УТВЕРЖДЕНА
приказом директора
ИП «PROFIT»
от «___» _____ 2017 г.
№ _____

Политика информационной безопасности ИП «PROFIT»

1. Назначение документа

Документ предназначен для определения целей и требований обеспечения информационной безопасности медицинской информационной системы «Надежда» (далее – МИС «Надежда») ИП «PROFIT».

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается предоставлением доступа к информационным ресурсам только авторизованным пользователям, целостность – в случае внесения изменений в данные авторизованными пользователями, доступность – в обеспечении возможности доступа к информационным ресурсам авторизованным пользователям в нужное для них время.

2. Глоссарий

Термины, использованные в настоящем документе, имеют следующие определения:

База данных – совокупность связанных данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования, независимая от прикладных программ. База данных является информационной моделью предметной области.

Информационная безопасность (ИБ) – комплекс правовых, технических и организационных мероприятий, направленных на обеспечение защиты информационных ресурсов от несанкционированного доступа, преднамеренного или случайного искажения и разрушения, физического разрушения, в том числе в результате воздействий техногенного и природного характера. А также состояние защищенности государственных информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации.

Информационная система – система, организующая, хранящая и преобразующая информацию, то есть систему, основным предметом и продуктом труда в которой является информация.

Администратор ИС – работник, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования всего комплекса МИС «НАДЕЖДА».

Пользователь ИС – работники, работающие с МИС «НАДЕЖДА».

Конфиденциальность информации – обеспечение предоставления информации только авторизированным лицам.

Целостность информации – состояние информации (информационных ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только авторизованными пользователями.

Доступность – обеспечение возможности доступа авторизованным пользователям к информационным ресурсам автоматизированной информационной системы в нужное время.

Перечень сокращений, использованных в настоящем документе, представлен в таблице.

3. Ссылки

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами и документами:

- Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»;
- СТ РК 34.005-2002 «Основные термины и определения в области информационных технологий»;
- СТ РК 34.006-2002 «Основные термины и их определения в области баз данных»;
- СТ РК 34.007-2002 «Основные термины и их определения в области телекоммуникационных сетей»;
- Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27002-2009 «Информационная технология. Средства обеспечения. Свод правил по управлению защитой информации»;
- Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27001-2008 «Методы и средства обеспечения безопасности системы управления информационной безопасностью».
-

4. Цели и задачи обеспечения ИБ

Целью обеспечения информационной безопасности является предотвращение и минимизация ущербов от реализации угроз информационной безопасности, а также повышение общего уровня

конфиденциальности, целостности и доступности информации в МИС «НАДЕЖДА».

Задачами обеспечения ИБ являются:

- обеспечение непрерывности деятельности МИС «НАДЕЖДА» организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов посредством комбинации предупреждающих и восстанавливающих мер и мероприятий;

- управление рисками в целях недопущения или снижения вероятности возникновения внештатных ситуаций;

- выявление и недопущение нарушений, а также условий для их реализации;

- создание механизма оперативного мониторинга и реагирования на нарушения.

5. Основные принципы обеспечения ИБ

Основным принципом является защита МИС «НАДЕЖДА» от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

Защита МИС «НАДЕЖДА» достигается посредством обеспечения и постоянного поддержания следующих свойств:

– доступности обрабатываемой информации;
– обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники (далее СВТ) и передаваемой по каналам связи;
– целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой и передаваемой по каналам связи.

Для обеспечения указанных свойств ИП «PROFIT» должно обеспечивать эффективное решение следующих задач:

– защиту от вмешательства в процесс функционирования посторонних лиц (возможность использования МИС «НАДЕЖДА» и доступ к ее ресурсам

должны иметь только зарегистрированные установленным порядком пользователи;

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:
- к информации;
- средствам вычислительной техники;
- аппаратным, программным и криптографическим средствам зашиты.
- регистрацию действий пользователей при использовании защищаемых ресурсов в системных журналах на периодический контроль корректности действий пользователей МИС «НАДЕЖДА» путем анализа содержимого этих журналов работником, ответственным за обеспечение ИБ;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности МИС «НАДЕЖДА», а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту конфиденциальной информации, информации с ограниченным доступом, персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту конфиденциальной информации, персональных данных, информации с ограниченным доступом, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам МИС «НАДЕЖДА», создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

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

6. Область распространения

7.

Политика информационной безопасности распространяется на функционирование МИС «НАДЕЖДА» в целом.

Политика информационной безопасности обязательна для исполнения всеми пользователями, работающими в МИС «НАДЕЖДА».

Исполнение требований политики информационной безопасности МИС «НАДЕЖДА» обеспечивают все пользователи, работающие с МИС «НАДЕЖДА».

8. Распределение обязанностей по обеспечению ИБ

Руководство ИП «PROFIT» обязано активно реализовывать комплекс мероприятий по поддержанию МИС «НАДЕЖДА» посредством дачи ясных указаний, демонстрированных обязательств, четких постановок задач и осведомленности работников об обязанностях по обеспечению ИБ:

- Руководство обеспечивает формирование и контроль выполнения всех пунктов данной политики;
- Руководство должно пересматривать эффективность реализации политики ИБ;
- Руководство должно обеспечить четкое управление и зримую поддержку инициатив в области поддержки Системы;
- Руководство должно обеспечивать координацию мер контроля за ИБ в МИС «НАДЕЖДА»;
- Руководство должно предоставлять ресурсы для обеспечения ИБ;
- Руководство должно утверждать распределение специфических ролей и обязанностей по ИБ;
- Руководство должно инициировать планы и программы по поддержанию осведомленности об ИБ;

Администраторы МИС «НАДЕЖДА» обязаны действовать в строгом соответствии с зонами их ответственности, согласно Руководству администратора МИС «НАДЕЖДА».

9. Координация ИБ

Действия по обеспечению ИБ должны координироваться руководством ИП «PROFIT» в соответствии с их компетенцией и должностным положением.

Координация ИБ должна включать взаимосвязь и сотрудничество, пользователей, администраторов, разработчиков прикладного программного обеспечения, и квалифицированных специалистов в таких областях, как кадровые ресурсы, информационные технологии и управление рисками. Эта деятельность должна:

- Обеспечивать соответствие выполнения мероприятий по обеспечению ИБ политике ИБ;
- Определять мероприятия по обеспечению ИБ в случае её несоответствия политике ИБ;
- Утверждать методологии и процессы обеспечения ИБ, например, оценку рисков, классификацию информации;
- Идентифицировать все изменения угроз ИБ и степень уязвимости информации и средств обработки информации к угрозам ИБ;
- Оценивать адекватность принимаемых решений и координировать реализацию мер контроля ИБ;
- Повышать профессиональный уровень пользователей за счет обучения, подготовке по ИБ и осведомленности о ней;
- Оценивать информацию, полученную от мониторинга и просмотра инцидентов по ИБ и рекомендовать соответствующие мероприятия в ответ на идентифицированные инциденты ИБ.

10. Обучение и осведомленность в вопросах ИБ

Требования к обучению и осведомленности в вопросах ИБ:

- Пользователи и администраторы МИС «НАДЕЖДА», должны быть ознакомлены с политикой ИБ;
- Ответственный за ИБ МИС «НАДЕЖДА» по запросу пользователей МИС «НАДЕЖДА» должен проводить первичный инструктаж по ИБ;
- Администратор МИС «НАДЕЖДА», обеспечивающий функционирование МИС «НАДЕЖДА» должен проходить регулярный инструктаж по соблюдению ИБ;
- В целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьей стороной мероприятия по управлению МИС «НАДЕЖДА»;
- Ответственный за ИБ по мере необходимости проходит курсы по повышению квалификации по информационной безопасности

- В целях обеспечения гарантированного уведомления ответственным за ИБ, всех заинтересованных сторон об инциденте и уязвимости ИБ по отношению к МИС «НАДЕЖДА» должны быть реализованы формальные процедуры по уведомлению об инциденте и проявлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры по сохранению ИБ;
- Ответственный за ИБ МИС «НАДЕЖДА» должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, о наступлении которых или предпосылках к таковым необходимо отправить уведомление;
- Администраторы МИС «НАДЕЖДА» обязаны как можно быстрее сообщать о любых событиях в сфере ИБ ответственному лицу по ИБ;
- Ответственные лица ИБ должны вести мониторинг посещения серверного помещения сотрудниками технической поддержки.

11. Управление инцидентами

В случае обнаружения нарушения информационной безопасности следует незамедлительно доложить ответственному по информационной безопасности.

Все сотрудники, подрядчики и пользователи, пользующиеся МИС «НАДЕЖДА» обязаны незамедлительно доложить ответственному по информационной безопасности и по возможности обеспечить минимизацию ущерба.

В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях».

12. Управление непрерывностью бизнеса

13.

- Необходимо внедрить процесс управления непрерывностью бизнеса с целью минимизации влияния на деятельность ИП «PROFIT» и восстановления после потери информационных активов (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования, и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью. Этот процесс должен идентифицировать важные бизнес-процессы и интегрировать требования непрерывности бизнеса управления информационной безопасностью с другими требованиями непрерывности

касательно таких аспектов, как операции, кадровое обеспечение, материалы, транспорт и оборудование.

- Последствия бедствий, нарушений безопасности, отказов в обслуживании и доступность сервисов должны быть предметом анализа степени влияния на бизнес. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью возобновления важных операций в течение требуемого времени при их нарушении. Информационная безопасность должна быть составной частью общего процесса непрерывности бизнеса, и других процессов управления в организации.
- Необходимо, чтобы обеспечение управления непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, в дополнение к общему процессу оценки степени риска, ограничения последствий разрушительных инцидентов, и обеспечения доступности информации, требуемой для процессов бизнеса.
- Необходимо разработать и поддерживать управляемый процесс непрерывности бизнеса для всей организации, который соответствует требованиям информационной безопасности, необходимым для обеспечения непрерывности бизнеса.
- В процессе должны быть собраны вместе следующие ключевые элементы управления непрерывности бизнеса:
- Понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов;
- Определение всех активов, задействованных в критических бизнес-процессах;
- Понимание возможных последствий нарушения бизнес-процессов, вызванных инцидентами нарушения информационной безопасности, в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации, соответствующих к целям бизнеса;
- Организация оптимального страхования результатов обработки информации, которое может быть частью общего процесса непрерывности бизнеса, а также частью управления операционным риском;
- Определение и рассмотрение вопроса реализации дополнительных превентивных и подавляющих средств контроля;
- Идентификация достаточных финансовых, организационных, технических ресурсов и ресурсов окружающей среды для соответствия идентифицированным требованиям информационной безопасности;
- Обеспечение безопасности персонала и защиты средств обработки информации и собственности организации;

- Формулирование и документирование планов обеспечения непрерывности бизнеса, удовлетворяющих требования информационной безопасности в соответствии с согласованной стратегией;
- Регулярное тестирование и обновление планов развития информационных технологий и существующих процессов;
- Обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса.
-

14. Анализ и оценка рисков

Требования к анализу и оценке рисков:

- Политика ИБ МИС «НАДЕЖДА» первоначально должна основываться на данных, полученных в результате анализа и оценки рисков ИБ;
- С целью совершенствования политики информационной безопасности МИС «НАДЕЖДА», должен проводиться ежегодный анализ, и оценка рисков информационной безопасности для МИС «НАДЕЖДА»;
- Анализ и оценка рисков должна проводиться в соответствии со стандартами, действующими на территории Республики Казахстан;
- При оценке рисков должно учитываться влияние реализации угроз ИБ на финансовое состояние. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз;
-

15. Пересмотр политики ИБ

Политика ИБ должна иметь владельца, который утвердил административную ответственность за развитие, пересмотр и оценку политики безопасности. Пересмотр должен включать возможности оценки для улучшения политики ИБ и подход к управлению ИБ в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

При пересмотре политики ИБ необходимо учитывать результаты пересмотров управления ИБ. Здесь должны быть определены процедуры пересмотра, включая график или продолжительности пересмотра.

Входные данные для пересмотра управления должны включать информацию по:

- Обратной связи от заинтересованных сторон;
- Результатам независимых пересмотров;
- Статусу превентивных и корректирующих;
- Результатам предыдущих пересмотров;
- Характеристикам процесса и соответствию политики безопасности информации;
- Изменениям, которые могут повлиять на подход организации к управлению ИБ, включая изменения в организационной среде, деловой ситуации,

наличии ресурсов, договорных, регулятивных или юридических условиях или в технической среде;

- Тенденции, связанные с угрозами и уязвимостями;
- Сообщенным инцидентам с информационной безопасностью;
- Рекомендациям, представленным соответствующими учреждениями.

Выходные данные из пересмотра управления должны включать любые решения и действия, связанные с:

- Усовершенствованием подхода организации к управлению информационной безопасностью и его процессами;
- Усовершенствованием целей и мер контроля;
- Улучшением распределения ресурсов и/или обязанностей.

Пересмотр управления ИБ необходимо регистрировать.

Политика ИБ МИС «НАДЕЖДА» должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности, адекватности и эффективности.

Пересмотренная политика должна утверждаться руководством.

16. Ответственность и контроль эффективности политики информационной безопасности

Для обеспечения необходимого уровня информационной безопасности необходимо производить постоянный контроль эффективности.

Руководство несет ответственность за выполнение всех пунктов данной политики.

Ответственность за контроль эффективности несут должностные лица ответственные за информационную безопасность.

Планирование и контроль состояния информационной безопасности в МИС «НАДЕЖДА» несет Ответственный за ИБ.

В случае нарушения требований настоящей Политики ИБ все субъекты МИС «НАДЕЖДА» привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	2	3	4	5

АТТЕСТАТ № 258.2017.219
соответствия объекта аттестации требованиям информационной безопасности

«Медицинская информационная система «Надежда»
(наименование объекта аттестации)

Индивидуальный предприниматель «PROFIT»
(наименование собственника/владельца)

Настоящим Аттестатом удостоверяется, что *«Медицинская информационная система «Надежда» ИП «PROFIT»* соответствует требованиям информационной безопасности, стандартам в области информационной безопасности. Состав комплекса программных и технических средств информационной системы прилагается к аттестату согласно приложению.
(наименование объекта аттестации)

С учетом результатов аттестационного обследования на объекте аттестации разрешается обработка *информации ограниченного доступа*.
(служебная, общедоступная и т.п.)

При эксплуатации объекта аттестации запрещается: *изменение состава и конфигурации компонентов, обеспечивающих обработку защищаемой информации, определяющих безопасность информации в ИС.*
(ограничения, которые могут повлиять на эффективность мер и средств защиты информации)

Контроль за эффективностью реализованных мер и средств защиты возлагается на соответствующие подразделения заявителя.

Подробные результаты аттестационного обследования приведены в акте аттестационного обследования *(№ 258.2017.А.372 от 24 ноября 2017 года)*.

Настоящий аттестат соответствия объекта аттестации требованиям информационной безопасности выдан на *срок промышленной эксплуатации объекта аттестации*, в течение которого должна быть обеспечена неизменность условий функционирования и функциональности объекта аттестации.
(срок действия аттестата)

Перечень характеристик информационной системы на момент аттестационного обследования указан в приложении к настоящему аттестату.

Председатель **А. Кожихов**
(Ф.И.О.)

М.П. «__» _____ 20__ г.

000241