Регламент действия персонала во внештатных ситуациях при работе с автоматизированными информационными системами

1. Определение

Регламент действий персонала во внештатных ситуациях содержит описания действий обслуживающего персонала, направленных на обеспечение работоспособности автоматизированной информационной системы и предупреждение возникновения внештатных ситуаций.

При работе с автоматизированной информационной системой могут возникнуть следующие ситуации:

1) Перебои или отсутствие энергопитания
2) Выход из строя технических средств автоматизированной информационной системы
3) Выход из строя линий телекоммуникаций
4) Возгорание в серверном помещении
5) Затопление серверного помещения
6) Нарушение в температурном режиме
7) Сбой в работе покупного (системного) программного обеспечения
8) Обнаружение факта несанкционированного доступа к автоматизированной информационной системе
9) Отказ системы кондиционирования
10) Потеря данных и/или нарушение целостности данных
11) Сбой в работе программного обеспечения

2. Ресурсы

1)не требуются

3. Документирование

1) Все сведения о возникших внештатных ситуациях, работах, проведенных для их устранения и факт устранения внештатной ситуации должны фиксироваться в журнале эксплуатации автоматизированной информационной системы.

4. Процедуры:

1) Перебои или отсутствие энергопитания

В случае отключения энергопитания, периодических перебоях или скачках в энергопитании серверное оборудование должно переводиться на резервные источники питания.

В зависимости от мощности серверного оборудования могут быть применены 2 различных вида резервных источников питания:

№ п/п	Наименование	Характеристика
1	Источник бесперебойного питания (ИБП)	Обеспечивает энергопитанием серверное оборудование в течение 30 минут. В течение этого времени необходимо либо произвести штатную остановку автоматизированной информационной системы либо перевести ее на альтернативный источник питания.

2	Автономный генератор	Позволяет обеспечивать энергопитанием серверное оборудование при отсутствии штатного питания. Генератор приводится в действие от внешнего двигателя (обычно применяется дизельный двигатель). Генератор должен быть оснащен устройством, автоматически запускающим его при отсутствии энергопитания.

Серверное оборудование автоматизированной информационной системы должно быть оснащено источниками бесперебойного питания. Система резервного питания должна автоматически корректно завершать работу приложений и сервера при остатке заряда батарей не менее 40% или переводить питание сервера автоматизированной информационной системы на автономное. Времени до окончательного разряда батарей должно быть достаточно для выполнения действий по выключению серверного оборудования или ее переводу на автономное питание.

В случае отсутствия или неисправности устройства, обеспечивающего автоматический запуск генератора, запуск генератора производится вручную, дежурным системным администратором.

При обнаружении отсутствия энергопитания ответственное лицо должно известить о выявленных неполадках руководство медицинской организации, а также организацию, ответственную за предоставление энергопитания.

2) Выход из строя технических средств информационной системы

При обнаружении фактов выхода из строя каких либо технических средств автоматизированной информационной системы необходимо известить об этом дежурного инженера по техническому обслуживанию. Дежурный инженер должен определить степень критичности ситуации и, при необходимости, произвести замену оборудования.

3) Выход из строя линий телекоммуникаций

В состав узла автоматизированной информационной системы входят линии коммуникации 2х типов: внутренние и внешние.

Внутренние линии обеспечивают связь между оборудованием, образующим узел автоматизированной информационной системы (сервера, рабочие станции и т.п.). Внутренние линии коммуникаций с соответствующим сетевым оборудованием и ПК образуют локальную сеть передачи данных (ЛВС).

Внешние линии обеспечивают связь с вышестоящим узлом и, при наличии, с нижестоящими узлами и используются для осуществления репликации данных между узлами Системы и/или связи с внешними системами.

В случае обнаружения выхода из строя внутренних линий коммуникаций и сетевого оборудования инженер по техническому обслуживанию узла должен выполнить ремонтные работы по приведению вышедшей из строя части ЛВС в работоспособное состояние или работы по замене вышедшей из строя линии и оборудования.

В случае обнаружения выхода из строя внешних линий телекоммуникаций системный администратор должен проверить факт автоматического переключения телекоммуникационного оборудования на использование резервных линий телекоммуникаций (или выполнить это переключение вручную) и известить руководство медицинской организации и администраторов вышестоящего и нижестоящих узлов.

В случае если резервные внешние линии телекоммуникаций отсутствуют, то дополнительно к вышеизложенному системным администратором узла должны быть выполнены работы по переводу узла автоматизированной информационной системы на работу с репликацией в режиме off-line.

После восстановления работоспособности внешних линий телекоммуникаций системным администратором узла должны быть проведены работы по переводу репликации в режим on-line.

4) Возгорание в серверном помещении

При обнаружении факта возгорания в серверном помещении необходимо привести в действие систему пожаротушения (в случае, если она не сработала автоматически), сообщить о пожаре в противопожарную службу по телефону 101, обесточить серверное помещение, уведомить о факте возгорания системного администратора узла и руководство организации здравоохранения, принять все разумные и доступные в сложившихся обстоятельствах меры для уменьшения ущерба и тушения пожара, обеспечить эвакуацию людей.

При выполнении дальнейших действий необходимо руководствоваться утвержденными в организации здравоохранения инструкциями по действиям при пожаре.

5) Затопление серверного помещения

При обнаружении факта затопления серверного помещения необходимо обесточить серверное помещение, уведомить о факте затопления системного администратора узла, руководство организации здравоохранения и соответствующие ремонтные службы, принять все разумные и доступные в сложившихся обстоятельствах меры для уменьшения ущерба.

6) Нарушение в температурном режиме

К оборудованию, критичному к соблюдению температурного режима можно отнести следующее оборудование: жесткие диски, процессоры, материнские платы и т.п.

При обнаружении факта нарушения температурного режима для устройств и/или оборудования (достижение или превышение максимально разрешенной температуры) необходимо принять меры к выходу из данной внештатной ситуации путем включения дополнительных охлаждающих устройств или штатной остановкой информационной системы.

После устранения нарушений в температурном режиме функционирования устройств и/или оборудования необходимо провести проверку оборудования на работоспособность и на сохранность данных.

Так же обслуживающему персоналу узла непосредственно после устранения нарушений необходимо провести ряд работ, направленный на выявление и устранение причин возникновения данной внештатной ситуации.

7) Сбой в работе покупного (системного) программного обеспечения

К системному программному обеспечению относится следующее программное обеспечение: операционная система (ОС), система управления базами данных (СУБД), антивирусное программное обеспечение.

Аппаратное обеспечение узла функционирует под управлением системного программного обеспечения. Сбой в работе системного ПО в конечном итоге может привести к сбою в работе аппаратного обеспечения, потери данных и/или нарушению их целостности.

При обнаружении сбоя в работе системного ПО администратору узла необходимо выполнить сервисные процедуры, рекомендованные производителем системного ПО для устранения выявленной неполадки.

После выполнения работ по устранению сбоя в работе системного ПО необходимо проверить работоспособность узла информационной системы и сохранность данных.

8) Обнаружение факта несанкционированного доступа к информационной системе

Несанкционированный доступ к информации – это доступ к информации, нарушающий правила разграничения доступа и с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Основным методом обнаружения факта несанкционированного доступа к информационной системе является ежедневный контроль и просмотр администратором системных журналов.

При обнаружении факта НСД к узлу Системы администратор узла должен выполнить следующие действия:

1) Произвести отключение всех подключенных пользователей узла информационной системы, в случае наличия связи в режиме on-line с вышестоящим и нижестоящими узлами так же произвести отключение подключенных узлов;

2) Известить руководство организации здравоохранения, системного администратора узла, системных администраторов вышестоящего и нижестоящих узлов;

3) Провести работы по аудиту состояния системных файлов операционной системы на предмет несанкционированных в них изменений и восстановлению корректных версий измененных файлов. В случае обнаружения большого количества изменений и/или невозможности восстановления файлов вручную необходимо полностью удалить системное программное обеспечение с последующим восстановлением из дистрибутива;

4) Произвести смену паролей для всех учетных записей узла (как непосредственно пользовательских, так и администраторских);

5) После приведения системного программного обеспечения в корректное состояние необходимо выполнить проверку информации, хранимой на узле информационной системы. В случае обнаружения факта изменений в составе информации, она должна быть восстановлена из дистрибутива.

9) Отказ системы кондиционирования

Отказ системы кондиционирования и охлаждения воздуха в серверном помещении может привести к внештатным ситуациям, связанным с нарушениями температурного режима эксплуатации оборудования.

В случае обнаружения факта отказа системы кондиционирования необходимо принять меры, по устранению возникшей внештатной ситуации, известить системного администратора узла и соответствующие ремонтные службы.

Должна быть задействована резервная система кондиционирования и охлаждения. В случае если резервная система отсутствует, системный администратор узла должен оценить критичность возникшей ситуации и принять решение необходимости остановки информационной системы. В случае принятие положительного решения, информационная система должна быть остановлена в штатном режиме, в случае, если принято решения не останавливать информационную систему, то необходимо усилить контроль над температурным режимом и в случае роста температуры оборудования информационная система должна быть остановлена.

10) Потеря данных узла информационной системы и/или нарушение целостности данных

Данные узла информационной системы могут быть потеряны или нарушена их целостность или достоверность в результате различных внештатных ситуаций, таких как: сбой оборудования и/или программного обеспечения, нарушение температурного режима, в результате несанкционированного доступа и т.п.

В случае обнаружения факта потери данных (нарушения целостности) на узле информационной системы администратор должен произвести штатную остановку информационной системы, известить о факте потери данных (нарушении целостности) руководство организации здравоохранения, администратора вышестоящего и нижестоящих узлов.

Должен быть проведен анализ потерянных данных и определена стратегия восстановления данных. Данные могут быть восстановлены из резервных копий или путем запроса данных у вышестоящего узла.

После проведения процедуры восстановления данных должны быть выполнены работы по их проверке на полноту и корректность. После того, как выполнена проверка, узел может быть запущен в работу.

11) Сбой в работе программного обеспечения

При произошедшем сбое в работе программного обеспечения администратор информационной системы должен выявить причины сбоя в работе программного обеспечения и устранить возможность потери данных в информационной системе. После обнаружения причины, администратор должен устранить причину сбоя и

выполнить установку, переустановку системного, сетевого или прикладного программного обеспечения.

При сбое в работе программного обеспечения и обнаружении потери данных в предыдущем разделе описаны действия по устранению возникших неполадок.

В случае обнаружения факта потери данных после восстановления работы программного обеспечения, администратор должен провести мероприятия по устранению потери данных согласно предыдущему пункту.

Администратор должен снизить вероятность сбоев в работе программного обеспечения путем проведения профилактических работ.

Форма журнала неисправностей

Таблица 1 – Образец журнала неисправностей

Дата	Ф.И.О. вызвавшего	Описание проблемы (причина вызова)	Проведенные работы по устранению	Подпись устранившего	Примечания