«УТВЕРЖДАЮ»
Директор
Университетского госпиталя
НАО «МУС»
Азизов Б.С.
«____» _____ 2026 год

ПОЛИТИКА
обеспечения кибербезопасности и защиты информации в Университетском госпитале НАО «Медицинский университет Семей

РАЗРАБОТАНО: Дмитриевым М.Л., начальником технического отдела, и службой медицинской техники

СОГЛАСОВАНО:

№	Должность	Ф.И.О.	Дата/подпись
1.	Заместителя директора по медицинской части	Журавлев Е.Г.	«__»_____20___ г.
2.	Заместитель директора по детству	Каримов Д.С.	«__»_____20___ г.
3.	И.о. заместителя директора по финансово-экономической службе и общим вопросам	Фоминых Т.Н.	«__»_____20___ г.
4.	Заместитель директора по административно-хозяйственной работе	Беленко И.Ю.	«__»_____20___ г.
5.	И.о. председателя профсоюзного комитета	Нурланова Р.Р.	«__»_____20___ г.
6.	Руководитель отдела HR-менеджмента	Жумабаева А.А.	«__»_____20___ г.
7.	Руководитель отдела правового и документационного обеспечения	Джартыбаев Т.Р.	«__»_____20___ г.

г. Семей, 2026 год

1. Общие положения

1.1. Настоящая Политика обеспечения кибербезопасности и защиты информации в (далее — Политика) устанавливает единые требования к обеспечению кибербезопасности, защите информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры, персональных данных и персональных медицинских данных.

1.2. Политика является обязательной для исполнения всеми работниками Университетского госпиталя НАО «Медицинский университет Семей» (далее – Госпиталь), независимо от занимаемой должности, формы занятости и места выполнения работы.

1.3. Требования Политики распространяются также на:

- заведующие отделением;
- врачи;
- средний медицинский персонал;
- младший медицинский персонал;
- административно управленческий персонал;
- работники административно хозяйственной части;
- временных работников;
- практикантов и стажеров;
- подрядчиков и сервисные организации;
- поставщиков информационных систем;
-специалистов, осуществляющих удаленное техническое обслуживание;
- иных лиц, получивших доступ к информационным ресурсам Госпиталя.

1.4. Целью Политики является обеспечение:

- конфиденциальности информации;
- целостности информации;
- доступности информационных ресурсов;
- защиты персональных данных;
- защиты персональных медицинских данных.

1.5. Политика является основой для разработки отдельных инструкций, регламентов и процедур по информационной безопасности.

2. Нормативная база

2.1. При разработке и применении настоящей Политики учитываются требования законодательства Республики Казахстан, в том числе: Закон Республики Казахстан «О кибербезопасности»; Закон Республики Казахстан «О персональных данных и их защите»; законодательство Республики Казахстан в сфере здравоохранения; законодательство Республики Казахстан

в сфере цифровизации и информационной безопасности; Правила осуществления сбора, обработки, хранения, защиты и предоставления персональных медицинских данных субъектами цифрового здравоохранения; Правила разграничения прав доступа субъектов цифрового здравоохранения; минимальные требования к медицинским цифровым системам в области здравоохранения; Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности; иные нормативные правовые акты Республики Казахстан, применимые к деятельности организации.

2.2. При противоречии настоящей Политики требованиям законодательства Республики Казахстан применяются требования законодательства, после чего Политика подлежит актуализации.

3. Основные понятия

3.1. В настоящей Политике используются следующие понятия:

Информационная безопасность (ИБ) — состояние защищенности информации, информационных систем и инфраструктуры от внутренних и внешних угроз.

Кибербезопасность — совокупность правовых, организационных и технических мер, направленных на защиту цифровых ресурсов и инфраструктуры от киберугроз.

Инцидент информационной безопасности — событие или совокупность событий, которые могут привести к нарушению конфиденциальности, целостности или доступности информации.

Персональные данные — сведения, относящиеся к определенному или определяемому физическому лицу.

Персональные медицинские данные — персональные данные, связанные с состоянием здоровья, диагностикой, лечением и оказанием медицинской помощи.

Учетная запись — уникальная совокупность идентификатора и средств аутентификации пользователя.

Привилегированная учетная запись — учетная запись с расширенными административными полномочиями.

Медицинская информационная система (МИС) — информационная система, обеспечивающая ведение медицинских процессов в электронном формате.

Критическая информационная система — система, нарушение работы которой может привести к существенному нарушению медицинской деятельности, безопасности пациентов или доступности медицинской помощи.

4. Принципы обеспечения кибербезопасности

4.1. В Госпитале применяются следующие основные принципы:

4.1.1. **Минимально необходимый доступ** - работнику предоставляется только тот объем доступа, который необходим ему для выполнения должностных обязанностей.

4.1.2. **Разделение полномочий** - административные права, права пользователя и права контроля по возможности разделяются между различными учетными записями и должностными лицами.

4.1.3. **Персональная ответственность** - каждый пользователь несет персональную ответственность за действия, совершенные с использованием его учетной записи.

4.1.4. **Запрет общих учетных записей** - использование одной учетной записи несколькими работниками запрещается, за исключением специально предусмотренных технологических учетных записей.

4.1.5. **Защита медицинской тайны** - доступ к медицинской информации предоставляется исключительно лицам, которым такой доступ необходим для исполнения служебных обязанностей.

4.1.6. **Непрерывность медицинской деятельности** - меры кибербезопасности не должны необоснованно препятствовать оказанию медицинской помощи.

5. Ответственность руководства

5.1. Руководитель организации:

5.1.1. утверждает настоящую Политику;

5.1.2. назначает ответственных лиц;

5.1.3. обеспечивает финансирование мероприятий по кибербезопасности;

5.1.4. обеспечивает внедрение организационных и технических мер защиты;

5.1.5. обеспечивает расследование серьезных инцидентов;

5.1.6. определяет порядок взаимодействия с государственными органами и внешними организациями.

6. Ответственный за информационную безопасность

6.1. В организации назначается лицо, ответственное за обеспечение информационной безопасности.

6.2. Ответственный за ИБ:

- организует выполнение требований настоящей Политики;
- контролирует состояние средств защиты;
- участвует в расследовании инцидентов;
- организует учет информационных ресурсов;
- контролирует предоставление и прекращение доступа;
- контролирует выполнение резервного копирования;
- организует обучение работников;

- участвует в оценке рисков.

6.3. В зависимости от структуры организации указанные функции могут выполняться отдельным специалистом, IT-службой либо специализированной организацией на основании договора.

7. Классификация информационных ресурсов

7.1. Информационные ресурсы организации классифицируются по уровню критичности.

Уровень 1 — критические

К ним относятся:

- МИС;
- электронная медицинская карта;
- серверы медицинских данных;
- PACS/RIS;
- серверы хранения медицинских изображений;
- сетевое оборудование, обеспечивающее работу критических медицинских систем.

Уровень 2 — важные

- бухгалтерские системы;
- кадровые системы;
- системы документооборота;
- электронная почта;
- файловые серверы;
- системы видеонаблюдения;
- системы контроля доступа.

Уровень 3 — вспомогательные

- офисные компьютеры;
- принтеры;
- сканеры;
- информационные панели;
- гостевые сети;
- вспомогательные сервисы.

8. Защита персональных и медицинских данных

8.1. Госпиталь обеспечивает защиту персональных медицинских данных посредством организационных и технических мер.

8.2. Обрабатываемые персональные данные должны соответствовать принципу необходимости и достаточности для выполнения задач организации.

8.3. Не допускается использование медицинских данных:

- в личных целях;

- для просмотра информации о знакомых, родственниках или сотрудниках без служебной необходимости;
- для передачи третьим лицам без законного основания;
- для публикации в социальных сетях;
- для передачи через несанкционированные мессенджеры;
- для копирования на личные устройства.

8.4. Медицинские данные не должны передаваться через:
- личные электронные почтовые ящики;
- личные облачные хранилища;
- личные флеш-накопители;
- несанкционированные мессенджеры;
- незащищенные каналы связи.

8.5. Действия пользователей с медицинскими информационными системами должны регистрироваться средствами журналирования в соответствии с установленными требованиями.

9. Управление учетными записями

9.1. Каждый работник получает персональную учетную запись.

9.2. Учетная запись должна быть заблокирована:
- при увольнении;
- при переводе на должность, не требующую соответствующего доступа;
- при длительном отсутствии;
- при выявлении компрометации учетных данных.

9.3. При увольнении работника доступ к информационным системам прекращается не позднее момента прекращения его трудовых полномочий.

9.4. Административные учетные записи должны использоваться только для административных операций.

10. Требования к паролям

10.1. Пароль пользователя должен:
- иметь длину не менее 8 символов;
- содержать буквы верхнего и нижнего регистра;
- содержать цифры;
- при возможности содержать специальные символы;
- не содержать имя пользователя;
- не содержать дату рождения.

10.2. Запрещается:
- передавать пароль другому лицу;
- записывать пароль на видном месте;
- использовать один пароль для нескольких систем;

- хранить пароли в открытом виде.

10.3. Для критических систем рекомендуется применение многофакторной аутентификации.

11. Разграничение доступа

11.1. Доступ предоставляется на основании:

- должностных обязанностей;
- утвержденной заявки;
- согласования руководителя подразделения;
- соответствующего решения ответственного за информационную безопасность.

11.2. Рекомендуется использовать ролевую модель доступа:

Роль – Доступ;

Врач – Медицинские данные пациентов своего профиля;

Медицинская сестра – Данные, необходимые для выполнения медицинских процедур;

Регистратура – Регистрационные данные пациентов;

Лаборатория – Данные, необходимые для лабораторной диагностики;

Администратор МИС – Администрирование МИС;

Бухгалтерия – Финансовые данные;

Руководство – Данные согласно полномочиям;

Внешний сервисный специалист – Только временный согласованный доступ.

11.3. Права доступа пересматриваются не реже одного раза в 6 месяцев.

12. Защита рабочих станций

12.1. На рабочих станциях должны использоваться:

- антивирусное/EDR-средство;
- актуальная операционная система;
- актуальные обновления безопасности;
- автоматическая блокировка экрана;
- средства защиты от вредоносного ПО.

12.2. Пользователю запрещается самостоятельно:

- отключать антивирус;
- отключать защитные механизмы ОС;
- устанавливать нелицензионное ПО;
- устанавливать программы из неизвестных источников;
- изменять настройки безопасности;
- подключать неизвестные USB-устройства.

13. USB-накопители и внешние устройства

13.1. Использование USB-накопителей допускается только при наличии служебной необходимости.

13.2. Перед использованием внешнего накопителя он должен быть проверен средствами защиты.

13.3. Для критических информационных систем рекомендуется техническое ограничение использования USB-накопителей.

13.4. Запрещается копировать персональные медицинские данные на личные флеш-накопители.

14. Электронная почта

14.1. Электронная почта организации используется исключительно для служебных целей.

14.2. Работникам запрещается:

- открывать подозрительные вложения;
- переходить по неизвестным ссылкам;
- передавать пароли электронной почтой;
- отправлять медицинские данные на личную почту;
- использовать рабочую почту для регистрации на сомнительных ресурсах.

14.3. При получении подозрительного письма работник обязан сообщить в IT-службу или ответственному за ИБ.

15. Интернет и веб-ресурсы

15.1. Доступ к Интернету предоставляется в соответствии с должностными обязанностями.

15.2. На уровне сетевой инфраструктуры рекомендуется использовать:

- DNS-фильтрацию;
- web-фильтрацию;
- блокирование вредоносных доменов;
- блокирование командных центров вредоносного ПО;
- фильтрацию подозрительных загрузок.

15.3. Запрещается использование рабочих компьютеров для:

- посещения вредоносных ресурсов;
- загрузки нелицензионного ПО;
- использования пиратских ресурсов;
- запуска неизвестных файлов.

16. Сетевая безопасность

16.1. Локальная сеть медицинской организации должна быть сегментирована.

16.2. Минимально рекомендуется выделить отдельные сетевые сегменты для:

- серверов;
- рабочих станций;

- медицинского оборудования;
- видеонаблюдения;
- IP-телефонии;
- Wi-Fi сотрудников;
- гостевого Wi-Fi;
- систем контроля доступа.

16.3. Гостевой Wi-Fi не должен иметь доступа к внутренним медицинским информационным системам.

16.4. Медицинское оборудование не должно иметь прямого доступа в Интернет, если такой доступ не требуется производителем и не обоснован технологически.

16.5. Межсетевое взаимодействие между сегментами осуществляется по принципу «запрещено всё, что явно не, разрешено».

17. Серверная инфраструктура

17.1. Серверное оборудование размещается в специально оборудованном помещении.

17.2. Доступ в серверную предоставляется только уполномоченным лицам.

17.3. Серверная должна быть защищена от:

- несанкционированного доступа;
- перегрева;
- затопления;
- скачков напряжения;
- пожара;
- физического повреждения.

17.4. Для критических серверов рекомендуется:

- ИБП;
- резервирование электропитания;
- RAID;
- резервное копирование;
- мониторинг состояния;
- резервирование сетевых соединений.

18. Медицинское оборудование

18.1. Медицинское оборудование, подключенное к сети организации, рассматривается как потенциальный источник киберриска.

18.2. К таким системам относятся:

- рентгеновские аппараты;
- КТ;
- МРТ;

- УЗИ;
- лабораторные анализаторы;
- аппараты ИВЛ с сетевыми интерфейсами;
- мониторы пациентов;
- PACS/RIS;
- серверы медицинских изображений;
- диагностические станции.

18.3. Для медицинского оборудования запрещается без согласования:

- устанавливать стороннее ПО;
- изменять сетевые настройки;
- подключать оборудование к внешней сети;
- устанавливать удаленный доступ;
- отключать защитные средства.

18.4. Удаленный доступ поставщика осуществляется только:

- по заявке;
- на ограниченный период;
- с разрешения ответственного лица;
- с использованием защищенного канала;
- с регистрацией действий специалиста.

19. Удаленный доступ

19.1. Удаленный доступ к внутренним системам разрешается только через утвержденные средства.

19.2. Рекомендуется использовать:

- VPN;
- многофакторную аутентификацию;
- индивидуальные учетные записи;
- журналирование сеансов;
- ограничение времени доступа.

19.3. Запрещается предоставлять поставщику постоянный удаленный доступ к медицинской сети без отдельного обоснования и разрешения.

20. Резервное копирование

20.1. Организация обязана обеспечивать регулярное резервное копирование критически важных данных.

20.2. Резервному копированию подлежат:

- базы данных программного обеспечения на серверах;
- конфигурации серверов;
- конфигурации сетевого оборудования;
- критические документы;
- настройки специализированных систем.

20.3. Рекомендуется применять правило:

- не менее 3 копий данных;
- на 2 различных типах носителей;
- 1 копия — отдельно от основной инфраструктуры.

20.4. Для защиты от ransomware рекомендуется иметь резервную копию, недоступную для изменения из основной сети.

20.5. Не реже одного раза в квартал проводится проверка восстановления данных.

21. Обновление программного обеспечения

21.1. Технический отдел обеспечивает контроль обновлений (при необходимости):

- операционных систем;
- серверного ПО;
- сетевого оборудования;
- антивирусных средств;
- МИС;
- PACS/RIS;
- другого критического ПО.

21.2. Перед обновлением критической системы проводится оценка совместимости.

21.3. Для критических систем должна существовать возможность восстановления предыдущей рабочей конфигурации.

22. Управление уязвимостями

22.1. Организация осуществляет регулярный поиск уязвимостей.

22.2. При выявлении критической уязвимости принимаются меры по:

- устранению уязвимости;
- установке обновления;
- временной изоляции системы;
- ограничению сетевого доступа;
- дополнительному мониторингу.

22.3. Критические уязвимости должны обрабатываться в приоритетном порядке.

23. Мониторинг и журналирование

23.1. В организации осуществляется регистрация событий информационной безопасности.

23.2. По возможности журналируются:

- входы пользователей;
- неудачные попытки входа;
- изменение прав;

- создание учетных записей;
- удаление учетных записей;
- административные действия;
- доступ к медицинским данным;
- изменение медицинских записей;
- удаление данных;
- сетевые события;
- события антивирусной защиты;
- события межсетевого экрана.

23.3. Журналы должны защищаться от несанкционированного изменения и удаления.

24. Выявление и реагирование на инциденты

24.1. Инцидентами считаются, в частности:

- заражение вирусом;
- утечка персональных данных;
- несанкционированный доступ;
- изменение медицинских данных без разрешения;
- удаление данных;
- отказ МИС;
- DDoS-атака;
- потеря ноутбука или носителя с данными.

24.2. При обнаружении инцидента пользователь обязан немедленно сообщить:

- IT-службе;
- Ответственному за ИБ

24.3. Пользователь не должен самостоятельно удалять подозрительные файлы, переустанавливать ОС или изменять настройки системы, если это может уничтожить следы инцидента.

25. Алгоритм действий при обнаружении шифрования файлов:

- немедленно прекратить работу на зараженном компьютере;
- отключить компьютер от локальной сети;
- не удалять зашифрованные файлы;
- не подключать резервные носители;
- не пытаться самостоятельно расшифровать данные;
- сообщить в технический отдел;
- сообщить ответственному за ИБ;

26. Фишинг

26.1. Работники должны рассматривать как подозрительные сообщения:

- требующие срочной оплаты;
- требующие ввода пароля;
- содержащие подозрительные ссылки;
- содержащие неизвестные вложения;
- имитирующие сообщения банков;
- имитирующие сообщения руководителя;
- содержащие необычные требования.

26.2. При сомнении работник обязан обратиться в технический отдел.

27. Использование мобильных устройств

27.2. Медицинские данные не должны храниться на личных смартфонах работников без законного основания и утвержденного механизма защиты.

28. Облачные сервисы

28.1. Использование облачных сервисов для хранения медицинских и персональных данных допускается только после проверки их соответствия требованиям законодательства и внутренним требованиям организации.

28.2. Запрещается размещать медицинские документы в личных аккаунтах:

- Google Drive;
- OneDrive;
- Dropbox;
- iCloud;
- иных облачных сервисах, если использование соответствующего сервиса официально не разрешено организацией.

29. Использование искусственного интеллекта

29.1. Работникам запрещается загружать в публичные системы искусственного интеллекта:

- Ф.И.О. пациентов;
- ИИН;
- медицинские карты;
- результаты анализов;
- изображения пациентов;
- результаты КТ/МРТ;
- медицинские документы;
- персональные данные работников;
- иную информацию ограниченного доступа.

29.2. Использование ИИ с медицинскими данными допускается только при наличии официально утвержденного решения, соответствующего

требованиям законодательства и внутренним требованиям информационной безопасности.

30. Обучение работников

30.1. Все работники до получения доступа к информационным системам проходят инструктаж по информационной безопасности.

30.2. Повторное обучение проводится не реже одного раза в год.

31. Контроль подрядчиков

31.1. Подрядчики, получающие доступ к информационным системам, должны соблюдать требования настоящей Политики.

31.2. В договорах с подрядчиками рекомендуется предусматривать:

- конфиденциальность;
- защиту персональных данных;
- ответственность за нарушение ИБ;
- порядок удаленного доступа;
- журналирование действий;
- порядок возврата/уничтожения данных;
- запрет передачи доступа третьим лицам.

32. Контроль программного обеспечения

32.1. Установка ПО производится только уполномоченными сотрудниками.

32.2. Запрещается установка:

- пиратского ПО;
- программ без установленного источника;
- взломанных версий;
- неизвестных драйверов;
- ПО удаленного доступа без разрешения.

33. Физическая безопасность

33.1. Серверы, сетевое оборудование и устройства хранения данных должны быть физически защищены.

33.2. Доступ в серверную осуществляется только уполномоченным персоналом.

33.3. Сетевые шкафы должны быть закрыты.

33.4. Резервные копии должны храниться таким образом, чтобы их повреждение одновременно с основной инфраструктурой было исключено или минимизировано.

34. Проверка эффективности мер защиты

34.1. Не реже одного раза в год проводится внутренний аудит информационной безопасности.

34.2. Проверяются:

- учетные записи;
- права доступа;
- резервное копирование;
- обновления;
- журналы событий;
- сетевые настройки;
- сегментация;
- удаленный доступ;
- выполнение требований настоящей Политики.

35. Порядок предоставления доступа внешним специалистам

35.1. Доступ внешнего специалиста предоставляется на основании заявки.

35.2. Заявка должна содержать:

- Ф.И.О. специалиста;
- организацию;
- цель доступа;
- перечень систем;
- срок доступа;
- ответственное лицо организации.

35.3. После завершения работ доступ должен быть отключен.

35.4. Для критических систем действия внешнего специалиста подлежат обязательному журналированию.

36. Запреты для работников

Работникам запрещается:

1. передавать свои учетные данные другим лицам;
2. использовать чужие учетные записи;
3. просматривать медицинские данные без служебной необходимости;
4. фотографировать медицинские документы на личный телефон;
5. копировать медицинские данные на личные носители;
6. подключать неизвестные USB-устройства;
7. самостоятельно отключать защитное ПО;
8. устанавливать неразрешенное ПО;
9. предоставлять удаленный доступ третьим лицам;

10. использовать личную электронную почту для медицинских данных;

11. размещать медицинскую информацию в социальных сетях;

12. передавать пароли через мессенджеры;

13. подключать личные роутеры и точки доступа к внутренней сети;

14. самостоятельно изменять сетевые настройки критических систем.

37. Ответственность работников

37.1. Работники несут ответственность за нарушение настоящей Политики в соответствии с законодательством Республики Казахстан и внутренними документами организации.

37.2. Нарушения могут повлечь:

- дисциплинарную ответственность;
- ограничение доступа;
- проведение служебного расследования;
- возмещение ущерба в случаях и порядке, предусмотренных законодательством;
- иные меры ответственности.

38. Пересмотр Политики

38.1. Политика пересматривается:

- не реже одного раза в год;
- при изменении законодательства;
- при существенном изменении IT-инфраструктуры;
- после серьезного инцидента информационной безопасности;
- при внедрении новой МИС;
- при подключении новых медицинских систем.

39. Заключительные положения

39.1. Настоящая Политика вступает в силу после утверждения руководителем организации.

39.2. Все работники, имеющие доступ к информационным системам, должны быть ознакомлены с Политикой под подпись либо посредством утвержденной электронной системы ознакомления.

39.3. Политика является базовым документом системы управления информационной безопасностью организации.

Лист ознакомления

№	Ф. И. О.	Должность	Дата	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				