические или виртуальные сетевые устройства необходимые для коммуникаций серверов, вычислительных ресурсов или виртуальных машин с корпоративной сетью,

сетью Интернет или друг с другом в соответствии с соглашением об уровне обслуживания.

- 13.7 Инфраструктура пула вычислительных ресурсов основывается на полном резервировании компонентов инфраструктуры (как коммуникационных, так и серверных) и размещении инфраструктурных компонентов в нескольких кампусах. Для сетевой части осуществляется резервирование всех коммуникационных потоков на физическом, канальном и сетевом уровне.
- 13.8 Полный доступ или неограниченный доступ к инфраструктуре пула вычислительных ресурсов (но не к предоставленным администраторам приложений вычислительным ресурсам), либо любой его аналог, могут иметь только инфраструктурные администраторы и сама система управления виртуализацией.
- 13.9 Портал может быть доступен только из корпоративной сети УрФУ.
- 13.10 Управляющие и программные компоненты пула вычислительных ресурсов должны размещаться в пуле вычислительных ресурсов.
- 13.11 Инфраструктура пула вычислительных ресурсов управляется УИТИ. Иным подразделениям университета не могут быть делегированы полномочия по управлению инфраструктурой пула вычислительных ресурсов.
- 13.12 Изменения в настройки инфраструктуры пула вычислительных ресурсов по запросам администраторов приложений не вносятся.
- 13.13 Конфигурация и дизайн инфраструктуры пула вычислительных ресурсов по запросу администраторов приложений не меняются.
- 13.14 Инфраструктура пула вычислительных ресурсов не может быть расширена или сокращена за счет компонентов, нарушающих дизайн хостинга или его компонентов, противоречащих их нормативной документации (например, нарушающих полное резервированием компонентов инфраструктуры).
- 13.15 Все компоненты инфраструктуры должны иметь сетевые настройки, соответствующие Положению об использовании адресации интернет протокола версии 4 в сети Уральского федерального университета имени первого Президента России Б.Н. Ельцина.
- 13.16 Не допускается создание дополнительных пулов вычислительных ресурсов, а также отдельной инфраструктуры по его управлению.

14. Пул вычислительных ресурсов

- 14.1 Пул вычислительных ресурсов является частью инфраструктуры сервиса хостинга.
- 14.2 В одном кампусе может размещаться не более одного помещения (или группы смежных помещений), в которых размещаются вычислительные мощности пула вычислительных ресурсов.
- 14.3 Инфраструктурные и сетевые администраторы должны поддерживать унифицированность, однородность аппаратных и программных решений, централизацию управления и однотипность сетевого и серверного оборудования, составляющего пул вычислительных ресурсов.
- 14.4 Подразделение может резервировать часть ресурсов пула вычислительных ресурсов для своих задач, если оно участвовало в расширении пула вычислительных ресурсов (приобретение аппаратных и программных компонент пула) за счет собственных средств.
- 14.5 УИТИ поддерживает и включает в пул вычислительных ресурсов те аппаратные и программные компоненты, которые:
- Полностью переданы в управление УИТИ;
 - Учитываются на балансе ДИТ;
 - Соответствуют требованиям техно-рабочей документации и дизайну хостинга, спецификациям, разработанными УИТИ, и иным нормативным документам УрФУ и имеют достаточный функционал;
 - Совместимы с текущими аппаратными и программными компонентами инфраструктуры хостинга;
 - Имеют возможность достаточной интеграции с другими компонентами инфраструктуры пула вычислительных ресурсов.
- 14.6 Окончательное решение о возможности расширения типа поддерживаемого оборудования в пуле вычислительных ресурсов принимается инфраструктурными администраторами, которые при необходимости проводят тестирование или проверку документации.
- 14.7 При поломке аппаратного обеспечения, окончания срока действия лицензий или прекращении поддержки, ресурсы могут исключаться из пула вычислительных ресурсов.

15. Порядок предоставления сервиса хостинга

- 15.1 Для получения доступа ко всем возможностям хостинга компьютеры и сервера пользователей и подразделений должны иметь адресацию согласно Положением об использовании адресации интернет протокола версии 4 в сети Уральского федерального университета имени первого Президента России Б.Н. Ельцина.
- 15.2 Доступ к ряду возможностей хостинга для пользователей, компьютеров, серверов или иных устройств, не имеющих адресацию согласно указанному Положению, может быть ограничен или невозможен.
- 15.3 Для получения доступа ко всем возможностям хостинга компьютеры пользователей и подразделений должны быть присоединены к домену AT.URFU.RU, а подразделение должно иметь назначенного Администратора подразделения в едином каталоге пользователей, выполняющего функции администрирования компьютеров и раздела подразделения в едином каталоге пользователей, в соответствии с Регламентом администрирования единого каталога пользователей Active Directory «AT.URFU.RU».
- 15.4 Доступ к ряду возможностей хостинга для пользователей с компьютеров и устройств, не присоединенных к домену «AT.URFU.RU» может быть ограничен или невозможен.
- 15.5 Пользователь должен иметь назначенного администратора приложения, чтобы иметь возможность воспользоваться хостингом.
- 15.6 Не поддерживается предоставление хостинга при отсутствии администратора приложений.
- 15.7 Если у Пользователя отсутствует администратор приложений, то предоставление вычислительных ресурсов подразделению прекращается. Если в течении 14 дней администратор приложений не назначается, то все данные Пользователю выделенные вычислительные ресурсы отключаются, а еще через 14 дней возвращаются в пул вычислительных ресурсов без возможности восстановления.
- 15.8 При нарушении администратором приложений данного регламента, сервис хостинга (или его часть) для данного администратора приложения или Пользователя приостанавливается, а через 10 рабочих дней предоставленные вычислительные ресурсы отзываются.
- 15.9 Для получения ресурсов и виртуальных серверов в «частном облаке» УрФУ факультетам и структурным подразделениям университета необходимо заполнить мотивированную Заявку на имя директора по информационным технологиям от Пользователя с указанием описания сервиса, приложений или информационной

системы со всеми компонентами и требованиями к вычислительным ресурсам, а также контактных данных назначенного Администратора приложений. Для формулировки Заявки можно воспользоваться Формой заявки на предоставление вычислительных ресурсов (см. Приложение).

- 15.10 Заявка на хостинг согласуется после подписания и до поступления адресату по следующему маршруту:
- a. Начальник ОБС (оценивает техническую возможность предоставления Хостинга),
 - b. Начальник УИБ (оценивает возможность предоставления хостинга с точки зрения информационной безопасности).
- 15.11 Директор по информационным технологиям принимает решение о предоставлении Хостинга основываясь на решениях начальника ОБС и начальника УИБ.
- 15.12 В случае положительного решения по заявке, заявка передаётся на исполнение инфраструктурным администраторам хостинга.
- 15.13 В случае отрицательного решения по заявке, пользователю сообщается мотивированный отказ в предоставлении хостинга.
- 15.14 Заявка должна быть подана средствами системы электронного документооборота.
- 15.15 В случае отсутствия в подразделении назначенного за работу в системе электронного документооборота сотрудника, заявку необходимо направить в ДИТ через службу технической поддержки посредством электронной почты на адрес sd@urfu.ru для дальнейшей её регистрации в системе электронного документооборота.
- 15.16 Параметры предоставляемых вычислительных ресурсов должны согласовываться администратором приложений с инфраструктурным администратором. Предоставление вычислительных ресурсов осуществляется только после взаимного согласования параметров и объемов предоставляемых вычислительных ресурсов. Предоставление вычислительных ресурсов осуществляется только при наличии достаточного объема свободных и незарезервированных ресурсов в пуле вычислительных ресурсов.
- 15.17 При требовании чрезмерного высокого объема вычислительных ресурсов, администратор приложений должен мотивировать необходимость именно данного объема ресурсов, а не меньшего.

- 15.18 Администратор приложений самостоятельно создает виртуальные машины (при необходимости или возможности из шаблона) с согласованными параметрами с помощью инструкции по использованию портала.
- 15.19 Администратор приложений при необходимости самостоятельно устанавливает и настраивает ОС на аппаратном или виртуализованном аппаратном обеспечении внутри предоставленных ему вычислительных ресурсов.
- 15.20 При необходимости внесения специальных настроек в параметры предоставляемых вычислительных ресурсов и отсутствии технической возможности у администраторов приложений выполнить их, инфраструктурным администраторам направляется запрос на внесение настроек в предоставленный вычислительный ресурс. При наличии технической возможности внесения требуемых специальных настроек, они выполняются администратором приложений.
- 15.21 На одной виртуальной машине допускается размещение не более одного сервиса или не более одной информационной системы.
- 15.22 Администратор приложений должен своевременно обновлять ПО (включая утилиты поддержки виртуализации внутри гостевой ОС) в том числе по запросам инфраструктурных администраторов.
- 15.23 Размещение приложений или системного ПО с высоким потреблением IOPS (200 и более) требует предварительного согласования с инфраструктурным администратором.
- 15.24 Размещение приложений или системного ПО с большим потреблением IOPS (50 и более) и преобладающим профилем нагрузки – случайная запись (более 50% операций) требует предварительного согласования с инфраструктурным администратором.
- 15.25 В виртуальных машинах изменение настроек swar-файлов (файлов подкачки) или swar-разделов допускается только при согласовании с инфраструктурными администраторами. При недостатке оперативной памяти в виртуальной машине следует инициировать запрос увеличения объема доступной оперативной памяти или оптимизации размещенного приложения.
- 15.26 Имена операционных систем, установленных на предоставленных вычислительных ресурсах, должны соответствовать имени предоставленного вычислительного ресурса (например, имени виртуальной машины). Это обеспечивается администратором приложений.

15.27 Администратор приложений должен обеспечить наличие описания у вычислительного ресурса.

15.28 Для размещения ИСПДн и иных прикладных систем, хранящих и обрабатывающих персональные или конфиденциальные данные, в инфраструктуре пула вычислительных ресурсов необходимо выполнить ряд дополнительных шагов и требований для каждой конкретной ИС:

- Размещать такие прикладные системы на одной серверной площадке под управлением одного типа гипервизора Hyper-V на выделенных специально приобретённых серверах;
- В случае необходимости использования технологий живой миграции или репликации между различными серверными площадками использовать отдельную сертифицированную оптическую линию связи между площадками;
- Приобрести и использовать сертифицированную ФСТЭК серверную операционную систему для хостов и гостевых систем с сертифицированным дистрибутивом (Windows Server), и использовать выделенные логические диски (LUN) на СХД для сертифицированных серверных операционных систем. Обеспечить изоляцию трафика для данной прикладной системы на уровне выделенных VLAN'ов. При необходимости обмена трафиком данной прикладной системы с иными сетями – использовать сертифицированные межсетевые экраны и средства шифрования.
- Разработать для каждой конкретной прикладной системы ряд организационных и распорядительных документов, включая:
 - Комплект документации описывающий информационную систему, её предназначение, статус, жизненный цикл, ответственных лиц, а также методы безопасного доступа, администрирования, архивирования;
 - Описание объектов защиты;
 - Модель угроз. (Согласно текущему ТЗ проектируется инфраструктура, для которой угроза «перетекания» трафика из одного VLAN в другой на серверном оборудовании не является существенной);
 - Технические меры по защите конфиденциальной информации;
 - Регламенты и инструкции по технической эксплуатации системы;
- Регламент или инструкцию по уничтожению данных на носителях информации в случае их утилизации или замены по гарантийному случаю.

16. Порядок диагностики и решения проблем

16.1 При возникновении проблем с сервисами, информационными системами или приложениями на предоставленных вычислительных ресурсах порядок выполнения диагностики следующий:

- 16.1.1 В первую очередь администратор приложений выясняет с помощью удаленного доступа к вычислительному ресурсу для администрирования, а также доступа к консоли, работоспособна ли виртуальная машина или физический сервер, операционная система, драйвера, работает ли аппаратное обеспечение, имеется ли сетевая связность.
- 16.1.2 Если неработоспособен вычислительный ресурс и отсутствует доступ к консоли, то администратор приложений выполняет запрос инфраструктурными администраторам посредством ЕДС.
- 16.1.3 Если неработоспособна операционная система, либо драйвера, то администратор приложений выполняет восстановление работы операционной системы с помощью стандартных компонент и утилит, предлагаемых инфраструктурными администраторами; либо иных компонент и утилит, которые администратор приложений может использовать внутри ВМ.
- 16.1.4 Если причина проблем сразу не ясна администратору приложений следует провести перезагрузку сервера, перезапуск приложений и сервисов и/или выполнить иные стандартные способы диагностики.
- 16.1.5 Если неработоспособно аппаратное обеспечение, то администратор приложений выполняет запрос инфраструктурными администраторам посредством ЕДС.
- 16.1.6 Если отсутствует сетевая связность (при наличии корректных сетевых настроек), то администратор приложений выполняет запрос сетевым администраторам посредством ЕДС.
- 16.1.7 Если виртуальная машина, операционная система, драйвера и аппаратное обеспечение работают штатно, а сетевая связность имеется, то администратор приложений выполняет диагностику информационной системы, сервиса или приложения согласно документации по данному ПО.
- 16.2 При возникновении проблем с сервисами, информационными системами или приложениями на сервера, не включенных в пул вычислительных ресурсов, порядок выполнения диагностики следующий:
- 16.2.1 Администратор приложений выполняет диагностику сервера и сетевой связности.
- 16.2.2 Если отсутствует сетевая связность (при наличии корректных сетевых настроек), то администратор приложений выполняет запрос сетевым администраторам посредством ЕДС.
- 16.2.3 Если отсутствует электропитание или охлаждение, то администратор приложений выполняет запрос инженерному отделу посредством ЕДС.

- 16.2.4 В иных случаях администратор приложений выполняет самостоятельно восстановление сервера, приложения, информационной системы или сервиса.
- 16.3 При необходимости инфраструктурные и сетевые администраторы создают или перенаправляют запросы инженерному отделу или друг другу.

17. Параметры предоставляемых вычислительных ресурсов

- 17.1 Закрепление виртуальных машин на определенных физических серверах или разделах и дисках систем хранения данных не осуществляется.
- 17.2 Проброс портов (USB, COM), смарт-карт и иных устройств в виртуальную машину или на физический сервер из пула вычислительных ресурсов должен осуществляться программным способом администратором приложений. Инфраструктурные администраторы не могут менять настройки гипервизоров, инфраструктуры пула вычислительных ресурсов для проброса данных устройств.
- 17.3 Поддерживаются виртуальные машины только на гипервизорах HyperV и VMware ESXi.
- 17.4 Высокая доступность для виртуальных машин поддерживается.
- 17.5 Высокая доступность сервисов на иных типах предоставленных вычислительных ресурсов поддерживается только для сервисов, размещенных в отказоустойчивом кластере.
- 17.6 Катастрофоустойчивость сервисов поддерживается только при размещении серверов не менее чем на двух площадках и в соответствии с нормативной документацией по обеспечению катастрофоустойчивости.

18. Сетевая связность вычислительных ресурсов

- 18.1 Администраторам приложений запрещено использование сетевых мостов и агрегации сетевых соединений внутри предоставленных вычислительных ресурсов без согласования с инфраструктурными и сетевыми администраторами.
- 18.2 Разрешено использование только выданных сетевыми или инфраструктурными администраторами, либо инфраструктурой хостинга MAC-адресов и IP-адресов. Запрещена подделка сетевых адресов, как вручную, так и с использованием различного ПО (в том числе при использовании Windows Network Load Balancing) без согласования с сетевыми и инфраструктурными администраторами.
- 18.3 Между кампусами (согласно стандарту ИП-адресации) осуществляется сетевая связность на третьем уровне (L3).
- 18.4 При необходимости администратору приложений обеспечения связности между кампусами (согласно стандарту ИП-адресации) на втором уровне (L2), либо при необходимости обеспечения избыточных сетевых подключений, от запрашивающего Пользователя может потребоваться оплата организации нестандартных топологий сетевых подключений.
- 18.5 Сетевые администраторы и инфраструктурные администраторы могут потребовать у администратора приложений провести диагностику сетевой связности между предоставленным вычислительным ресурсом и иными сетевыми узлами (маршрутизаторами, серверами). Администратор приложений результаты диагностики должен предоставить сетевым и инфраструктурными администраторам.

19. Сетевая адресация вычислительных ресурсов

- 19.1 Все вычислительные ресурсы из пула вычислительных ресурсов должны иметь ИП-адреса согласно Положению об использовании адресации интернет протокола версии 4 в сети Уральского федерального университета имени первого Президента России Б.Н. Ельцина.
- 19.2 А при наличии статического или зарезервированного ip-адреса должны быть зарегистрированными в сервисе регистрации ip-адресов и ip-сетей согласно стандарту ip-адресации (ip.dit.urfu.ru), если ip-адресация на сетевом интерфейсе вычислительного ресурса вообще предусматривается.
- 19.3 IP-адрес на предоставляемых вычислительных ресурсах может быть статическим или быть полученным с помощью сервиса получения сетевых настроек

DHCP (динамическим). Согласно стандарту IP-адресации для всех сетевых устройств, включая сервера, используется DHCP для получения настроек.

- 19.4 Предоставление вычислительному ресурсу одного или более статического IP-адреса требует обязательного обоснования невозможности работы сервиса, приложения или информационной системы с DHCP администратором приложений. Необоснованное в достаточной степени назначение статического ip-адреса не допускается, а уже назначенные статические ip-адреса отзываются.
- 19.5 IP-адрес, полученный по DHCP на вычислительном ресурсе, может быть зарезервированным, а может не быть зарезервированным.
- 19.6 Настройка резервации получаемого по DHCP IP-адреса требует обязательного обоснования невозможности использования клиентами приложения, сервиса или информационной системы автоматически-регируемого DNS-имени предоставленного вычислительного ресурса администратором приложений. Сетевые администраторы могут обеспечить резервацию Ip-адреса также при необходимости настройки списка контроля доступа на межсетевых экранах.
- 19.7 IP-адрес на предоставленных вычислительных ресурсах может быть частным или публичным.
- 19.8 Предоставление публичного IP-адреса требует обязательного обоснования факта, что сервисом, приложением или информационной системой будут пользоваться пользователи из вне корпоративной сети через сеть Интернет, а иные способы публикации сервиса невозможны или непрактичны. Также для предоставления публичного IP-адреса администраторам приложений необходимо предоставить сетевым администраторам список протоколов, по которым клиенты из вне корпоративной сети через сеть Интернет будут использовать сервис.
- 19.9 Публичный IP-адрес на вычислительных ресурсах может быть размещен в сегменте DMZ (сегмент сервисы по стандарту ip-адресации) или во внутреннем сегменте корпоративной сети (сегмент подразделения по стандарту IP-адресации).
- 19.10 Предоставление публичного IP-адреса во внутреннем сегменте корпоративной сети требует обязательного обоснования невозможности размещения сервиса, приложения или информационной системы в сегменте DMZ, либо необходимости доступа сервиса к большому числу сетевых сегментов корпоративной сети по нескольким протоколам.
- 19.11 Частные ip-адреса согласно стандарту ip-адресации разделяются по нескольким сегментам. Администратор приложения должен предоставить достаточно информации

о размещаемых на предоставляемых вычислительных ресурсах для определения корректного сетевого сегмента для частного ip-адреса, либо определить корректный сетевой сегмент самостоятельно.

- 19.12 Другие варианты IP-адресации вычислительных ресурсов не допускаются.
- 19.13 По умолчанию всем вычислительным ресурсам предоставляются динамические (DHCP) частные ip-адреса без резерваций в клиентском сегменте.
- 19.14 При изменении требований, тип предоставленного ip-адреса может быть изменен.
- 19.15 IP-адреса назначаются на сетевой интерфейс предоставленных вычислительных ресурсов.
- 19.16 Одному вычислительному ресурсу (виртуальной машине) для одного сетевого интерфейса может быть назначено несколько статических ip-адресов из одного сетевого сегмента. Для этого администратор приложения должен предоставить обоснование необходимости данной конфигурации.
- 19.17 При назначении статического IP-адреса администратору приложений в обязательном порядке предоставляется только IP-адрес, маска подсети и шлюз по умолчанию, который соответствует стандарту ip-адресации. Остальными сетевыми параметрами (в том числе DNS, WINS, NTP) администратор приложений управляет самостоятельно. Например, получить IP-адреса внутренних кеширующих DNS-серверов администратор приложений может в соответствии с регламентом администрирования единого каталога пользователей at.urfu.ru (Active Directory). Например, адреса NTP можно получать, разрешая DNS-имя ntp.urfu.ru (так как ip-адрес может меняться). Ответственность за внесение и обновление таких настроек несет администратор приложений.
- 19.18 Администратор приложений при наличии необходимости устанавливает согласованный статический IP-адрес на предоставленный вычислительный ресурс самостоятельно.
- 19.19 При назначении статического IP-адреса или настройке резервации, часть возможностей хостинга может быть недоступна. Список таких возможностей, например, может включать в себя:
- Возможность перемещения виртуальных машин между зданиями;
 - Возможность автоматической настройки иных сетевых параметров (в том числе DNS, WINS). Администратору приложения потребуется самостоятельно поддерживать их актуальность;

- Автоматическое соответствие DNS-имени IP-адресу вычислительного ресурса. Администратору приложения потребуется самостоятельно обеспечивать поддержку соответствия по процедуре регистрации DNS-имени или настройке Dynamic DNS;
- Возможность загрузки по сети для установки, обновления и устранения неполадок с ОС.

19.20 Зарезервированные динамические ip-адреса, а также статические ip-адреса могут быть отозваны при неиспользовании в течении 20 рабочих дней.

19.21 Для обеспечения работы Dynamic DNS, чтобы IP-адрес и DNS-имя сохранялись и не изменялись при получении IP-адреса по протоколу DHCP администратор приложений должен отключить освобождения ip-адреса (dhcp release) при выключении сетевых интерфейсов, выключении или перезагрузки ОС.

19.22 Администраторы приложений отвечают за работоспособность и настройки сетевого адаптера внутри предоставленных ему вычислительных ресурсов, включая ip-адреса, DHCP-клиент и его настройки, сетевые драйвера и драйвера дисков и дисковых контроллеров и т.д. Если внутри ОС на предоставленных вычислительных ресурсах не работает DHCP-клиент, хотя DHCP-сервер с виртуальной машины доступен, то администратор приложений должен устранить проблему с DHCP-клиентом.

Приложение №1 к регламенту
предоставления вычислительных ресурсов на
основе технологий частного облака

Форма заявки на выделение вычислительных ресурсов

УрФУ

Подразделение

Директору по информационным
технологиям
И. А. Богданович

СЛУЖЕБНАЯ ЗАПИСКА

№ от

О выделении вычислительных
ресурсов

Прошу Вас выделить в инфраструктуре «Частного облака» УрФУ вычислительные ресурсы со следующими характеристиками:

Вычислительный ресурс № 1:

Описание и спецификация	
Назначение*	
Операционная система и её версия*	
Число процессорных ядер с частотой 2 ГГц	
Максимальный объем оперативной памяти	
Максимальный объем жесткого диска	
Дополнительные требования	
Организация сетевого доступа	
Требуется ли доступ из сети Internet, если да - указать сетевые протоколы и порты	
Требуется ли доступ к сети Internet	
Дополнительные требования к сетевому доступу	
Контакты	
Подразделение*	
Ф.И.О. Администратора приложений*	

Е-mail администратора приложений*	
Контактный телефон	
Примечания	

* - обязательные для заполнения сведения

Администратор приложений

И. О. Фамилия

Руководитель подразделения

И. О. Фамилия