Утверждаю
И.о главного врача
КГП «Костанайский областной
Центр фтизиопульмонологии»
_____Ж.Ж. Молдатаевой
_____2023 год

Политика информационной безопасности

КГП «Костанайский областной центр фтизиопульмонологии»

На 11 листах

РАЗРАБОТАНО
И.о. начальника отдела
программного обеспечения
_____ Н. Уразов

«04» 01 2023 г.

г. Костанай, 2023 г.

Содержание

1. Назначение документа

1.1Документ предназначен для определения целей и требований обеспечения информационной безопасности для информационных систем, использующихся в КГП «Костанайский областной центр фтизиопульмонологии» УЗАКО .

1.2Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечение возможности получения доступа к данным авторизованным лицам в нужное для них время.

2. Глоссарий

Используемые сокращения:

КОЦФП	Костанайский областной центр фтизиопульмонологии
ИБ	Информационная безопасность
ИС	Информационные системы, используемые в КОЦФП
ЛВС	Локальная вычислительная сеть
ОС	Операционная система
ПО	Программное обеспечение
СПО	Системное программное обеспечение
ППО	Прикладное программное обеспечение
БД	База данных
СВТ	Средства вычислительной техники
ИБП	Источник бесперебойного питания

Используемые термины при составлении документа:

Информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз

Субъекты информатизации – государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации;

Услуги в сфере информатизации – услуги по созданию, развитию и сопровождению информационных систем, созданию электронных информационных ресурсов;

Информационная инфраструктура ИС – каналы связи, оборудование, программное обеспечение, обслуживающий персонал ИС, участники, документация, информация ИС;

Конфиденциальность информации - обеспечение предоставления информации только авторизированным лицам;

Целостность информации - состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право;

Доступность - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно;

3. Ссылки

3.1Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» (с изменениями и дополнениями по состоянию на 01.01.2023 г.);

3.2Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 КОНЦЕПЦИЯ кибербезопасности («Киберщит Казахстана»).

3.3Постановление Правительства Республики Казахстан от 31 декабря 2019 года № 1047.

3.4Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защиты информации – Введен впервые»;

3.5СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования» Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью.

3.6 Постановление Правительства Республики Казахстан от 31 октября 2018 года № 703 Об утверждении Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях.

4. Область распространения

4.1Политика информационной безопасности ИС распространяется на функционирование всей информационной инфраструктуры ИС;

4.2Политика информационной безопасности ИС обязательна для исполнения всеми лицами, работающими с информационной инфраструктурой ИС;

4.3Исполнение требований политики информационной безопасности ИС обеспечивают все лица, работающие с информационной инфраструктурой ИС.

5. Цели

5.1Целью обеспечения информационной безопасности является минимизация экономического, финансового, социального,

институционального и экологического ущербов от реализации угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИС.

6. Ответственность и обязательства руководства

6.1Руководство КОЦФП (далее - руководство), обеспечивающее управление, разработку, сопровождение и эксплуатацию ИС обеспечивает контроль выполнения всех пунктов данной политики.

6.2Ответственность и полномочия организаций описываются в соответствующих дополнительных регламентирующих документах.

6.3Руководство несет ответственность за выполнение всех пунктов данной политики.

6.4Руководство должно обеспечить четкое управление и зримую поддержку инициатив в области поддержки информационной безопасности ИС.

6.5Руководство должно обеспечивать координацию мер контроля за информационной безопасностью в ИС.

6.6Руководство должно предоставлять ресурсы для обеспечения информационной безопасности.

6.7Обслуживающий персонал при нарушении требований пунктов политики информационной безопасности ИС будет привлекаться к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

6.8Руководство должно утверждать разрабатываемые нормативные документы по информационной безопасности ИС.

6.9Новые программные обеспечения и аппаратные средства должны быть соответствующим образом одобрены со стороны руководства, авторизующих их цель и использование. Одобрение следует также получать от менеджера, ответственного за поддержание среды безопасности информационной системы.

6.10 Руководство обеспечивает контроль издания и доведения до сведения, утвержденных документов по ИС до обслуживающего персонала и участников ИС.

7. Конфиденциальность

Общие требования конфиденциальности

7.1Информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для организации.

7.2Главным требованием конфиденциальности является обеспечение предоставления информации только авторизированным лицам.

7.3Подключения участников к ИС должны фиксироваться в полном и тщательном виде.

7.4Служебная и иная защищаемая информация, обрабатываемая в ИС подлежит копированию и передаче третьему лицу только с официального разрешения руководства.

7.5Посредством ИС не должна осуществляться передача документов с вложением, содержащие государственные секреты и информацию с ограниченным доступом.

7.6При работе с ИС должна исключаться возможность наблюдения за отображаемой информацией на экране монитора пользователя ИС посторонними лицами.

7.7При работе с ИС должны использоваться специальные лицензионные программные или аппаратные средства обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.

8. Требования к осведомленности в вопросах информационной безопасности.

8.1Обслуживающий персонал ИС, должен быть ознакомлен с политикой информационной безопасности ИС.

8.2Обслуживающий персонал ИС должен принять соглашение о конфиденциальности ИС.

8.3Обслуживающий персонал обязан как можно быстрее сообщать о любых событиях в сфере информационной безопасности в соответствующее подразделение.

9. Требования по аутентификации пользователей в системе.

9.1Для аутентификации пользователей в ИС создаются уникальные идентификационные файлы (ID-файлы) / учетные записи (логин, пароль).

9.2Ответственность за сохранность ID-файла / неразглашение сведений об учетной записи возлагается на пользователей ИС.

10. Требования к учетным записям и паролям пользователей.

10.1 Для работы в ИС пользователям необходимо иметь *ID-файл / учетную запись*. В процессе регистрации устанавливается стандартный пароль. После получения *ID – файла / сведений об учетной записи* пользователю ИС необходимо изменить пароль.

10.2 Результатом выполнения процесса регистрации является формирование в составе БД ИС учетной записи пользователя ИС.

10.3 Учетная запись пользователя ИС представляет собой специальную уникальную запись в БД. Пользователь ИС взаимодействует с учетной записью посредством пароля, вводимого в соответствующий элемент интерфейса при входе в ИС.

10.4 В качестве пароля используется случайная последовательность символов. Пароль должен отвечать следующим требованиям:

10.5 Длина пароля должна быть не менее 8 символов;

10.6 В числе символов пароля обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (§, @, #, $, &, *, % и тому подобное);

10.7 Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименование автоматизированного рабочего места - АРМ и так далее), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

10.8 Использовать измененный пароль возможно только в период установленного времени (по умолчанию данный пароль действителен 30 дней). По истечении этого периода система должна потребовать от пользователя ИС изменить его. Данное требование в принудительном порядке реализуется посредством системного программного обеспечения;

10.9 Учетные записи пользователей ИС не имеют ограничения по срокам, если иное не оговорено особо.

10.10 В реестре заявок на регистрацию пользователей ИС, хранятся заявки, содержащие следующие реквизиты:

1) фамилия, имя, отчество пользователя;
2) организация;
3) наименованием структурного подразделения;
4) должность;
5) адрес, телефон, кабинет;
6) уровни доступа;
7) дата присвоения учетной записи пользователя из списка пользователей ИС;
8) дата удаления учетной записи пользователя из списка пользователей ИС;
9) отметка об увольнении и снятии с учета

10.11 Следует использовать средства информационной безопасности для ограничения доступа несанкционированных пользователей к действующим системам. Эти средства должны обеспечивать:

1) аутентификацию санкционированных пользователей в соответствии с определённой политикой контроля доступа;
2) регистрацию успешных и неудавшихся доступов к системе;
3) регистрацию использования специальных системных привилегий;
4) выдачу сигналов тревоги при нарушении политик безопасности системы;
5) предоставление подходящих средств аутентификации;

11. Контроль обеспечения конфиденциальности

11.1 С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

1) Ежегодная сверка списка официально зарегистрированных участников, работающих с ИС на основе журналов системы, с результатом в виде протокола.

2) Постоянный мониторинг инструментальными средствами информационной безопасности серверов ИС и сети, в которой они находятся.

12. Целостность

12.1 Требования к применению электронной почты и Интернета

1) Для уменьшения риска, которому подвергаются производственные процессы и система безопасности, связанного с использованием электронной почты, следует применять (по необходимости) соответствующие средства контроля. Необходимо учитывать:

a) уязвимость электронных сообщений по отношению к несанкционированному перехвату и модификации;
b) уязвимость данных, пересылаемых по электронной почте, по отношению к ошибкам, например, неправильная адресация или направление сообщений не по назначению, а также надежность и доступность сервиса в целом;
c) влияние изменения характеристик коммуникационной среды на производственные процессы, например, влияние повышенной скорости передачи данных или изменения системы адресации между организациями и отдельными лицами;
d) правовые соображения, такие, как необходимость проверки источника сообщений и др.;
e) последствия для системы безопасности от раскрытия содержания каталогов;
f) необходимость принятия защитных мер для контроля удаленного доступа пользователей к электронной почте.

Организации должны задать четкие правила, касающиеся статуса и использования электронной почты.

12.2 Требования к резервному копированию и восстановлению

1) Резервному копированию в предприятии подлежат базы данных ПО 1С:Предприятие.

2) Резервное копирование архивированных БД должно производится ежедневно.

3) Во избежание ущерба от пожара, наводнения, землетрясения, взрыва, гражданского неповиновения, вирусной и хакерской атаки и других видов природных и антропогенных катастроф резервные копии производятся как на

сервере 1С, так и на внешнем облачном ресурсе и локально на компьютере сотрудника отдела программного обеспечения

4) Резервная информация должна быть обеспечена уровнем физической защиты и защиты от воздействий окружающей среды, в соответствии с уровнем безопасности в основном здании.

12.3 Требования к антивирусной безопасности.

Антивирусные программные средства обнаружения вирусов следует применять для проверки рабочих станций ИС и носителей информации на наличие вирусов. Антивирусные программные средства должны регулярно обновляться и использоваться в соответствии с инструкциями поставщика на серверах и рабочих станциях ИС.

13.Доступность

13.1 Общие требования

1) На случай возникновения аварий, стихийных бедствий и иных внештатных ситуаций должны быть предусмотрены соответствующие меры защиты и обеспечения непрерывной работы и восстановления.

2) Аварии, стихийные бедствия и иные внештатные ситуации должны фиксироваться в полном и тщательном виде. С сохранением данной информации на срок не менее 1 года.

3) В случае возникновения инцидента информационной безопасности или другой внештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей во внештатных (кризисных) ситуациях».

4) Если важное бизнес - приложение должно работать в среде совместного использования, необходимо выявить другие приложения, с которыми будет осуществляться совместное использование ресурсов, и согласовать это с владельцем важного бизнес приложения и соответствующие риски должны идентифицироваться.

13.2 Требования к отказоустойчивости.

1) Аппаратно-программное обеспечение должно обеспечивать выполнение задач ИС со временем однократного простоя не более 24 часов и суммарным временем простоя не более 48 часов в год.

2) В случае возникновения внештатной ситуации произошедшей с производственным сервером ИС восстановление ППО, СПО и ОС должно быть произведено в течение не более 48 часов.

13.3 Требования по обеспечению резервирования и дублирования мощностей.

1) Система хранения данных должна предусматривать автоматический периодический контроль целостности дисков, анализ плохих секторов,

проверку состояния резервных батарей, без вмешательства администратора и без влияния на работу пользователей.

13.4 Требования по обеспечению оперативного мониторинга состояния доступности.

1) Мониторинг ИС включающий в себя опрос состояния ППО, СПО и ОС должен производится ежедневно в течение рабочего дня с помощью специализированного программного обеспечения, в случае изменения состояния доступности ИС должно производиться оповещение администраторов в режиме онлайн.

2) Администраторы должны оперативно устранять выявленные уязвимости в ППО, СПО и ОС.

14.Пересмотр политики информационной безопасности.

14.1 Политика информационной безопасности ИС должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности, адекватности и эффективности.

14.2 Пересмотр политики информационной безопасности КОЦФП должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006.

15. Контроль на соответствие требованиям информационной безопасности

15.1 Контроль требований настоящей политики информационной безопасности центра фтизиопульмонологии на соответствие требованиям информационной безопасности осуществляется сотрудниками подразделения по обеспечению информационной безопасности центра фтизиопульмонологии.

Лист согласования для утверждения Политики информационной безопасности КГП «Костанайский областной центр фтизиопульмонологии»

Должность	Ф.И.О	Подпись	Дата
И.о. главного врача	Молдатаева Ж.Ж.		
И.о зам.главного врача по леч.работе	Досмагамбетова Ж.М.		
Зам.главного врача по орг.метод.работе	Жабагина Г.С.		
Зам.главного врача по экономике и АХЧ	Доспанов Е.С.		
Главный бухгалтер	Турмагамбетова Р. А.		
Зав. организационно-методического кабинета	Андрющенко С.С.		
Зав. отделения внелегочного туберкулеза и дифференциальной диагностики	Досмагамбетова Ж.М.		
Зав. детско-подросткового легочного отделения	Какенова А.Д.		
Зав. терапевтического отделения №1	Тищук Г.Г.		
Зав. отделения для принудительного лечения туберкулезом	Наурызбаева Г.М.		
Зав. терапевтического отделения №2	Искаков И.С.		
Зав. консультативно - диагностического отделения	Жумабаева З.Е.		
Зав. бактериологической лабораторией	Шарипов О.Э.		
Зав. клинико-диагностической лаборатории	Медетова А.А.		