**Утверждено Приказом**
**Главного врача**
**КГКП «Жамбылский областной центр**
**по профилактике и борьбе со СПИД»**
**УЗ акимата Жамбылской области**
**_____Кыдырбаева Б.Д.**
**№_____от «____»_____2025 г.**

# СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

# ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА «ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

г. Тараз
2025 г.

**Содержание** стр.

# 1 Общие положения

1.1. Настоящяя политика об информационной безопасночти (далее – «Политика») Коммунального государственного казенного предприятия "Жамбылский областной центр по профилактике и борьбе с синдромом приобретенного иммунодефицита управления здравоохранения акимата Жамбылской области" (далее - Жамбылский ОЦ СПИД) разработано в соответствии с действующими законодательством Республики Казахстан и НПА.

1.2. Настоящая Политика информационной безопасности (далее-Политика) определяет комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов.

1.3. Настоящая Политика учитывает современное состояние и ближайшие перспективы развития системы информационной безопасности, цели, задачи, эксплуатации, режимы функционирования, а также анализ угроз безопасности для объектов информатизации.

# 2 Область применения

Настоящая Политика применяется сотрудниками и входит в комплект документации системы менеджмента качества (СМК).

# 3 Термины, определения и сокращения

## 3.1 Термины

| | |
|---|---|
| Информационная безопасность | Процесс обеспечения защиты информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от неавторизованного доступа, использования. |
| Информационная система | Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса; |
| Несанкционированный доступ | Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к ней; |

## 3.2Сокращения и обозначения

| | |
|---|---|
| АРМ | Автоматизированное рабочее место |
| ВС | Вычислительная система |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| ЛИС | Лабораторная информационная система LIS K-Lab |
| МЗ РК | Министерство Здравоохранения Республики Казахстан |
| ОИКН | Отдел информатики и компьютерного надзора за ВИЧ инфекцией |
| ЗОИКН | Заведующий отделом информатики и компьютерного надзора за ВИЧ инфекцией |
| ПК | Персональный компьютер |
| ПО | Программное обеспечение |
| Система электронного слежения за случаями ВИЧ инфекции | Электронное слежение за случаями ВИЧ-инфекции |
| ОТ | Оргтехника |

## 4 Ссылки на документы

| | |
|---|---|
| СТ РК ISO 15189-2015 | «Лаборатории медицинские. Требования к качеству и компетентности» |
| Кодекс Республики Казахстан от 18 сентября 2009 года № 193-IV | Кодекс Республики Казахстан «О здоровье народа и системе здравоохранения» |
| Закон Республики Казахстан от 24 ноября 2015 года № 418-V | «Об информатизации» |
| Закон Республики Казахстан от 21 мая 2013 года № 94-V | «О персональных данных и их защите» |
| Постановление Правительства | «Единые требования в области информационно-коммуникационных технологий и обеспечения |

| | |
|---|---|
| Республики Казахстан от 20 декабря 2016 года № 832 | информационной безопасности |

## 5 Ответственность

5.1 Ответственность за утверждение данной Политики несет главный врач.

5.2 Ответственность за внедрение и управление процессами, указанными в данной Политике несет заведующий отделом информатики и компьютерного надзора за ВИЧ инфекцией (далее - РОИКН).

5.3 Ответственность за разработку данной Политики несет ЗОИКН.

5.4 Все сотрудники руководствуются требованиями настоящей Политики.

## 6 Цель и задачи Политики информационной безопасности

6.1 Главной целью, на достижение которой направлены все положения настоящей Политики, является надежное обеспечение информационной безопасности, и как следствие недопущение нанесения материального, физического или иного ущерба в результате информационной деятельности.

6.2 Для достижения поставленных целей обеспечивается исполнение следующих задач:

– защита от вмешательства посторонних лиц в процессе функционирования ВС;

– разграничение доступа зарегистрированных пользователей к информации, а также к аппаратным, программно-аппаратным и программным средствам;

– контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

– защита системы от внедрения вредоносных кодов, включая компьютерные вирусы;

– защита служебной информации и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;

– обеспечение аутентификации пользователей, участвующих в информационном обмене;

– своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

– создание механизма оперативного реагирования на угрозы

информационной безопасности и негативные тенденции;

– создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

6.3 В комплект нормативных документов в области информационной безопасности включены следующие документы:

| **Название детальной политики** | **Периодичность действия** | **Ответственные** | | |
|---|---|---|---|---|
| | | **Все** | **ОИКН** | **Материальный бухгалтер** |
| Журнал заявок пользователей | По заявкам | + | + | |
| Журнал регистрации внештатных ситуаций | По мере обнаружения внештатных ситуаций | | + | |
| Регламент по проведению системно-технического обслуживания программно-аппаратных средств, информационных систем | По мере необходимости | | + | |

## 7 Инструкция по защите информации

В целях обеспечения защиты информационной безопасности, в том числе коммуникационных средств от несанкционированного доступа предусматривается следующие меры по информационной безопасности:

1) использование для производственных целей прикладного программного обеспечения, не входящего в состав базового комплекса;

2) обеспечение прохождения инструктажа и дополнительного обучения с сотрудниками МО по нормам законодательства Республики Казахстан в области информационной безопасности, в том числе с вновь поступившими на работу;

3) закрепление в договорах обязательства поставщиков товаров, работ и услуг о неразглашении предоставленных им сведений;

4) создание надежной системы охраны зданий и сооружений (видеонаблюдение) закрепленный за инженером по технике по безопасности;

Защита ЭВМ пользователей от несанкционированного доступа в МО, которая предусматривает следующие направления:

1) создание средств регистрации пользователей.

2) использование лицензионного антивирусного программного обеспечения, регулярное обновление антивирусных программ. Антивирусные программы применяются, где это возможно, для проверки рабочих станций,

серверов центра, переносных носителей информации на наличие вредоносного кода.

3) тестирование перед вводом в эксплуатацию программных продуктов и аппаратных средств с целью проверки их работоспособности. Не пригодное к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются.

4) принятие мер, связанных с внедрением средств защиты, которые используются в случае стихийных бедствий (пожаров, наводнений и землетрясений), а также в различных внештатных ситуациях. Контроль за внештатными ситуациями производится путем внесения о них записей в журнал.

## 8 Правила о парольной защите

8.1 Настоящие Правила о парольной защите в МО регламентирует организационно-техническое обеспечение процессов использования, смены и прекращения действия личных паролей пользователей персональных компьютеров и администраторов информационных систем, удаления учетных записей.

**Правила формирования личного пароля**

8.2 Личные пароли выбираются пользователями и администраторами информационных систем самостоятельно с учетом следующих требований:

– пароль не включает в себя легко вычисляемые сочетания символов (имена и даты рождения, номера автомобилей, телефонов другие сведения), которые можно угадать, основываясь на информации о пользователе, а также стандартное расположение букв на клавиатуре (zyxwvuts, 123, 123321, qwerty); рекомендуется использовать пароли случайного набора символов; пароли, которые уже использовались ранее, не выбираются повторно в течение шести месяцев с момента их изменения;

– личный пароль не подлежит разглашению. За разглашение пароля, который относится к служебной тайне, работник привлекается к дисциплинарной ответственности.

**Ввод пароля**

8.3 Ввод пароля осуществляется с учетом регистра и с учетом раскладки клавиатуры.

8.4 Во время ввода паролей, исключается возможность распознания его посторонними лицами или компрометации пароля посредством технических средств. Пароли в автоматизированный процесс регистрации не включаются.

**Хранение пароля**

8.5 Пользователи при хранении пароля придерживаются следующих

требований:

– личный пароль, а также пароли для доступа к другим информационным ресурсам, в том числе к интернет-ресурсу не подлежит разглашению;

– не допускается использование логинов и паролей, используемых в корпоративной сети, интернет-ресурсе, общедоступных международных интернет-ресурсах, почтовых и других информационных системах.

8.6 Прекращение доступа к ВС уволенных пользователей производится ОИКН. Кадровая служба информирует ОИКН об увольнении сотрудника не позднее чем за 3 рабочих дня до увольнения.

## 9 Инструкция по организации антивирусной защиты

9.1 Антивирусные программы устанавливаются специалистами ОИКН на все персональные компьютеры и сервера корпоративной вычислительной сети.

9.2 Настройка антивирусных средств должна обеспечивать:

- автоматический запуск антивирусного монитора при каждой перезагрузке компьютера (для серверов – при перезапуске);
- в определенное время дня полную антивирусную проверку (сканирование) локальных дисков, установленных на компьютере;
- обновление антивирусных баз в определенное время дня;
- лечение зараженных вирусов файлов или удаление при невозможности лечения;
- оповещение пользователя о подозрительных и зараженных объектах;
- проверку всех файлов на электронных или оптических носителях информации, и файлов, полученных из сетей, на наличие вредоносного кода перед работой с этими файлами;
- проверку любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования, эта проверка может быть выполнена в разных точках, например, на серверах электронной почты, персональных компьютерах или при входе в сеть организации;

**Порядок проведения антивирусного контроля**

9.3 Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только специалистами ОИКН.

9.4 Устанавливаемое (изменяемое) на компьютер программное обеспечение должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

9.5 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съемных носителей (магнитные диски, ленты, CD-ROM, и т.п.), получаемых от сторонних лиц и организаций.

9.6 Контроль информации на съемных носителях производится непосредственно перед ее использованием.

9.7 Особое внимание следует обратить на съемные носители (дискеты, флешки, компакт-диски), принадлежащие лицам, временно допущенным к работе на персональном компьютере (студенты-практиканты, временно замещающие и т.п.). Работа этих лиц должна проводиться под непосредственным контролем, особенно если работа происходит с использованием ресурсов локальной вычислительной сети.

## 10 Правила использования сети интернет и электронной почты

10.1 Все сообщения, материалы, созданные, переданные или полученные с помощью системы электронной почты и Интернет, а также другими информационными ресурсами являются и остаются собственностью и не могут быть личной собственностью ни одного из сотрудников.

10.2 Руководство оставляет за собой право на мониторинг (просмотр, удаление) любых сообщений и информации, созданных, полученных или переданных сотрудникам, а также уполномочить конкретных сотрудников на проведение данных действий.

10.3 В случае обнаружения фактов или выявления потенциальной угрозы информационной безопасности ЗОИКН немедленно информирует руководство.

10.4 При использовании электронной почты и служб Интернет запрещается:

– использовать ресурсы для агитации или рекламы коммерческих предприятий, пропаганды религиозных или политических идей, иных целей, не связанных с выполнением служебных обязанностей;

– создавать оскорбительные или провокационные сообщения. Таковыми считаются сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, а также другую информацию, запрещенную законодательством Республики Казахстан;

– использовать вложения графических, видео, исполняемых и т.п. файлов, не относящихся к служебной деятельности, а также файлов, размер которых превышает 15 МБ;

– запрашивать и отправлять сообщения, содержащие сведения, составляющие государственные секреты и иную служебную и/или конфиденциальную информацию без шифрования;

– пользоваться групповой рассылкой в личных целях;

– использовать ресурсы для рассылки писем-пирамид, писем «счастья», сообщений рекламного характера и другой подобной информации, не имеющей отношения к служебной деятельности;

– распространять вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

– использовать учетные записи других почтовых систем и пользователей;

– получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством);

– осуществлять вложение файлов при использовании служб Интернет-сообщений;

– распространять в сети Интернет оскорбительные и провокационные заявления;

– посещать веб-сайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности;

– посещать сомнительные и вредоносные сайты, а также сайты, информация на которых не связана с исполнением функциональных обязанностей;

– загружать (передавать) вредоносные файлы и программы, программное обеспечение и материалы, защищенные авторским правом, а также мультимедийные файлы всех типов;

– использовать службы Интернет-чатов;

– осуществлять подключение компьютеров к сети Интернет через сторонних Интернет-провайдеров (за исключением случаев, письменно разрешенных руководством МО), а также использовать несанкционированное модемное подключение.

## 11 Регламент действий персонала во внештатных ситуациях

11.1 Настоящий Регламент о порядке действий пользователей во внештатных (кризисных) ситуациях в МО, определяет основные меры, и средства сохранения (поддержания) работоспособности информационной системы при возникновении различных кризисных ситуаций, а также способы и

средства восстановления информации и процессов ее обработки в случае нарушения работоспособности информационной системы и ее основных компонентов. Кроме того, настоящий Регламент описывает действия различных пользователей персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

11.2 Ситуация, возникающая в результате нежелательного воздействия на информационную систему, приведшая к угрозе информационной безопасности, называется внештатной (кризисной). Внештатная (кризисная) ситуация возникает в результате преднамеренных или непреднамеренных действий пользователей, или аварий, стихийных бедствий, при проблемах с электрическим питанием.

11.3 По размерам наносимого ущерба внештатные (кризисные) ситуации подразделяются на следующие категории:

1) угрожающая - внештатная (кризисная) ситуация, приводящая к полному выходу из строя информационной системы и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, наиболее важной информации.

К угрожающим внештатным (кризисным) ситуациям относятся:

– нарушение подачи электроэнергии в здании;
– 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).

2) серьезная - внештатная (кризисная) ситуация, 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.

К серьезным внештатным (кризисным) ситуациям относятся:

– 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;
– стихийные бедствия (пожар, наводнение, ураган).

Источники информации о возникновении внештатной (кризисной) ситуации:

– пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;

– средства защиты, обнаружившие кризисную ситуацию.

11.4 Все пользователи, работа которых нарушается в результате возникновения угрожающей или серьезной внештатной (кризисной) ситуации, немедленно оповещаются посредством средств телекоммуникаций (телефоны, эл. почта и т.п.). Дальнейшие действия по устранению причин нарушения работоспособности информационной системы, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями РОИКН.

11.5 Каждая серьезная внештатная (кризисная) ситуация анализируется РОИКН. По результатам этого анализа вырабатываются предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и другие меры по информационной безопасности, при необходимости проводится расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

11.6 Серьезные и угрожающие внештатные (кризисные) ситуации требуют оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

11.7 Оперативное восстановление данных в случае их уничтожения или порчи в серьезной или угрожающей внештатной (кризисной) ситуации обеспечивается резервным копированием и хранением копий.

11.8 Резервному копированию подлежат данные и программы, необходимые для полного восстановления работоспособности серверов в случае сбоя оборудования или программного обеспечения.

11.9 Все программные средства, используемые в системе, имеют установочные копии.

**Действия пользователей во внештатных (кризисных) ситуациях**

11.10 Пользователь, в случае обнаружения внештатной (кризисной) ситуации:

– Уведомляет РОИКН, который извещает о случае внештатной ситуации руководство.

11.11 При обнаружении признаков пожара (дым, угарный газ, пламя) сообщает об инциденте главному врачу МО и сотрудникам пожарной службы; пытается обесточить серверное, телекоммуникационное оборудование, источники бесперебойного питания особенно в месте возникновения пожара; пытается погасить пожар ручным огнетушителем, при открытой двери серверного помещения.

11.12 При затоплении: выключает рубильник (автомат) электрического

питания; сообщает об инциденте главному врачу МО.

## 12 Правила резервного копирования, хранения резервных файлов и восстановления данных в случае чрезвычайных ситуаций.

12.1 Настоящая инструкция о резервном копировании информации определяет требования к организации мероприятий по резервному копированию программных и информационных ресурсов корпоративной вычислительной сети МО.

12.2 Ответственным за организацию резервного копирования данных серверного оборудования в МО является РОИКН.

**Копирование программных и информационных ресурсов, контроль за проведением резервного копирования и восстановления**

12.3 В целях обеспечения возможности оперативного восстановления информации и процессов ее обработки в случае нарушения работоспособности информационных систем, используется резервное копирование информационных ресурсов.

12.4 Резервному копированию подлежит база данных сервера управления МО, содержащая информацию о персональных данных пациента, о результатах лабораторных исследований.

12.5 Резервное копирование данных не должно нарушать работу серверов и пользователей компьютерной сети.

12.6 Периодически ЗОИКН проверяет результаты резервного копирования.

12.7 Восстановление информации с резервной копии на сервер управления МО производится сотрудниками ОИКН.

12.8 Хранению подлежат текущая и не менее двух предыдущих копий.

12.9 Хранятся на выделенных дисковых массивах сервера и компьютера РОИКН.

Доступ к носителям информации с резервными копиями информационных ресурсов имеет ЗОИКН и представитель компании, обслуживающей информационную систему ЛИС в соответствии с функциональными обязанностями и договорными обязательствами.

## 13 Правила технического обслуживания компьютерного оборудования

1. Отключить компьютер от электрической и локальной сетей.
2. Открыть корпус системного блока компьютера.
3. Провести внешний осмотр корпуса системного блока, установленных устройств. При осмотре необходимо обращать внимание на состояние корпуса, отсутствие механических повреждений, потемнения покрытий, вздутия или

обугливания частей устройств и элементов, что свидетельствует о воздействии на них слишком высокой температуры, вызванной, например, неисправностью устройства.

4. Проверить качество соединений:

– разъемов блока питания с дисководами, жестким диском и материнской платой;

– шин данных с дисководами, жестким диском и материнской платой;

– плат компьютера с материнской платой.

5. Выполняется удаление пыли и других посторонних частиц природного и промышленного происхождения из оборудования, с поверхности отдельных устройств, проводов, кабелей, расположенных в корпусе ПК. Удаление пыли производится при помощи продувки или с помощью салфеток для оргтехники.

6. При вскрытом корпусе системного блока включить его в электрическую сеть.

7. Проверить работу вентиляторов, блока питания и процессора. При необходимости произвести их смазку.

8. Отключить системный блок от электрической сети.

9. Закрыть крышку корпуса системного блока.

10. Подключить компьютер к электрической и локальной сетям.

## 14 Инструкция пользователя по эксплуатации компьютерного оборудования и программного обеспечения

14.1 Всем пользователям МО необходимо знать требования безопасности и методы защиты оставленного без присмотра оборудования.

14.2 Носители с важной или критичной служебной информацией, например, на бумажном или электронном носителе, когда она не требуется, следует убирать и запирать, особенно когда помещение пустует.

14.3 Пользователь должен следить, что бы закрепленная за ним ОТ стояла на горизонтальной поверхности.

14.4 Пользователь должен следить, что бы отверстия ОТ предназначенные для вентилирования не были закрыты посторонними предметами.

14.5 Пользователь должен следить, что бы ОТ была подключена к сети электропитания через блоки бесперебойного питания или через сетевые фильтры.

14.6 Пользователь должен следить, чтобы провода, к которым подключена ОТ не подвергались перегибам, повреждениям или были передавлены и не располагались в местах, где они могут быть легко повреждены.

14.7 Пользователям запрещается использовать нестандартные, самодельные или неисправные провода.

14.8 В случае если пользователь обнаружил повреждение проводки или неисправность ОТ, он должен обратиться к инженеру программисту с требованием принять меры по их исправлению.

14.9 Пользователям запрещается вставлять металлические и другие предметы в отверстия, которые имеются в корпусе ОТ.

14.10 Пользователям запрещается ставить ОТ вплотную к батареям центрального отопления или нагревательным приборам.

14.11 Пользователям запрещается употреблять пищу в близи ОТ.

14.12 Пользователям запрещено самостоятельно устанавливать, удалять, модифицировать ПО или его конфигурацию.

14.13 Пользователям запрещается работать с правами администратора на ПК.

14.14 Пользователям запрещается перемещать оборудование, относящееся к локальной сети, перемещать ОТ из одного помещения в другое.

14.15 Пользователям запрещается осуществлять попытки несанкционированного проникновения на ПК других пользователей, оборудования вычислительной сети и в служебные помещения, а также осуществлять доступ к внешним информационным ресурсам.

14.16 Пользователям запрещается использовать ПО и ОТ организации в неслужебных целях.

14.17 Пользователям запрещается использовать электронную почту и Интернет в неслужебных целях.

14.18 Пользователям запрещается использовать чужой идентификатор и пароль при работе в сети МО и Интернет.

14.19 Пользователям запрещается предоставлять свой идентификатор и пароль для работы в сети МО и Интернет другому лицу.

14.20 Пользователям запрещается предоставлять в общий сетевой доступ, диски, файлы на ПК.

14.21 Пользователям запрещается осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц.

14.22 Пользователям запрещается оставлять включенным без присмотра свой ПК, не активировав блокировку экрана.

14.23 Пользователям запрещается осуществлять с помощью модема или другого коммуникационного оборудования самостоятельное подключение к информационным ресурсам.

14.24 Пользователям запрещается умышленно использовать в программном обеспечении или в настройках средств защиты недокументированные свойства и ошибки, которые могут привести к возникновению внештатной (кризисной) ситуации (об обнаружении такого рода ошибок необходимо ставить в известность руководителя своего подразделения).

14.25 Пользователям запрещается использовать некачественную бумагу при печати и копировании ОТ.

14.26 Пользователям запрещается хранить личные файлы в системных папках или корневом каталоге.

14.27 Пользователям запрещается допускать к технике посторонних лиц, самостоятельно вскрывать ОТ и сетевые устройства.

14.28 Пользователь должен проверить съемный носитель перед использованием.

14.29 Пользователь должен следить за количеством свободного места на жестком диске. В случае если свободного пространства менее чем 500 МБ, пользователь должен обратиться инженеру программисту для принятия требуемых мер.

14.30. Пользователь не должен использовать электронную почту, мессенджеры не Казахстанского сегмента.

## 15 Техника безопасности при работе с персональным компьютером (ПК)

15.1 Любой компьютер является электроприбором и представляет собой потенциальную угрозу. Поэтому при работе с компьютером необходимо соблюдать требования безопасности.

15.2 Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера и его работоспособности. Недопустимо использование некачественных и изношенных компонентов в системе электроснабжения, а также их суррогатных заменителей: розеток, удлинителей, переходников, тройников. Недопустимо самостоятельно модифицировать розетки для подключения вилок, соответствующих иным стандартам. Электрические контакты розеток не должны испытывать механических нагрузок, связанных с подключением массивных компонентов (адаптеров, тройников и т. п.). Все питающие кабели и провода должны располагаться с задней стороны компьютера и периферийных устройств.

15.3 Запрещается производить какие-либо операции, связанные с подключением, отключением или перемещением компонентов компьютерной системы без предварительного отключения питания. Компьютер не следует

устанавливать вблизи электронагревательных приборов и систем отопления. Недопустимо размещать на системном блоке, мониторе и периферийных устройствах посторонние предметы: книги, листы бумаги, салфетки, чехлы для защиты от пыли. Это приводит к постоянному или временному перекрытию вентиляционных отверстий. Запрещается внедрять посторонние предметы в эксплуатационные или вентиляционные отверстия компонентов компьютерной системы.

15.4 Некоторые составные части компьютеров способны сохранять высокое напряжение в течение длительного времени после отключения от сети. Поэтому не следует разбирать или ремонтировать их самостоятельно. В случае поломок необходимо обращаться к ОИКН.

**Особенности электропитания системного блока**

15.5 Все компоненты системного блока получают электроэнергию от блока питания. Блок питания ПК — это автономный узел, находящийся в верхней части системного блока.

**Система гигиенических требований**

15.6 Длительная работа с компьютером может приводить к расстройствам состояния здоровья. Кратковременная работа с компьютером, установленным с грубыми нарушениям гигиенических норм и правил, приводит к повышенному утомлению.

15.7 Вредное воздействие компьютерной системы на организм человека является комплексным. Параметры монитора оказывают влияние на органы зрения. Оборудование рабочего места влияет на органы опорно-двигательной системы.

**Требования к видеосистеме**

15.8 На рабочем месте монитор должен устанавливаться таким образом, чтобы исключить возможность отражения от его экрана в сторону пользователя источников общего освещения помещения.

Расстояние от экрана монитора до глаз пользователя должно составлять от 50 до 70 см. Не надо стремиться отодвинуть монитор как можно дальше от глаз, опасаясь вредных излучений (по бытовому опыту общения с телевизором), потому что для глаза важен также угол обзора наиболее характерных объектов.

15.9 Оптимально, размещение монитора на расстоянии 1,5 D от глаз пользователя, где D — размер экрана монитора, измеренный по диагонали.

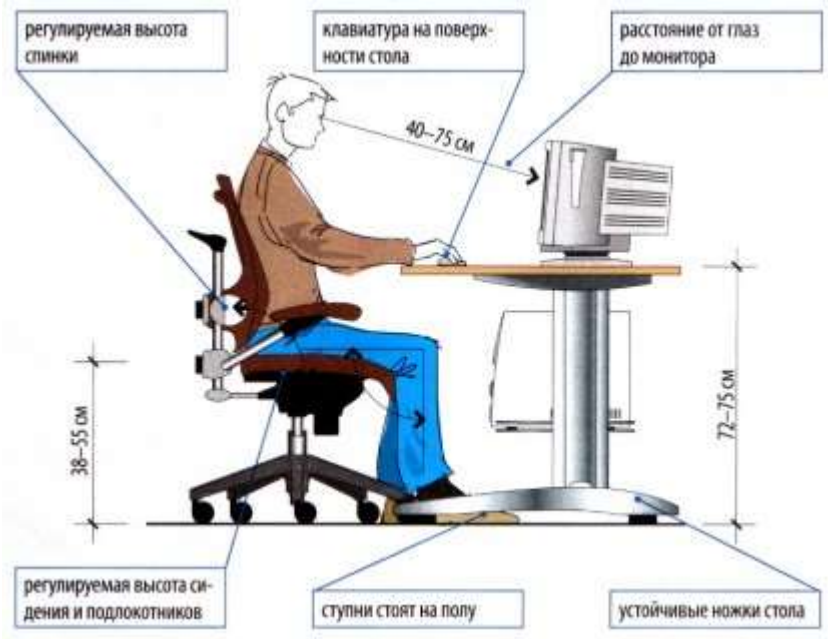
**Требования к рабочему месту.**

15.10 В требования к рабочему месту входят требования к рабочему столу, посадочному месту (стулу, креслу). Необходимо обеспечить правильное

размещение элементов компьютерной системы и правильную посадку пользователя чрезвычайно трудно.

15.11 Монитор должен быть установлен прямо перед пользователем и не требовать поворота головы или корпуса тела.

15.12 Рабочий стол и посадочное место должны иметь такую высоту, чтобы уровень глаз пользователя находился чуть выше центра монитора. На экран монитора следует смотреть сверху вниз, а не наоборот. Даже кратковременная работа с монитором, установленным слишком высоко, приводит к утомлению шейных отделов позвоночника.




15.13 Клавиатура должна быть расположена на такой высоте, чтобы пальцы рук располагались на ней свободно, без напряжения, а угол между плечом и предплечьем составлял 100° — 110°. Для работы рекомендуется использовать специальные компьютерные столы, имеющие выдвижные полочки для клавиатуры. При длительной работе с клавиатурой возможно утомление сухожилий кистевого сустава.

15.14 При работе с мышью рука не должна находиться на весу. Локоть руки или хотя бы запястье должны иметь твердую опору. Если предусмотреть необходимое расположение рабочего стола и кресла затруднительно, рекомендуется применить коврик для мыши, имеющий специальный опорный валик.

## 16 Приложения

### Қолданушыларға арналған журнал
### Журнал заявок пользователей

| № | Күні Дата | Тапсырыстың мәні Суть заявки | Себебі Причина | Қызметкерлердің аты-жөні /лауазымы/ Ф.И.О. сотрудника /должность | Қабылданған шаралар Принятые меры | Қолы Подпись |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

### Штаттан тыс оқиғалар тіркелетін журнал
### Журнал регистрации внештатных ситуаций

| №п/п | Қызметкерлердің аты-жөні /лауазымы/ ФИО сотрудника /должность | Күні мен уақыты Дата и время | Штаттан тыс оқиға Внештатная ситуация | Шақырған қызметкедің қолы Роспись сотрудника вызвавшего | Қабылданған шаралар Принятые меры | Қызметкердің қолы Роспись специалиста | Ескертулер Примечание |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## Регламент по проведению системно-технического обслуживания программно-аппаратных средств, информационных систем

В период с «___»_____20___г. . по «__»_____20___г. в _____ оказаны профилактические работы по обеспечению системно-технического обслуживания программно-аппаратных средств, информационных систем и выполнены следующие мероприятия:

1. Плановое техническое обслуживание вычислительной техники производится 4 раза в год - ежеквартально.
2. В плановое техническое обслуживание вычислительной техники входят следующие виды работ :

– Настройка операционных систем;
– Настройка учетных записей и параметров доступа к серверу на уровне операционной системы;
– Проверка на наличие вирусов и лечение;
– Чистка системной области от файлов пользователей;
– Проверка надежности кабельных соединений, разъемов, отсутствия нежелательных скруток;
– Проверка/тестирование производительности машины и периферийных устройств, а также всей системы в целом;
– Удаление загрязнения с корпусов и съемных крышек.

## Лист регистрации изменений

| ДАТА | ПРИЧИНА ИЗМЕНЕНИЙ |
|---|---|
| | Истечение срока 3 лет |

## Лист ознакомления

| Должность | ФИО | Дата | Подпись |
|---|---|---|---|
| Главный врач | Кыдырбаев Б.Д. | | |
| Заместитель главного врача | Калметова Г.А. | | |
| Заместитель главного врача | Әбдібай Е.М. | | |
| Главный бухгалтер | Сулейменова С.М. | | |
| Главная медицинская сестра | Сатмаханова Л.О. | | |
| Отдел кадров | Койшыбаев Е.Н. | | |
| Зав.эпид.отделом | Ахметова Г.Т. | | |
| Зав.леч.отделением | Ниязалиева Ф.А. | | |
| ИО Зав.лаборатории ИФА | Малимов А.Ә. | | |
| Зав.отделом информатики и компьютерного надзора за ВИЧ-инфекцией | Кемелбекова Ф.К. | | |
| Зав.филиала лаб.ИФА г.Шу | Салыкбаева А.Ш. | | |