Наименование структурного подразделения:	**Все структурные подразделения**		
Названия документа:	**СОП «Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях информационных систем»**		
Утвержден:		Руководитель на ПХВ «ЛГП» Чалкаров А.Б.	
Дата утверждения:			
Разработчик:	*Должность*	*Ф.И.О.*	*Подпись*
	Заместитель гл.врача по контролю качества мед.услуг	Рысбаев С.Т.	
	Программист	Сопов А. Сухинин А.	
Согласовано:	Заместитель гл.врача по лечебному делу	Анаркулова У.О.	
	Заместитель гл.врача по ОМД	Кабылбеков Г.К.	
	Врач эксперт		
Дата согласования:	04.01.2024г.		
Дата введения в действие	04.01.2024г.		
Версия №	**Копия №_____**	04 /01 / 2024г. Ф.И.О. _____ Подпись _____	

Дата последнего пересмотра «09» «01» 2024г
Дата следующего пересмотра «_____» «_____» 2027г

Запрещается несанкционированное ксерокопирование документа

1. Область применения

1.1 Настоящая Инструкция действий пользователей во внештатных (кризисных) ситуациях информационных систем (далее - Инструкция) предназначена для организации порядка действий пользователей во внештатных (кризисных) ситуациях в информационных системах ГКП на ПХВ "Ленгерская Городская Поликлиника"(далее - ИС).

1.2 Требования настоящей Инструкции обязательны к применению администраторами ИС в Ленгерская Городской Поликлиники.

2. Нормативные ссылки

В настоящей Инструкции использованы ссылки на следующие нормативные документы:

1. СТ РК 34.005-2002 Информационная технология. Основные термины и определения;
2. СТ РК 34.006-2002 Информационная технология. Базы данных. Основные термины и определения;
3. СТ РК 34.007-2002 Информационная технология. Телекоммуникационные сети. Основные термины и определения;
4. СТ РК ИСО/МЭК 17799-2006 Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации.

3. Определения, обозначения и сокращения

3.1 В настоящей Инструкции приведены следующие определения, обозначения и сокращения:

Администраторы ИС - Сотрудники, осуществляющие системно-техническое обслуживание программно-аппаратных средств и сопровождение ИС;
ИБ - Информационная безопасность;
ИС, Система - Информационные системы;
ОС - Операционная система;
ПО - Программное обеспечение;
ЭКС - Ответственный специалист по эксплуатации систем.

4. Общие положения

Настоящая Инструкция содержит описания о порядке действий пользователей во внештатных (кризисных) ситуациях ИС, направленных на поддержание технического оборудования, прикладного ПО и ПО ИС в рабочем состоянии, а также обеспечения ИБ ИС при администрировании и сопровождении ИС в соответствии с Политикой информационной безопасности.

Запрещается несанкционированное ксерокопирование документа

5. Требования

5.1 Кризисные ситуации.

1. Ситуация, возникающая в результате нежелательного воздействия на ИС, не предотвращенного средствами защиты, называется кризисной.
2. Кризисная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, аварий, стихийных бедствий и т.п.).
3. По степени серьезности и размерам наносимого ущерба кризисные ситуации разделяются на следующие категории:

1) Угрожающая - приводящая к полному выходу ИС из строя и ее неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;
2) Серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но тем не менее требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы) к критическим не относятся.

К угрожающим кризисным ситуациям, например, могут быть отнесены:

- нарушение подачи электроэнергии в здание;
- выход из строя сервера (с потерей информации);
- выход из строя сервера (без потери информации);
- частичная потеря информации на сервере без потери его работоспособности;
- выход из строя локальной сети (физической среды передачи данных).

К серьезным кризисным ситуациям, например, могут быть отнесены:

- выход из строя рабочей станции (с потерей информации);
- выход из строя рабочей станции (без потери информации);
- частичная потеря информации на рабочей станции без потери ее работоспособности;

К ситуациям, требующим внимания, например, могут быть отнесены:

- несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Источники информации о возникновении кризисной ситуации:

Запрещается несанкционированное ксерокопирование документа

- Пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- Средства защиты, обнаружившие кризисную ситуацию;
- Системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

5.2 Меры обеспечения непрерывной работы и восстановления работоспособности ИС.

Непрерывность процесса функционирования ИС и своевременность восстановления ее работоспособности достигается:

1. Проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывной работы и восстановления (далее - НРВ) вычислительного процесса;
2. Назначением и подготовкой должностных лиц, отвечающих за организацию и осуществление практических мероприятий по обеспечению НРВ информации и вычислительного процесса;
3. Четким знанием и строгим соблюдением всеми должностными лицами использующими средства вычислительной техники ИС, требований руководящих документов по обеспечению НРВ;
4. Применением различных способов резервирования аппаратных ресурсов эталонного копирования программных и страхового копирования информационных ресурсов системы;
5. Эффективным контролем за соблюдением требований по обеспечению НРВ должностными лицами и ответственными;
6. Постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты.

5,3 Общие требования.

1. Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.
2. Серьезная и угрожающая кризисная ситуация может потребовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий
3. Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в

Запрещается несанкционированное ксерокопирование документа

серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

4. Резервному копированию подлежат программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное ПО, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.
5. Программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии. Необходимые действия персонала по созданию, хранению и использованию резервных копии программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.
6. Каждый носитель, содержащий резервную копию, должен иметь метку, содержащую данные о классе, ценности, назначении хранимой информации, ответственном за создание, хранение и использование, дату последнего копирования, место хранения и др.
7. Дублирующие аппаратные ресурсы предназначены для обеспечения работоспособности системы в случае выхода из строя всех или отдельных аппаратных компонентов в результате угрожающей кризисной ситуации.
8. Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает, возможно, более полное восстановление про1раммных аппаратных, информационных и других поврежденных компонентов системы.
9. В случае возникновения любой кризисной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба определение виновных и принятие соответствующих мер.

5.4. Управление инцидентами ИБ.

1. Под инцидентом ИБ (далее - инцидент) понимается любое незаконное, неразрешенное (в том числе Политикой информационной безопасности ИС) или неприемлемое действие, которое совершается в ИС.
2. В целях обеспечения гарантированного уведомления ответственных лиц за информационную безопасность и всех заинтересованных сторон об инциденте и слабости ИБ по отношению к ИС, должны быть реализованы формальные процедуры по уведомлению об инциденте и появлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры.
3. Администраторы ИС, должны знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов Системы, о наступлении которых или предпосылках к таковому необходимо отправить уведомление.

Запрещается несанкционированное ксерокопирование документа

4. Администраторы ИС обязаны можно быстрее сообщать о любых событиях в сфере ИБ непосредственно ответственному специалисту по информационно безопасности.

5.5 Сбор доказательств.

Все доказательства, собираемые в процессе расследования инциндентов в ИС, Независимо от того , будут ли они использованы при дисциплинарных мерах, или в процессе судебного разбирательства, должны быть собраны и сохранены в соответствие с общими правилами , обеспечивающими:

1. Допустимость доказательства : действительно ли доказательство может быть использовано в суде;
2. Весомость доказательства: качество и полнота доказательства.

Любая работа в интересах судебного разбирательства должна выполняться только с копиями материялов доказательств.

Копирование материалов доказательств должно контролироваться заслуживающим доверие персоналом, должен быть создан отчет со следующий информацией: где и когда был выполнен процесс копирования, кто выполнил операции копирования , какие инструментальные ссредства и программы использовались, данные о носителе (поставщик/ изготовитель , тип, заводской норем носителя)

5.6 Действия при возникновенния ситуации, не подподающих под перечисленный список.

В случак возникновения важных, критических или внештатных ситуации с ИС, не попадающих под выше перечисленный список необходимо:

1. Поставить в известность непосредственное руководство, ответсвенные лица за серверное оборудование, информационную безопасность и эксплуатацию систем о возникшей ситуации ИС;
2. При необходимости принять участие в устранении последствий внештатной ситуаций.
3. Самостоятельно или при участии администратора ОС, и ответсвенного сотрудника за телекоммуникацию устранить причину недоступности ИС;
4. Дежурный специалист по эксплуатации систем делает отметку в журнале регистации внештатных ситуаций.

5.7. Контроль возникновения внештатных или кризисных ситуации и крректирующих действий по ним.

Контроль возникновения внештатных ситуаций осуществляется с помощью следующих функций:

1. Составлением актов, в случае необходимости, с описанием внештатной ситуации и корректирующих действий, приложения поясняющие материалы (копии экрана, распечатка журнала событий и другое);

Запрещается несанкционированное ксерокопирование документа

2. Средствами оперативного мониторинга. Мониторинг ИС должен производится ежедневно с помощью специализированного программного обеспечения, в случае изменения состояния доступности ИС должно произойти оповещение администратора ОС в режиме «онлайн».

В случаях получения информации о возможных предстоящих внештатных ситуациях должно быть обеспечено оперативное оповещение всех причастных лиц и структур.

Дежурный специалист по эксплуатации системы должен произвести соответствующую запись возникновения внештатных ситуаций в журнале «Внештатных (кризисных) ситуаций» (приложение 1).

Администраторы ИС обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственному специалисту за информационную безопасность.

6. Ответственность

Все лица, отвечающие за работоспособность ИС несут ответственность:

1. За надлежащее выполнение своих функциональных обязанностей;
2. За сохранность, доступность, конфиденциальность обрабатываемой информации, в рамках своей компетенции.

В кратчайшие сроки предпринимают меры по восстановлению работоспособности. Предпринимаемые меры согласуются с ответственным специалистом за информационную безопасность.

В случае нарушения требований настоящего Инструкции, руководство и обслуживающий персонал привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

Выполнение требований настоящих правил контролируется руководителями, ответственных за эксплуатацию систем и структурных подразделений курирующих ИС.

Администраторы ИС несут ответственность за соблюдение требований Инструкции и утвержденных в ее рамках НД по ИБ.

Специалист за ИС несет ответственность за разработку, актуализацию и соблюдению требований изложенных в настоящей Инструкции.

Запрещается несанкционированное ксерокопирование документа

Лист ознакомления

№	Фамилия И.О.	Должность	Дата	Подпись
	Сухинин А.А.	программист	04.01.2024	
	Сонов А.В.	программист	04.01.2024	

Запрещается несанкционированное ксерокопирование документа

Приложение 1(рекомендуемое)

Журнал внештатных (кризисных) ситуаций.

Выяснение причины сбоя (при обнаружении индиндента)							Уточнение информации (после устранения инцинданта)						
№	Проект СТП	Дата	время	Источник сообщения № запроса	Оповещенные сотрудники ФИО	Описание инцидента	Территория локализации инцидента	Оповеститель (ФИО)	Причина сбоя	**Дата исправления**	**Время испавления**	Меры устранения инцинта	Время простоя

1. Указание условии пересмотра СОП: Пересмотр СОП проводиться 1 раз в 3 года или при появлении новых требовании.

2. Нормативные ссылки:

1. Приказ и.о. Министра здравоохранения Республики Казахстан от 30 октября 2020 года «Об утверждении форм учетной документации в области здравоохранения, а также инструкций по их заполнению» № КР ДСМ-175/2020;
2. Приказ и.о. Министра здравоохранения Республики Казахстан от 5 ноября 2021 года «Об утверждении стандартов аккредитации медицинских организаций» № КР ДСМ – 111;
3. Приказ Министра здравоохранения Республики Казахстан от 24 августа 2021 года № «Об утверждении «Правил оказания первичной медико-санитарной помощи» КР ДСМ-90;

Лист регистрации изменений

№	№ раздела, пункта стандарта, в которое внесено изменение	Дата внесения изменения	ФИО лица, внесшего изменения

Запрещается несанкционированное ксерокопирование документа