|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Регламент резервного копирования**

“Программный комплекс удаленного мониторинга и контроля за работой медицинского оборудования с предиктивным механизмом выявления наступления неисправностей”

**Москва**

**2024**

#

[**1. Введение 3**](#_fccwrsmsvvye)

[**2. Характеристики программного обеспечения 4**](#_3w7555un6cca)

[**3. Резервное копирование данных Комплекса 4**](#_p29w8488lg2y)

[3.1. Порядок резервного копирования 4](#_6b7zm1a1s1aw)

[3.1.1. Методика резервного копирования 5](#_6a5uhbwups7s)

[3.1.2. Обязанности лиц, ответственных за резервное копирование и восстановление данных 6](#_ev4uw4pdeizk)

[3.1.3. Восстановление информации из резервных копий 7](#_rk6c5f40uwgy)

[**4. Перечень сокращений 8**](#_xgxiree3hajj)

#

# Введение

Обеспечение мероприятий по резервному копированию - это набор организационно-технических решений, направленных на обеспечение сохранности данных и непрерывности функционирования Программного комплекса удаленного мониторинга и контроля за работой медицинского оборудования с предиктивным механизмом выявления наступления неисправностей. В настоящем документе рассмотрены базовые организационно-технические мероприятия, направленные на обеспечение сохранности данных и непрерывности функционирования комплекса

# Характеристики программного обеспечения

Программное обеспечение серверной стороны Комплекса включает

1. Операционная система: Debian 12.
2. Необходимое программное обеспечение:
3. комплект разработчика приложений на языке PHP Laravel8;
4. веб-сервер NGINX;
5. СУБД PostgreSQL. Сервер баз данных может быть установлен на другом компьютере (это рекомендуемый режим для создания более производительных конфигураций).

# Резервное копирование данных Комплекса

Резервное копирование и размещение резервных копий БД и Комплекса должно осуществляться на серверах облачной инфраструктуры Комплекса

## Порядок резервного копирования

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью. Расписание заданий выполняется по московскому времени. Методика проведения резервного копирования описана в п. 3.1.1. Ответственными лицами являются ответственный за резервное копирование и администратор резервного копирования Системы.

Периодичность проведения резервного копирования, срок хранения резервных копий, количество хранимых копий и график резервного копирования приведены в Таблице 3.1.

Таблица 3.1 – Расписание автоматического резервного копирования

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование** | **Периодичность** | **Срок****хранения** | **Количество хранимых копий** | **График резервного копирования** |
| 1. Прикладное и системное программное обеспечение
 |
| 1. Годовая копия (извлекается из библиотеки)
 | 1 раз в год | 1 год | 1 шт. | в 24:00 31 декабря каждого года |
| 1. Полная копия (хранится в библиотеке)
 | 1 раз в месяц | 1 месяц | 1 шт. | ежемесячно, в 24:00 последнего календарного дня месяца  |
| 1. Системный журнал и конфигурационные файлы (хранится в библиотеке)
 | 1 раз в сутки | 3-ое суток | 3 шт. | в 24:00 ежедневно |
| 1. Базы данных
 |
| 1. Полугодовая копия (извлекается из библиотеки)
 | 2 раза в год | 1 год | 2 шт. | в 24:00 31 декабря и 31 июня каждого года |
| 1. Полная копия (хранится в библиотеке)
 | 2 раза в неделю | 1 месяц | 5 шт. | в 24:00 каждой среды и субботы |

### Методика резервного копирования

Запись резервной копии осуществляется в специальный раздел дисковой подсистемы сервера резервного копирования. При этом количество хранимых копий, в том числе полных, аккумулированных на специальной дисковой системе, не должно быть менее одной, а срок хранения должен составлять 3-е суток, чем достигается возможность оперативного восстановления со специального раздела дисковой подсистемы.

В случае если система резервного копирования находится в аварийном состоянии, то в этот период времени осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

В целях контроля корректности выполнения резервного копирования выполняются процедуры тестирования резервных копий, в том числе:

* тестирование целостности резервных копий;
* тестирование восстановления из резервных копий.

При проведении тестирования целостности резервной копии осуществляется проверка по контрольным суммам блоков данных.

В случае восстановления из резервной копии выполняется тестирование, моделирующее сценарий сбоя.

Тестирование резервных копий производится со следующей периодичностью:

* тестирование целостности резервной копии – не реже 1 раза в месяц;
* тестирование восстановления из резервной копии – не реже 1 раза в 6 месяцев.

###

### Обязанности лиц, ответственных за резервное копирование и восстановление данных

Обязанности ответственного за резервное копирование:

* контроль наличия системных ошибок процесса резервного копирования;
* извещение администратора резервного копирования в случае возникновения ошибок или нештатных ситуаций.

Обязанности администратора резервного копирования:

* настройка процедуры резервного копирования в соответствии с настоящим Регламентом;
* изготовление резервных копий информации;
* контроль и анализ содержания системного журнала резервного копирования не реже 1 раза в неделю;
* проведение процедур тестирования целостности резервных копий;
* проведение процедур тестирования восстановления из резервных копий;
* анализ объемов данных резервного копирования;
* контроль состояния оборудования системы резервного копирования;
* замена неработоспособных или выработавших свой ресурс носителей резервной информации или оборудования системы резервного копирования;
* восстановление программ и данных из резервных копий в случае порчи или утери данных.

Все процедуры по установке и извлечению носителей из системы резервного копирования осуществляются администратором резервного копирования в присутствии ответственного за резервное копирование.

По мере выработки ресурса носителей резервной информации они подлежат замене на новые. Вся информация с носителей, которые перестают использоваться в системе резервного копирования, стирается.

Учет носителей резервной информации, проведенных процедур (в том числе тестирование резервный копий, стирание информации с носителей резервной информации, выработавших ресурс, и их уничтожение на основании актов) осуществляется в Журнале контроля резервного копирования, который ведется ответственным за резервное копирование.

### **Восстановление информации из резервных копий**

Любое восстановление информации, не связанное с потерей работоспособности Системы или ее компонентов, выполняется администратором резервного копирования на основании заявки Государственного заказчика.

Процедура восстановления данных следующая:

* Государственный заказчик определяет резервную копию, на основании которой необходимо восстановить данные Системы.
* Исполнитель восстанавливает данные из указанной резервной копии.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями Системы, но в течение не более 36 часов с момента поступления заявки.

В случае выхода из строя каких-либо компонентов Системы необходимо произвести восстановление повреждённых файлов или данных. В случае если удаётся быстро идентифицировать файлы, требующие восстановления – произвести восстановление только этих файлов.

Для восстановления используется последняя из имеющихся резервных копий. В случае невозможности произвести восстановление из последней имеющейся копии, используется предпоследняя резервная копия и далее в порядке устаревания резервной копии. По решению Государственного заказчика для восстановления может использоваться любая из имеющихся резервных копий.

# Перечень сокращений

Раздел определяет примененные в инструкции термины и сокращения с приведением их краткого описания (Расшифровка). Применяемые в Техническом задании термины и сокращения приведены в таблице 6.1

Таблица 6.1 Термины и сокращения

| Сокращение | Расшифровка |
| --- | --- |
| Комплекс | Программный комплекс удаленного мониторинга и контроля за работой медицинского оборудования с предиктивным механизмом выявления наступления неисправностей |
| Протокол  | Набор команд и структура данных, передаваемых между участниками Комплекса |
| REST | (от англ. Representational State Transfer) - «передача репрезентативного состояния» или «передача „самоописываемого“ состояния» |
| API | (англ. Application Programming Interface[1]) - описание способов взаимодействия одной компьютерной программы с другими |
| JSON | (англ. JavaScript Object Notation) - текстовый формат обмена данными, основанный на JavaScript |
| Балансировщик | Программно-аппаратное средство для маршрутизации и организации потока запросов к обслуживающим эти запросы системам |
| Сервер | Отказоустойчивая ЭФМ увеличенной мощности, расположенная в защищенных помещениях |
| Виртуальный сервер | Логически выделенная мощностная (ресурсная) часть Сервера, предназначенная для выполнения определенных задач |
| НСД | Несанкционированный доступ к функциям или данным |
| HTTP | HyperText Transfer Protocol – протокол передачи данных. |
| HTTPS | Hypertext Transfer Protocol Secure– расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTPS, «упаковываются» в криптографический протокол SSL или TLS, тем самым обеспечивается защита этих данных. |
| БД | База данных |
| ГОСТ | Государственный стандарт. |
| ЕСКД | Единая система конструкторской документации |
| ЕСПД | Единая система программной документации |
| ОС | Операционная система |
| Пользователь | Сотрудник КО, КНВШ или ЦО, эксплуатирующий портал для достижения целей по управлению олимпиадным движениеми научно-исследовательской деятельности |
| РД | Руководящий документ |
| РФ | Российская Федерация |
| СУБД | Система управления базой данных |
| ЭВМ | Электронно-вычислительная машина |

#