	Министерство образования и науки Российской Федерации
	Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Рязанский государственный радиотехнический университет»

УТВЕРЖДАЮ
проректор по РиБ

С.В. Чернышев
«12» сентября

С.В. Чернышев
2012 г.

РАБОЧАЯ ИНСТРУКЦИЯ
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

*Создание и хранение резервных копий
конфигураций серверного и
каналообразующего оборудования центрального
сегмента корпоративной вычислительной сети*

Выпуск 01

Рязань 2012

Изменение №

Дата

1. Общие положения

1.1 Настоящая рабочая инструкция разработана в соответствии с приказом ректора РГРТУ №14 от 31.01.2012 «О сервере резервного копирования».

1.2 Рабочая инструкция предназначена для работников подразделений управления телекоммуникаций и информационных ресурсов, осуществляющих конфигурирование серверного и каналобразующего оборудования, входящего в состав центрального сегмента корпоративной вычислительной сети.

1.3 Рабочая инструкция может использоваться работниками других подразделений, осуществляющих сопровождение серверного оборудования, составляющего центральный сегмент корпоративной вычислительной сети университета.

1.4 Рабочая инструкция определяет правила хранения конфигурационных файлов серверного и каналобразующего оборудования, копий баз данных, файлов журналов и резервных копий серверного программного обеспечения.

1.5 Рабочая инструкции вводится в действие с даты её утверждения проректором по режиму и безопасности.

2. Цели создания и хранения копий конфигурационных файлов серверного и каналобразующего оборудования, копий баз данных, файлов журналов и резервных копий серверного программного обеспечения

2.1 Копии конфигурационных файлов серверного и каналобразующего оборудования, копий баз данных, файлов журналов и резервных копий серверного программного обеспечения создаются и хранятся для:

- повышения надёжности функционирования корпоративной сети РГРТУ и сокращения времени восстановления работоспособности в случае отказов аппаратного и программного обеспечения;
- обеспечения доступа к системному программному обеспечению оборудования с правами администратора в случае отсутствия штатного администратора;
- обеспечения возможности восстановления работоспособности оборудования в случае порчи конфигурационных файлов;
- обеспечения возможности восстановления баз данных;
- обеспечения централизованного доступа к файлам журналов;
- обеспечения возможности восстановления работоспособности серверного программного обеспечения.

2.2 Документация, составляемая при вводе в эксплуатацию новых серверов и функционирующих на них информационных системах, должна содержать разделы, связанные с процедурой создания резервных копий и восстановления. Целесообразно включать вопросы создания резервных копий и восстановления работоспособности с использованием резервных копий в программы и методики испытаний серверов и информационных систем.

2.3 Вопросы, связанные с резервным копированием и восстановлением, должны включаться в список регламентных работ по обслуживанию серверов и информационных систем.

<i>Изменение №</i>	<i>Дата</i>
--------------------	-------------

3. Управление паролями администратора для доступа к серверному и каналобразующему оборудованию центрального сегмента корпоративной вычислительной сети

3.1 Доступ к системному программному обеспечению серверного и телекоммуникационного оборудования с правами администратора осуществляется, как правило, с использованием регистрационного имени и пароля.

3.2 Регистрационное имя и пароль для доступа к оборудованию определяются работником, устанавливающим системное программное обеспечение.

3.3 Работник, устанавливающий системное программное обеспечение, должен сообщать регистрационные имена и пароли исключительно лицам, имеющим отношение к сопровождению установленного программного обеспечения в пределах их прав доступа.

3.4 После инсталляции работник доводит регистрационное имя и пароль (все регистрационные имена и пароли, кроме личных, в том случае, если их несколько) до сведения начальника отдела корпоративной информационной системы.

3.5 Начальник отдела корпоративной информационной системы ведёт журнал, в котором фиксирует регистрационные имена и пароли, кроме личных, для доступа к системному программному обеспечению серверного и коммуникационного оборудования с правами администратора. В журнале хранятся фамилии, имена, отчества, должности и регистрационные имена пользователей, имеющих доступ к системному программному обеспечению серверного и коммуникационного оборудования с правами администратора. Форму журнала определяет начальник отдела корпоративной информационной системы.

3.6 Не рекомендуется хранить регистрационные имена и пароли в электронном виде. Допускается хранение паролей в электронном виде на съёмном носителе в одном экземпляре без права копирования на компьютеры. Такой электронный носитель должен храниться в сейфе, доступ к носителю имеет только начальник отдела корпоративной информационной системы, а в случае его отсутствия работник, назначаемый начальником управления телекоммуникаций и информационных ресурсов.

3.7 В том случае, если работник изменяет или добавляет новое регистрационное имя и (или) пароль для доступа к оборудованию с правами администратора, он обязан поставить в известность об этом начальника отдела корпоративной информационной системы. Начальник корпоративной информационной системы вносит необходимые изменения в журнал.

3.8 Журнал регистрационных имён и паролей хранится в помещении, закреплённом за отделом корпоративной информационной системы. Шкаф (или ящик), в котором хранится журнал, должен быть закрыт на ключ. Ключ хранится у начальника отдела корпоративной информационной системы. Начальник отдела корпоративной информационной системы не имеет права выносить ключ за пределы отдела корпоративной информационной системы.

3.9 Работники, сопровождающие конкретное серверное и коммуникационное оборудование, имеют право вести собственные журналы (блокноты, тетради) в которых записывать регистрационные имена и пароли для доступа к системному программному обеспечению оборудования с правами администратора. В этих журналах (блокнотах, тетрадях) могут содержаться только записи, имеющие отношение к непосредственно сопровождаемому программистом оборудованию. Работники не имеют право выносить такие журналы (блокноты, тетради) за пределы помещений, закреплённых за управлением телекоммуникаций и информационных ресурсов.

3.10 В случае временного отсутствия (отпуск, командировка, болезнь и т.п.) работника, осуществляющего сопровождение конкретного серверного или коммуникационного оборудования, работник имеет право передавать журнал (блокнот, тетрадь) с регистрационными именами и паролями работнику, назначенному начальником отдела корпоративной информационной системы по согласованию с начальником управления телекоммуникаций и информационных ресурсов, который будет выполнять его обязанности во время его отсутствия. Работник, получивший журнал (блокнот, тетрадь) во временное использование, не имеет права копировать информацию о регистрационных ключах и паролях и обязан вернуть журнал (блокнот, тетрадь) после возвращения программиста, передавшего журнал (блокнот, тетрадь) во временное использование.

3.11 В случае негодности к использованию журнала (блокнота, тетради) работник обращается с целью его восстановления к начальнику отдела корпоративной информационной системы. Начальник отдела корпоративной системы изымает из использования пришедший в негодность журнал (блокнот, тетрадь) и предоставляет программисту всю информацию, необходимую ему для исполнения должностных обязанностей.

3.12 Во время временного отсутствия начальника отдела корпоративной системы его функции выполняет работник, назначаемый начальником управления телекоммуникаций и информационных ресурсов по согласованию с проректором по режиму и безопасности.

3.13 Если сопровождение серверного или коммуникационного оборудования, входящего в центральный сегмент корпоративной вычислительной сети, осуществляют работники, не являющиеся работниками управления телекоммуникаций и информационных ресурсов, то на них распространяются все правила настоящей рабочей инструкции в части управления паролями администраторов.

4. Документирование конфигураций серверного и коммуникационного оборудования

4.1 Все конфигурационные файлы серверного и коммуникационного оборудования, должны содержать комментарии (в том случае, если имеется техническая возможность создания таких комментариев), достаточные для их понимания работником, имеющим достаточную квалификацию. При отсутствии технической возможности создания комментариев создаётся файл описания конфигурационных файлов, в котором содержится описание изменяемых настроек и комментариев к ним. На файлы описаний распространяются все положения настоящей рабочей инструкции наравне с конфигурационными файлами. Файл описаний хранится вместе с конфигурационными файлами.

4.2 Запрещается использование конфигурационных файлов не содержащих достаточных комментариев.

4.3 За комментирование конфигурационных файлов несёт ответственность работник, осуществляющий инсталляцию и (или) сопровождение конкретного серверного оборудования. Начальник отдела корпоративной информационной системы имеет право требовать от работников качественно комментировать конфигурационные файлы, а работники обязаны выполнять требования начальника отдела корпоративной информационной системы.

4.4 Копии конфигурационных файлов должны храниться в электронном виде в централизованном хранилище таких файлов, обеспечивающих разграничение полномочий по доступу к ним и внесение в них изменений.

<i>Изменение №</i>	<i>Дата</i>
--------------------	-------------

4.5 Имена конфигурационных файлов, находящихся в централизованном хранилище, должны содержать указания на оборудование, в котором используется конфигурационный файл, и дату начала использования конфигурационного файла.

4.6 Конфигурационный файл, находящийся в хранилище конфигурационных файлов, должен содержать преамбулу, в которой описаны отличия этой версии конфигурационного файла от предыдущих версии, находящихся в хранилище, и причину возникновения этих отличий.

4.7 В централизованном хранилище рекомендуется хранить не менее 3 последних версий конфигурационного файла. Количество хранимых версий в каждом конкретном случае определяет начальник отдела корпоративной информационной системы. Все вопросы, связанные с удалением конфигурационных файлов из централизованного хранилища, решает начальник отдела корпоративной информационной системы.

4.8 Не реже 1 раза в год начальник отдела корпоративной информационной системы организует сохранение копии централизованного хранилища конфигурационных файлов на оптических дисках.

4.9 Оптический диск, содержащий копию хранилища конфигурационных файлов маркируется, путём указания того, что на данном диске хранится именно копия централизованного хранилища конфигурационных файлов с указанием даты создания копии.

4.10 Оптические диски, содержащие копии хранилища конфигурационных файлов (архив конфигурационных файлов), хранятся в помещении, закреплённом за отделом корпоративной информационной системы в шкафу или ящике, запирающемся на ключ. Такие оптические диски образуют архив конфигурационных файлов.

4.11 Начальник отдела корпоративной информационной системы поддерживает в актуальном состоянии опись архива конфигурационных файлов. Опись архива конфигурационных файлов представляет собой документ, в котором фиксируются даты поступления оптических дисков в архив.

4.12 Начальник отдела корпоративной информационной системы ведёт журнал выдачи оптических дисков из архива конфигурационных файлов, в котором отмечает каждый случай выдачи оптического диска, находящегося в архиве: кому выдан диск, когда, с какой целью, когда возвращён. Все операции с оптическими дисками осуществляются под личную роспись работника, получающего оптический диск и роспись начальника отдела корпоративной информационной системы. Выдача оптических дисков осуществляется на основании служебной записки от имени руководителя подразделения на имя начальника отдела корпоративной вычислительной системы.

4.13 Выдача оптических дисков работникам управления телекоммуникаций и информационных ресурсов осуществляется начальником отдела корпоративной вычислительной системы без предоставления служебной записки. При этом должна производиться запись в журнал выдачи оптических дисков.

4.14 Опись архива конфигурационных файлов, журнал выдачи оптических дисков из архива и папка со служебными записками хранятся в том-же шкафу или ящике, в котором хранится архив конфигурационных файлов.

4.15 Начальник отдела корпоративной информационной системы обязан предоставлять доступ к архиву конфигурационных файлов ректору, проректору по режиму и безопасности и начальнику управления телекоммуникаций и информационных ресурсов, работникам, имеющим такое право на основании распоряжения ректора или проректора по режиму и безопасности, по их первому требованию.

4.16 Ответственность за создание хранилища конфигурационных файлов и архива конфигурационных файлов, их сохранность а также обеспечение доступа к ним несёт начальник отдела корпоративной информационной системы.

4.17 Работники отдела корпоративной информационной системы имеют право на чтение любых конфигурационных файлов, содержащихся в централизованном хранилище.

4.18 Во время отсутствия начальника отдела корпоративной информационной системы его функции по доступу к централизованному хранилищу конфигурационных файлов выполняет один из сотрудников управления телекоммуникаций и информационных ресурсов, назначаемых начальником управления телекоммуникаций и информационных ресурсов, по согласованию с проректором по режиму и безопасности.

5. Создание и хранение резервных копий баз данных

5.1 Создание и хранение резервных копий баз данных производится в целях обеспечения восстановления работоспособности информационных систем различного назначения, использующих системы управления базами данных.

5.2 Создание резервных копий баз данных возлагается на администратора, сопровождающего информационную систему.

5.3 Начальник отдела корпоративной информационной системы имеет право ставить в известность руководителя подразделения, сопровождающего любую информационную систему, функционирующую на серверном оборудовании, размещённом в серверной РГРТУ, о том, что создание резервных копий баз данных информационной системы не производится или производится ненадлежащим образом.

5.4 Копирование и хранение баз данных, содержащих персональные данные, осуществляется оператором персональных данных РГРТУ.

5.5 Ответственность за создание и хранение копий баз данных несёт руководитель подразделения, ответственного за функционирование информационной системы, исполнителем процедуры создания и сохранения копий является работник, осуществляющий сопровождение информационной системы.

5.6 Способ создания копий баз данных определяет работник, осуществляющий сопровождение информационной системы. Выбранный способ согласуется с руководителем подразделения и начальником отдела корпоративной информационной системы.

5.7 Частоту создания копий баз данных определяет администратор соответствующего сервера, исходя из значимости данных, хранимых в базе данных, и частоты их изменения.

6. Создание и хранение резервных копий программного обеспечения серверного оборудования

6.1 Решение о хранении полной копии программного обеспечения серверного оборудования принимает администратор сервера по согласованию с начальником отдела корпоративной информационной системы.

6.2 При принятии решения о хранении полной копии принимаются во внимание технические возможности по осуществлению такого хранения в централизованном хранилище.

6.3 Резервные копии программного обеспечения серверного оборудования, о целесообразности хранения которых принято положительное решение, обновляются после каждого изменения, но не реже 1 раза в год.

<i>Изменение №</i>	<i>Дата</i>
--------------------	-------------

7. Хранение копий файлов журналов

7.1 Состав файлов журналов серверного и телекоммуникационного оборудования, копии которых хранятся в централизованном хранилище, определяется работником, сопровождающим серверное или телекоммуникационное оборудование, согласуется с начальником отдела корпоративной информационной системы и утверждается начальником управления телекоммуникаций и информационных ресурсов.

7.2 Ответственность за хранение копий файлов журналов несёт работник, осуществляющий сопровождение сервера или информационной системы.

7.3 Контроль за хранением копий файлов журналов осуществляет начальник отдела корпоративной информационной системы.

7.4 Частота обновления копий файлов журналов определяется администратором серверного или телекоммуникационного оборудования, исходя из объёмов файлов журналов и практической целесообразности хранения их копий.

7.5 Рекомендуемая продолжительность хранения копий файлов журналов — 1 год.

8. Централизованное хранилище (сервер резервного копирования) конфигурационных файлов, копий баз данных, файлов журналов и полных копий серверного программного обеспечения

8.1 Для обеспечения централизованного хранения конфигурационных файлов, копий баз данных, файлов журналов и полных копий серверного программного обеспечения создаётся централизованное хранилище (сервер резервного копирования).

8.2 Хранилище предназначено для хранения копий конфигурационных файлов, копий баз данных, копий файлов журналов и полных копий серверного программного обеспечения, сопровождаемых управлением телекоммуникаций и информационных ресурсов.

8.3 Сопровождение аппаратных и программных средств централизованного хранилища осуществляет отдел корпоративной информационной системы.

8.4 Начальник отдела корпоративной информационной системы имеет право принимать решение о возможности хранения конфигурационных файлов, копий баз данных, копий файлов журналов, полных копий серверного программного обеспечения информационных систем, сопровождаемых другими подразделениями университета, при условии, что серверное оборудование, на котором функционируют информационные системы, размещено в серверной РГРТУ. При принятии решения о возможности использования централизованного хранилища другими подразделениями, начальник отдела корпоративной информационной системы руководствуется техническими характеристиками централизованного хранилища.

8.5 Принцип организации централизованного хранилища определяет начальник отдела корпоративной информационной системы.

9. Технические вопросы сопровождения сервера резервного копирования

9.1 Подключение к серверу резервного копирования

9.1.1 Доступ к серверу резервного копирования по протоколу FTP

Для подключения к серверу резервного копирования по протоколу ftp может быть использован любой ftp-клиент.

<i>Изменение №</i>	<i>Дата</i>
--------------------	-------------

9.1.2 Доступ к серверу резервного копирования по протоколу NFS с клиентских серверов, функционирующих под управлением операционной системы FreeBSD

Для того, чтобы подключиться к серверу резервного копирования с сервера, функционирующего под управлением операционной системы FreeBSD, необходимо выполнить один из двух следующих вариантов действий.

1) В файл `/etc/rc.conf` добавить

```
nfs_client_enable="YES"
```

После этого запустить `nfsclient` с помощью команды

```
# /etc/rc.d/nfsclient start
```

2) Запустить клиент без редактирования файла `rc.conf`

```
# /etc/rc.d/nfsclient onestart
```

Далее монтировать сетевую папку командой

```
# mount -t <nfs-type> <host>:/home/backups/<имя_пользователя>/dumps/  
    </local/directory>
```

где:

`<nfs-type>` - для freeBSD - `nfs`, для Linux может быть `nfs` или `nfs4`;

`<host>` - адрес сервера резервного копирования.

После завершения копирования на сервер резервного копирования необходимо размонтировать с помощью команды:

```
# umount </local/directory>
```

9.2 Добавление пользователя на сервере резервного копирования

Для добавления нового пользователя на сервере резервного копирования необходимо выполнить следующие команды:

```
useradd -M -d /home/backups/<имя_пользователя> -s /sbin/nologin -G <имя_группы>  
    <имя_пользователя>
```

```
passwd <имя_пользователя>
```

```
mkdir /home/backups/<имя_пользователя>
```

```
cp -R /home/templates/ /home/backups/<имя_пользователя>
```

```
chown -R <имя_пользователя>.<имя_пользователя> /home/backups/<имя_пользователя>
```

```
chmod 700 /home/backups/<имя_пользователя>
```

где `<имя_группы>=admin_backup`

9.3 Добавление каталога на NFS-сервере

Для добавления каталога на NFS-сервере необходимо внести следующие изменения в файл `/etc/exports`:

```
/home/backups/<ip_адресс_сервера>/dumps/ \
```

```
    <ip_адресс_сервера>(rw, sync, all_squash, anonuid= <uid>, anongid= <gid>)
```

9.4 Добавление пользователя на FTP-сервере

Для того, чтобы добавить пользователя на ftp-сервере, необходимо добавить имя пользователя в файл `/etc/vsftpd/conf/userlist`. После этого создать файл с именем пользователя в папке `/etc/vsftpd/conf_user/` и добавить в созданный файл строку `write_enable=YES` с помощью команды

```
# echo "write_enable=YES" > /etc/vsftpd/conf_users/<имя_пользователя>
```


9.5 Ограничение выделяемого дискового пространства

Для определения существующих ограничений дискового пространства и установки новых ограничений необходимо использовать следующие команды.

```
# quota <имя пользователя> - просмотр информации по ограничениям для указанного пользователя;
# repquota /home — просмотр информации по ограничениям для всех пользователей;
# edquota <имя пользователя> - открывает файл для редактирования файл, содержащий описание ограничений для пользователя. Ограничение дискового пространства указывается в четвертом столбце таблицы, содержащейся в открытом файле:
```

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/mapper/vg_backup-lv_home	20	0	40000	5	0	0

9.6 Добавление разрешающих правил в фаервол

Для того, чтобы добавить разрешающие правила, выполните следующие команды:

```
# iptables -A -p tcp -s <адрес сервера> -d <адрес backup-сервера> -j ACCEPT
# service iptables save
```

9.7 Добавление пользователя и разрешений с помощью скрипта

В папке `/usr/local/etc` сервера резервного копирования находится скрипт `add_server_backup` выполняющий действия, описанные в разделах 9.2-9.4 настоящей рабочей инструкции. Скрипт `add_server_backup` уменьшает трудоёмкость добавления пользователя.

Добавление правил в фаервол и ограничение выделяемого дискового пространства осуществляются вручную с помощью описанных команд.

10. Заключительные положения

10.1 Изменения в настоящее положение вносят начальник управления телекоммуникаций и информационных ресурсов или начальник отдела корпоративной информационной системы по согласованию с проректором по режиму и безопасности.

РАЗРАБОТАНО:

Начальник управления телекоммуникаций
и информационных ресурсов




А.А. Митрошин

Начальник отдела корпоративной
информационной системы



В.Ф. Тетёркин

Программист 1 категории
отдела корпоративной информационной системы



А.В.Цуканов

Изменение №

Дата

СОГЛАСОВАНО:

Руководитель службы качества



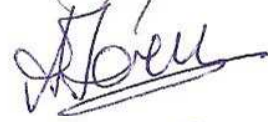
И.В. Горюнов

Начальник правового управления



А.А. Галицын

Директор ЦНИТ



А.М. Гостин

Начальник отдела
информационных ресурсов



А.А. Новиков

Изменение №

Дата