Астана қаласы әкімдігі ШЖҚ «Көпсалалы медицина орталығы» МКК
ГКП на ПХВ «Многпрофильный медицинский центр» акимата города Астаны

Код:	**Пол-1**		
Название документа:	**Политика информационной безопасности**		
Утвержден:	Приказом директора ГКП на ПХВ «Многопрофильный медицинский центр» от «19» января 2024г №92-Ө		
Разработчик:	**Должность**	**ФИО**	**Подпись**
	Руководитель службы экономики и гос.закупок, IT	Сергазина Н.Г.	
	Системный администратор	Қисап Б.	
	Системный администратор	Қапкешев А.	
Согласовано:	Заместитель директора по экономическим вопросам	Нурбеков Б.Б.	
Дата следующего пересмотра – 2027 года			

Астана, 2024

Астана қаласы әкімдігі ШЖҚ «Көпсалалы медицина орталығы» МКК
ГКП на ПХВ «Многпрофильный медицинский центр» акимата города Астаны

Политика информационной безопасности

1. Цель

Целью обеспечения информационной безопасности является минимизация экономического, финансового, социального, институционального и экологического ущерба от реализации угроз информационной безопасности, а также повышение общего уровня конфиденциальности, целостности и доступности информации в информационной системе в ГКП на ПХВ «Городской онкологический центр» УЗ г.Шымкент (далее - Центр).

2. Область применения

1) Политика предназначена для обеспечения информационной безопасности и распространяется на всех работников Центра.
2) Политика обязательна для исполнения всеми лицами, работающими с инфраструктурой Центра, в том числе для третьих лиц, выполняющих работы по технической поддержке/сопровождению информационной системы Центра.

3. Нормативные ссылки

1) Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» (с изменениями и дополнениями по состоянию на 16.05.2018 г.);
2) Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года»;
3) Постановление Правительства Республики Казахстан от 23 мая 2016 года № 298 «Об утверждении Правил проведения аттестации информационной системы, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа на соответствие требованиям информационной безопасности» (с изменениями от 09.04.2018 г.);
4) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 «Информационная технология. Методы обеспечения защиты. Свод правил по управлению защитой информации»;
5) СТ РК ISO/IEC 27001-2015 Информационная технология Методы и средства обеспечения безопасности Системы менеджмента информационной безопасностью. Требования;

4. Термины, определения и сокращения

1) *Аутентификация*- подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованных в системе
2) *Авторизация* - предоставление прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.
3) *Государственные секреты* - защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной медицинской, военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права
4) *Доступность* - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно
5) *Аутентификация*- подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа, реализованных в системе
6) *Авторизация* - предоставление прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.
7) *Государственные секреты* - защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной медицинской, военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права
8) *Доступность* - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно
9) *Информационная безопасность (далее - ИБ)*- состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации.
10) *ИБП* - источник бесперебойного питания
11) *ИС*- информационные системы

12) *Инфраструктура ИС*- каналы связи, оборудование, программное обеспечение, сотрудники и пользователи, документация, информация информационных систем.
13) *Конфиденциальность информации*- обеспечение предоставления информации только авторизированным лицам по уровням доступа
14) *ОМС* - организационно-методическая служба
15) *ОС* - операционная система
16) *ПО* - программное обеспечение
17) *Пользователи ИС*- лица, работающие с ИС
18) *ПП РК*- Постановления Правительства Республики Казахстан
19) *СВТ*- средства вычислительной техники
20) *Целостность информации*- состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право

5. Ответственность

1) Специалисты, отвечающие за информационную безопасность ответственность за контроль за выполнением всех пунктов данной Политики. Должен обеспечить четкое управление и зримую поддержку инициатив в области поддержки информационной безопасности информационной системы.
2) Специалисты, отвечающие за информационную безопасность должны обеспечивать координацию мер контроля в эксплуатируемых информационных системах.
3) Специалисты, отвечающие за информационную безопасность должны предоставлять ресурсы для обеспечения мер информационной безопасности.
4) Директор, и/или лицо назначенное Директором должен утверждать распределение специфических ролей и обязанностей по информационной безопасности.
5) Обслуживающий персонал при нарушении требований пунктов Политики информационной безопасности будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.
6) Специалисты, отвечающие за информационную безопасность должны обеспечить контроль издания и доведения до сведения утвержденных документов по информационной безопасности до обслуживающего персонала и пользователей информационных систем Медицинской организации
7) Специалисты, отвечающие за информационную безопасность должны инициировать планы и программы по поддержанию осведомлённости об информационной безопасности.
8) Ответственность на администраторов информационных систем возлагается в соответствии с зонами их ответственности.

9) Администраторы информационных систем обязаны:
a) обеспечивать обязательность процедуры идентификации и аутентификации для доступа к ресурсам информационных систем;
b) не допускать получения права доступа к информационным системам неавторизированным пользователям и представлять пользователям входные имена и начальные пароли только после заполнения установленных регистрационных форм;
c) обеспечивать защиту оборудования, в том числе специальных межсетевых программных средств;
d) оперативно и эффективно реагировать на события, содержащие угрозу, принимать меры по отражению угрозы и выявлению нарушителей, фиксировать и информировать специалистов, отвечающие за информационную безопасность о попытках нарушения защиты.

6. Ресурсы

1) Серверное помещение, отвечающее всем требованиям;
2) Источник бесперебойного питания необходимой мощности;
3) Внутренние нормативные документы.

7. Общие положения

7.1. Настоящая Политика информационной безопасности является внутренним нормативным документом Центра. Политика устанавливает требования к обеспечению Центра, определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих Положений, Правил, Инструкций. Под 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 – обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Целью обеспечения ИБ является минимизация экономического, финансового, социального, институционального и экологического ущербов от реализации угроз ИБ, а также повышение общего уровня конфиденциальности, целостности и доступности информации в ИС.

7.2. Политика ИБ распространяется на функционирование всей инфраструктуры Центра.

7.3. Политика ИБ обязательна для исполнения всеми лицами, работающими с инфраструктурой, в том числе для третьих лиц, выполняющих работы по сопровождению либо развитию ИС.

7.4. Исполнение требований политики ИБ обеспечивают все лица, работающие с инфраструктурой информационных систем.

7.5. Действия по обеспечению ИБ должны координироваться руководством и специалистами, ответственных за ИБ.

7.6. Координация ИБ должна осуществлять следующую деятельность:

a) обеспечивать соответствие выполняемых действий по обеспечению ИБ политике ИБ;

b) определение действий в случае несоответствия выполняемых действий по обеспечению ИБ политике по ИБ;

c) утверждение методологии и процессов обеспечения ИБ, например, оценку рисков, классификацию информации;

d) идентифицировать значительные изменения угроз и подвергание информации и средств обработки информации угрозам;

e) оценивание адекватности и координирования реализации мер контролю ИБ;

f) эффективное способствование обучению, подготовке по ИБ и осведомлённости о ней;

g) оценивание информации, полученной от мониторинга и пересмотра инцидентов ИБ, и внесение рекомендаций в ответ на идентифицированные инциденты ИБ.

8.Описание управления информационной безопасностью

8.1. Конфиденциальность

1) Главным требованием конфиденциальности является обеспечение предоставления информации только авторизированным лицам.

2) Информация, обрабатываемая и хранящаяся в ИС, подлежит копированию и передаче третьему лицу только с официального разрешения руководства.

3) При работе с ИС должна исключаться возможность наблюдения за отображаемой информацией посторонними лицами.

4) В ИС не должны размещаться документы, содержащие государственные секреты, коммерческую тайну и иную информацию с ограниченным доступом.

5) Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации.
6) При работе с ИС должны использоваться специальные лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.
7) Информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для ИС.

8.2.Соглашения о конфиденциальности

1) Требования по соглашениям о конфиденциальности или неразглашении, отражающие потребности по защите безопасности, должны быть определены и регулярно пересмотрены.
а)Для определения требований по соглашениям о конфиденциальности или неразглашении необходимо рассмотреть следующие элементы:
a) определение информации, которая должна быть защищена (т.е. конфиденциальная информация или информация, содержащая коммерческую тайну);
b) предполагаемая продолжительности соглашения, включая случаи, когда конфиденциальность должна поддерживаться бесконечно;
c) требуемые действия по окончанию соглашения;
d) обязанности и действия подписавших сторон во избежание несанкционированного разглашения информации (такого как «принцип необходимого знания»);
e) собственность на информацию, коммерческие секреты и интеллектуальную собственность и то, как она связана с защитой конфиденциальной информации;
f) разрешённое использование конфиденциальной информации и право подписавшей стороны использовать информацию;
g) право аудита и мониторинга действий, в которых задействована конфиденциальная информация;
h) процесс уведомления и сообщения о несанкционированном разглашении или нарушении конфиденциальности информации и коммерческой тайны;
i) условия о возврате или уничтожении информации при прекращении действия соглашения;
j) предполагаемые действия в случае нарушения данного соглашения.
В соглашении о конфиденциальности или неразглашении могут потребоваться другие элементы, основанные на требованиях безопасности. Соглашения о конфиденциальности и неразглашении должны соответствовать всем применяемым правовым нормам и правилам юрисдикции, которые применяются.

9. Требования

9.1. Требования к обучению и осведомленности в вопросах ИБ

1) Обслуживающий персонал ИС, пользователи и администраторы ИС, должны быть ознакомлены с политикой ИБ.
2) Обслуживающий персонал ИС должен предоставить пользователям ИС рабочую документацию (Инструкция о парольной защите ИС).
3) Обслуживающий персонал ИС по запросу пользователей должен проводить первичный инструктаж по ИБ.
4) Обслуживающий персонал, обеспечивающий функционирование ИС должен проходить регулярно инструктаж по соблюдению ИБ.
5) Обслуживающий персонал ИС должны принять пользовательское соглашение о конфиденциальности.
6) В целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьей стороной мероприятия по управлению ИС.
7) В целях обеспечения гарантированного уведомления подразделения ответственного за ИБ, обслуживающего персонала ИС 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.
8) В рамках работ осуществляется обучение новых сотрудников в работе ИС, разъясняется функция копирования и вставки информации в электронную медицинскую карту и стратегиям и тактикам, применяемым для планового и внепланового простоя ИС.
9) Обслуживающий персонал ИС должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, и о наступлении которых или предпосылках к таковому необходимо отправить уведомление.
10) Обслуживающий персонал и администраторы ИС обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственным за ИБ лицам.

9.2. Требования по аутентификации ИС

Администраторы и пользователи ИС должны проходить безопасную аутентификацию, идентифицирующую их и исключающую возможность подбора пароля и перехвата авторотационных данных.

9.3. Требования к пользовательским учетным записям и паролям

Требования к пользовательским учетным записям и паролям приведены во внутреннем нормативном документе «Инструкция о парольной защите ИС».

9.4. Контроль обеспечения конфиденциальности

С целью контроля обеспечения конфиденциальности должны обеспечиваться следующие мероприятия:

a) ежегодный анализ ИБ ИС на соблюдение требований ИБ, с результатом в виде отчета.

b) постоянный мониторинг инструментальными средствами ИБ серверов ИС и сети, в которой они находятся.

c) обеспечение предоставления информации авторизированным лицам.

d) подключение пользователей ИС должны строго фиксироваться с сохранением данной информации.

e) информация, обрабатываемая и хранящиеся в ИС, подлежит копированию и передаче третьим лицам только с официального разрешения руководства.

f) при работе с ИС должна исключаться возможность наблюдения за отображаемой информацией третьими лицами.

g) в ИС не должны размещаться документы, содержащие государственные секреты и информацию с ограниченным доступом.

h) электронные истории болезни, электронные амбулаторные карты, результаты инструментальной диагностики и лабораторных исследований, хранящиеся в ИС, не подлежат копированию и передаче третьим лицам, только по запросу уполномоченного органа или иное предусмотренное законом Республики Казахстан.

i) при работе с ИС должны использоваться лицензионные программные или аппаратные средства, обеспечивающие защиту от вредоносных программ, вирусов и сетевых атак.

j) информация должна классифицироваться с точки зрения ее ценности, правовых требований, секретности и критичности для ИС Центра.

9.5. Целостность

1) Главным требованием целостности является обеспечение изменения информации только авторизированными лицами по уровням доступа.

2) Новые программно-аппаратные средства, внедряемые должны быть соответствующим образом одобрены со стороны руководства и специалистов, ответственных за обеспечение ИБ.

3) Аппаратные средства и программное обеспечение перед внедрением следует проверять на совместимость с другими компонентами системы.

9.6. Требования к антивирусной безопасности

Требования к антивирусной защите приведены во внутреннем нормативном документе «Инструкция по организации антивирусной защиты».

9.7. Требования к применению электронной почты и Интернета

Требования по использованию электронной почты и Интернета приведены во внутреннем нормативном документе «Инструкция по использованию электронной почты и служб Интернет на подстанциях».

9.8. Доступность

1) Главным требованием доступности является обеспечение состояния информации (ресурсов автоматизированной информационной системы), при котором авторизированные лица могут работать с ней беспрепятственно.
2) В случае возникновения внештатных ситуаций, аварий, стихийных бедствий и иных ситуаций, которые могут повлиять, должны быть предусмотрены соответствующие меры защиты и обеспечения непрерывной работы и восстановления.
3) Аварии, стихийные бедствия и иные внештатные ситуации должны фиксироваться в полном и тщательном виде, с сохранением данной информации на срок не менее 2-х лет.
4) В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей во внештатных (кризисных) ситуациях».

9.9. Требования по бесперебойному питанию

Бесперебойное электропитание обеспечивается ИБП (источником бесперебойного питания) необходимой мощности, который должен гарантировать, как минимум, корректное завершение работы приложений и сворачивание операционной системы при отключении внешнего электропитания.

9.10. 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.
2) Система хранения данных должна обеспечивать возможность «горячей» замены дисков.

9.11.Требования по обеспечению оперативного мониторинга состояния доступности

Мониторинг ИС производится ежедневно в течение рабочего дня с помощью специализированного программного обеспечения, в случае изменения состояния доступности ИС произойдет оповещение администратора в режиме «онлайн».

9.12.Управление инцидентами и несоответствиями требованиям ИБ

Кроме сообщений о случаях нарушения и слабых местах ИБ для обнаружения инцидентов нарушения ИБ должен применяться мониторинг систем, предупреждений и уязвимостей. Для процедур управления инцидентами нарушения ИБ должны рассматриваться следующие правила:

1) Для работы с различными типами инцидентов необходимо установить следующие процедуры:
   a) сбои информационных систем и утрата сервисов;
   b) вредоносный код;
   c) отказ в обслуживании;
   d) ошибки вследствие неполных или неточных данных;
   e) нарушения конфиденциальности и целостности;
   f) неправильное использование информационных систем;
2) Дополнение к обычным планам обеспечения непрерывности должны существовать процедуры касательно:
   a) анализа и идентификации причины инцидента;
   b) локализации;
   c) планирования и внедрения средств, предотвращающих повторное проявление
   d) инцидентов, при необходимости;
   e) взаимодействия с лицами, на которых инцидент оказал воздействие, или участвующих в устранении последствий инцидента;
   f) информирования о действиях соответствующих должностных лиц;
   g) действия по устранению сбоев систем и ликвидации последствий инцидентов нарушения ИБ должны быть под тщательными формализованным контролем.
3) Необходимо наличие процедур с целью обеспечения уверенности в том, что:
   a) только полностью идентифицированному и авторизованному персоналу предоставлен доступ к системам и данным в среде промышленной эксплуатации;
   b) все действия, предпринятые при чрезвычайных обстоятельствах, подробно документально оформлены;

c) о действиях, предпринятых при чрезвычайных обстоятельствах, сообщено руководству, и они проанализированы в установленном порядке;
d) целостность бизнес-систем и систем контроля подтверждена в минимальные сроки.
e) цели управления инцидентами нарушения ИБ должны быть согласованы с руководством и лица, ответственные за управление инцидентами, должны знать приоритеты при работе с инцидентами нарушения ИБ.

Администраторы ИС должны оперативно устранять выявленные уязвимости.

9.13.Требования к документации

a) Обязательно требуемые к разработке внутренние нормативные документы:
b) Правила паспортизации средств вычислительной техники и использования информационных ресурсов;
c) Инструкция о парольной защите;
d) Инструкция о порядке действий пользователей во внештатных (кризисных) ситуациях;
e) Инструкция пользователя по эксплуатации компьютерного оборудования и программного обеспечения;
f) Инструкция по организации антивирусной защиты;
g) Инструкция по закреплению функций и полномочий администратора сервера;
h) Правила доступа пользователей и администраторов в серверные помещения;
i) Правила регистрации пользователей в корпоративной информационной сети;
j) Памятка для работы системных администраторов;
k) Памятка пользователю средств вычислительной техники;
l) Инструкция по использованию электронной почты и служб Интернет на рабочих станциях;
m) Инструкция о резервном копировании информации.

9.14.Требования к анализу и оценке рисков

1) Политика ИБ первоначально должна основываться на данных, полученных в результате анализа и оценки рисков ИБ.
2) С целью совершенствования политики ИБ должен проводиться ежегодный анализ и оценка рисков ИБ.
3) Анализ и оценка рисков должны проводиться в соответствии со стандартами, действующими на территории Республики Казахстан, а также внутренними нормативными документами.
4) При оценке рисков должно учитываться влияние реализации угроз ИБ на финансовое состояние. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.
5) Формализованная процедура проведений анализа рисков описана в Приложении.
6) На основе результатов анализа затрат и выгод рисков, руководство соответствующего СТП определяет, наиболее экономически эффективные меры для снижения риска. Выбранные меры должны объединить технические, эксплуатационные и управленческие меры для обеспечения надлежащей безопасности для ИС.
7) Уровень мониторинга конкретных средств обработки информации следует определять на основе оценки рисков. При мониторинге следует обращать внимание на:

a) авторизованный доступ, включая следующие детали:
b) пользовательский ID;
c) даты и время основных событий;
d) типы событий;
e) файлы, к которым был осуществлен доступ;
f) используемые программы/утилиты;
g) все привилегированные действия, такие как:

1) использование привилегированных учетных записей, например, корневого каталога, администратора;
2) запуск и остановка системы;
3) подсоединение/отсоединение устройства ввода/вывода;
4) попытки несанкционированного доступа, такие как:
5) неудавшиеся или отвергнутые действия пользователя;
6) неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;
7) нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;
8) предупреждения от собственных систем обнаружения вторжения.

9.15 Пересмотр политики ИБ

1) Политика ИБ должна быть закреплена за ответственным лицом, который имеет право утверждать административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики ИБ ИС и подход к управлению ИБ в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.
2) При пересмотре политики ИБ необходимо учитывать результаты пересмотров управления. Здесь должны быть определены процедуры пересмотра, включая график или продолжительности пересмотра.
3) Входные данные для пересмотра управления должны включать информацию по:
a) обратной связи от заинтересованных сторон;
b) результатам независимых пересмотров;
c) статусу превентивных и корректирующих действий;
d) результатам предыдущих пересмотров;
e) характеристикам процесса и соответствию политики безопасности информации;
f) изменениям, которые могут повлиять на подход ССМП к управлению ИБ, включая изменения в организационной среде, деловой ситуации, наличии ресурсов, договорных, регулятивных или юридических условиях или в технической среде;
g) тенденции, связанные с угрозами и уязвимостями;
h) сообщённым инцидентам ИБ;
i) рекомендациям, представленным соответствующими учреждениями.
4) Политика ИБ должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности.

9.15.Контроль на соответствие требованиям ИБ

Контроль требований настоящей политики ИБ осуществляют специалисты, отвечающие за ИБ.

10. Документирование

Ежегодный анализ информационной безопасности информационных систем с результатом в виде отчет

Приложение 1

Оценка возможных технических рисков

Вид риска	Описание	Измерения и меры по снижению риска
Выход из строя сервера	Сбой в работе аппаратного или ПО сервера.	Измеряется в процентной доле времени штатного функционирования. Предусматривать длительный срок гарантийного обслуживания при заключении договора, а по его окончании - резервирование серверов
Выход из строя рабочей станции	Сбой в работе аппаратного или ПО рабочей станции.	Измеряется в процентной доле времени штатного функционирования. Приобретение только у ведущих мировых производителей, имеющих сертифицированные сервис центры
Потеря или искажение данных при передаче	Частичная потеря или искажение данных при передаче по каналам связи из-за сбоев в телекоммуникационном оборудовании с учетом корректирующих свойств коммуникационных протоколов.	Измеряется в доле потерянных либо искаженных данных. Перевод на наземные каналы связи и резервирование каналов
Потеря или искажение данных при хранении	Риск вызван возможностью сбоев в файловой системе диска или физическими ошибками на накопителях, с учетом способа хранения данных в БД.	Измеряется в среднем времени между отказами в часах. Наращивание систем хранения информации, периодическое резервное копирование согласно инструкции.
Быстрое моральное устаревание технологий	Неприятие ППО пользователями	Уточнение требований заявителя по платформенной независимости ППО
Приобретение морально-устаревшей техники	Отсутствие комплектующих материалов Отсутствие технической поддержки морально-устаревшего оборудования	Уточнение требований заявителя составлением детальных технических спецификаций на работы при подписании договоров с Поставщиками услуг
Снижение ИБ	Внешнее воздействие на информационные сети, в том числе атаки хакеров и компьютерных вирусов	Мониторинг и аудит системы обеспечения ИБ. Осуществление анализа эффективности принятых мер по защите информации с учетом изменений ИКТ-среды, появление новых угроз, инцидентов и проблем. Внедрение дополнительных мер защиты