Код:	MOI – 05		
Название:	**Политика информационной безопасности**		
Утвержден:	Приказ председателя правления АО «Национального научного медицинского центра» от «10» декабря 2019 года № 528		
Разработчик:	Должность	Ф.И.О.	Подпись
	Специалист по информационной безопасности	Қ.Сатыбалдиев	
	Руководитель отдела по внедрению информационных технологий	А.Әбдунабі	
Проверил:	Руководитель службы стратегии и качества	Ж.Нуразханова	
	Руководитель ОМКиС	Б.Кубжасарова	
Согласовано:	Первый заместитель председателя правления	Е. Кадырова	

Дата последнего пересмотра 25.11.2019 год
Дата следующего пересмотра 25.11.2022 год

Нур-султан– 2019 год

Содержание

1. Сокращения

ИБ – Информационная безопасность.
ИС – Информационная система – совокупность программных и аппаратных средств, процедур и технологий, а также человеческих ресурсов, которые обеспечивают выполнение задач по обработке, хранению и передачи информации в соответствии с заключенными с заказчиками соглашениями или в их интересах.
КД – Корректирующие действие.
ОМКиС – Отдел по менеджмента качеств и стандартизации.
ПД – Предупреждающие действие.
ПО – Программное обеспечение.
РК – Республика Казахстан.
СИБ – Ответственный специалист в сфере обеспечния ИБ.

2. Определения

Администраторы – технические специалисты ННМЦ, обеспечивающие ввод в эксплуатацию, поддержку, сопровождение и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
Аутентификация – Процедура проверки подлинности.
Политика – Политика информационной безопасности.

3. Цели политики информационной безопасности

Основными целями Настоящей Политики являются:
1. повышение уровня доступности, конфиденциальности, целостности ресурсов, находящихся в инфраструктуре ННМЦ;
2. минимизация возможного ущерба, связанного с нарушениями требований информационной безопасности.

4. Пользователи

К пользователям информационных систем относятся:
1. сотрудники ННМЦ – служащие, осуществляющие свою деятельность в ННМЦ и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
2. вспомогательный персонал – обслуживающий и технический персонал подведомственных и сторонних организаций, осуществляющих взаимодействие с ННМЦ в качестве поставщиков и потребителей (пользователей) информации и услуг. В том числе:
2.1 администраторы корпоративной сети передачи данных, ответственные за

сопровождение телекоммуникационного оборудования;
2.2 системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;
2.3 разработчики прикладного программного обеспечения;
2.4 инженеры-системотехники, технические специалисты;
2.5 специалисты по информационной безопасности (специальных средств защиты) и др.;
2.6 потребители услуг ННМЦ – лица и/или сторонние организации, использующие информационные ресурсы ННМЦ.
3. пациенты.

5. Описание
5.1 Принципы и их описание

1) Политика базируется на следующих принципах:
1. законность;
2. системность;
3. комплексность;
4. эффективность;
5. целесообразность;
6. конфиденциальность;
7. целостность;
8. доступность;
9. осведомленность и персональная ответственность.

2) Описание принципов:
1. законность – соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;
2. системность – подход к вопросам организации ИБ должен быть логическим и последовательным, основанным на оценке рисков ИБ;
3. комплексность – подход к обеспечению ИБ должен быть целостным и охватывать все необходимые аспекты;
4. эффективность – реализуемые в разумно достаточном объеме меры и мероприятия по управлению ИБ должны сводить риски к минимуму;
5. целесообразность – соблюдение соразмерности затрат на обеспечение защиты информации и потенциального ущерба при реализации угроз;
6. конфиденциальность – предоставление доступа к информации только авторизованным пользователям, защита чувствительной информации от несанкционированного доступа;
7. целостность информации – существование информации в неискаженном виде, неизменном по отношению к ее некоторому фиксированному состоянию, а также возможность ее изменения только теми лицами, которые имеют на это право;

8. доступность – наличие доступа к информации авторизованному пользователю в любое время;
9. осведомленность и персональная ответственность – пользователи и Администраторы ИС должны быть информированы об угрозах ИБ и мерах противодействия им, а также нести персональную ответственность за несоблюдение требований ИБ.

5.2 Общие положения

3) Настоящая Политика информационной безопасности (далее – Политика) предназначена для определения целей и требований обеспечения информационной безопасности в АО «Национальный научный медицинский центр» (далее –ННМЦ).
4) Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности.
5) Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – обеспечением возможности получения доступа к данным авторизованным лицам в нужное для них время.

5.3 Требования по управлению информационной безопасности

6) Требования по управлению информационной безопасностью:
1. обеспечение защиты ресурсов, находящихся в инфраструктуре ННМЦ, от проникновения вредоносного ПО;
2. обеспечение защиты ресурсов, находящихся в инфраструктуре ННМЦ, от сетевых атак;
3. обеспечение защиты ресурсов, находящихся в инфраструктуре ННМЦ, от несанкционированного доступа;
4. обеспечение сбора событий из журнала событий ИС и регистрации отчетов об инцидентах в ОМКиС, находящихся в инфраструктуре ННМЦ, для использования в качестве доказательной базы;
5. обеспечение конфиденциальности предоставляемой информации находящихся в инфраструктуре ННМЦ, путем использание специальных средств;
6. обеспечение изменения информации в ресурсов, находящихся в инфраструктуре ННМЦ, только уполномоченными на то Пользователями;
7. обеспечение надежного и бесперебойного функционирования ресурсов, находящихся в инфраструктуре ННМЦ;

8. систематическое выполнение работ по выявлению и устранению технических уязвимостей ресурсов, согласно реестра управления рисками находящихся в инфраструктуре ННМЦ;
9. разделение сред разработки, тестирования и промышленной эксплуатации ИС;
10. организация резервного копирования и тестирования резервных копий;
11. проведение анализа и оценки рисков ИБ ИС, находящихся в инфраструктуре ННМЦ;
12. обеспечение оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
13. проведение внутреннего аудита ресурсов, находящихся в инфраструктуре ННМЦ, с периодичностью не реже 1 раза в год.

5.4 Обязанности руководства по достижению целей по управлению информационной безопасности

7) Представитель высшего руководства - первый заместитель председателя правления (далее – ПВР) обеспечивает своевременное выделение необходимых ресурсов (финансовых, человеческих и т.д.) для достижения целей Политики.
8) СИБ планирует контроль достижение целей Политики ИБ, контроль над выполнением требований ИБ, обеспечивает эффективную реализацию мер ИБ и проводит КД, ПД по улучшению.
9) СИБ осуществляет общее управление ИБ ИС, находящихся в инфраструктуре ННМЦ и обеспечивает необходимые условия для:
1. реализации запланированных мероприятии по оценке рисков информационной безопасности и защиты информации;
2. мониторинга, анализа, поддержания и непрерывного улучшения системы управления ИБ;
3. регулярного обучения Администраторов ИС в сфере ИБ.
4. четкого управления внедрением инновации, реализацией инициатив в области поддержки ИБ ИС, находящихся в инфраструктуре ННМЦ.
10) Администраторы и Пользователи ИС несут персональную ответственность за соблюдение требований нормативно-технических документов по ИБ и обязаны сообщать обо всех выявленных инцедентов в области ИБ в отдел стратегии, менеджмента качества и безопасности пациентов и ответственным за ИБ.

5.5 Требования при нарушении политики информационной безопасности

11) При выявлении фактов нарушения Политики или требований иных нормативно-технических документов по ИБ в ННМЦ предпринимаются мероприятия по снижению возможного ущерба и восстановлению штатного функционированию ресурсов(при необходимости).

12) Руководитель ОМКиС формирует рабочую группу для проведения служебного расследования, по результатам которого производится:
1. анализ корневых причин инцидента;
2. переоценка рисков;
3. анализ эффективности существующих КД и ПД по недопущению нарушений требований ИБ и реагированию на них, а при необходимости – выработка дополнительных КД и ПД с последующей их реализацией;
4. привлечение к ответственности Администраторов и Пользователей, допустивших нарушение требований ИБ.

5.6 Функции сотрудников в рамках управления информационной безопасностью

13) Функции сотрудников в рамках управления ИБ документированы в настоящей Политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех Пользователей и Администраторов. Документированные требования по управлению ИБ доводятся до сведения Администраторов и Пользователей.
14) Администраторы и Пользователи получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей. Осуществляется их информирование, обучение и повышение квалификации работников в сфере ИБ. Прохождение обучения в сфере ИБ осуществляется при устройстве на работу.
15) Администратор в рамках управления информационной безопасностью обязан обеспечивать защиту активного сетевого оборудования, серверов, приложений.

5.7 Требования к документации

16) Требуемые к разработке обязательные документы:
1. Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;
2. Методика оценки рисков информационной безопасности;
3. Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;
4. Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;
5. Правила проведения внутреннего аудита информационной безопасности;
6. Правила использования криптографических средств защиты информации;
7. Правила разграничения прав доступа к электронным ресурсам;
8. Правила использования сети Интернет и электронной почты;
9. Правила организации процедуры аутентификации;
10. Правила организации антивирусного контроля;

11. Правила использования мобильных устройств и носителей информации;
12. Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов;
13. Руководство администратора по сопровождению объекта аттестации;
14. Регламент резервного копирования и восстановления информации;
15. Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и внештатных (кризисных) ситуаций.
17) Все перечисленные документы регулярно пересматриваются и в случае появления существенных изменений, актуализируются и утверждаются по мере необходимости.

5.8 Ответственность и обязательства руководства

18) Руководства должно активно поддерживать меры по поддержанию ИБ ИС, находящихся в инфраструктуре ННМЦ, посредством ясных указаний, открыто принятых обязательств, четких постановок задач и осведомленности работников об обязанностях по обеспечению ИБ:
1. обеспечивать координацию мер контроля над информационной безопасностью в ИС;
2. эффективно способствует обучению, подготовке по ИБ и осведомлённости о ней;
3. оценивать информацию, полученную от мониторинга и пересмотра инцидентов ИБ, и рекомендовать соответствующие действия в ответ на идентифицированные инциденты ИБ;
4. идентифицировать значительные изменения, подвергания информации и средств обработки информации угрозам;
5. контролировать включение в должностные инструкции сотрудников ННМЦ необходимые аспекты, связанные с информационной безопасностью в соответствии с исполняемой должностью, и контролировать их соблюдение;
6. формулировать, пересматривать, утверждать Политику.

5.9 Пересмотр политики информационной безопасности

19) Политика должна пересматриваться и переутверждаться в случае существенных изменений инфраструктуре ННМЦ, возникновении новых угроз информационной безопасности или на основании анализа и оценки:
1. состояния и эффективности системы информационной безопасности;
2. выявленных инцидентов и нарушений требований информационной безопасности;
3. рисков и технологий, влияющих на состояние системы информационной безопасности;

4. законодательства Республики Казахстан и в области информационной безопасности;
5. результатов аудита по информационной безопасноти.

5.10 Рассылка политики информационной безопасности

20) Рассылка Политики проводится специалистом ОМКиС по всем отделам ННМЦ.
21) Политика распространяется на функционирование всей инфраструктуры и обязательна для исполнения всеми лицами, работающими в ННМЦ.

6. Базовая ссылка:

1. Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи» (с изменениями, внесенными Законом РК от 20.12.04 г. № 13-III);
2. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;
3. Закон Республики Казахстан «О техническом регулировании » от 9 ноября 2004 года №603;
4. Закон Республики Казахстан от 24 ноября 2015 года №418-V «Об информатизации»;
5. СТ РК ИСО/МЭК 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования»;
6. СТ РК ИСО/МЭК 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

7. Лист регистрации изменений и дополнений

№	№ раздела, подраздела, пункта стандарта, к которому относится изменение	Номер листа	Дата введения изменения	Основание (№ и дата приказа)	Дата внесения изменения	Подпись лица, внесшего изменения

8. Лист ознакомления

№	Ф.И.О.	Занимаемая должность	Дата	Подпись	Примечание