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

Политика информационной безопасности МИС «Надежда»

1. Термины и определения

Авторизация - предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация - проверка устанавливающая подлинность лица, получающего доступ к системе, путем сопоставления идентификатора и предъявленного фактора.

Безопасность информации – состояние защищенности данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность при их обработке в информационных системах.

*Доступность информаци*и - обеспечение возможности доступа авторизованным пользователям к информационным ресурсам автоматизированной информационной системы в нужное время.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Инцидент – событие, являющееся следствием одного или нескольких нежелательных, или неожиданных событий, имеющих вероятность компрометации бизнес-операции и создания угроз в ИБ.

Информационная безопасность - комплекс административно-правовых, организационно-распорядительных и технических мер, направленные на обеспечение конфиденциальности, целостности и доступность информации в процессе ее сбора, обработки, передачи и хранения.

Информационная система – системы, предназначенные для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Защита информации – информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами к коммерческой, служебной или иной охраняемой законом.

Конфиденциальность- предотвращение разглашения секретной информации третьим лицам.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь – лицо или организация, использующая действующую систему для выполнения конкретных функций.

Угроза - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным или данным системы, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе.

Уязвимость – слабость в информационной системе, которую можно использовать для нарушения системы или содержащейся в ней информации приводящая к реализации угрозы.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Список использованных сокращений и определений

ИБ	Информационная безопасность
ИС	Информационная система
МИС	Медицинская информационная система
НСД	Несанкционированный доступ
ПО	Программное обеспечение

2. Назначение документа

Настоящая Политика информационной безопасности далее (Политика) разработана с целью предоставления высокоуровневых задач и требований обеспечения информационной безопасности, применяемых в медицинской информационной системе «Надежда» (далее – МИС «Надежда»). Разработчиком и Владельцем МИС «Надежда» является Компания ИП «PROFIT» (далее – Компания)

Обеспечение информационной безопасности- необходимое условие для успешного осуществления деятельности МИС «Надежда».

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.

Внедрение информационной безопасности позволяет снизить риски и экономические потери, связанные с угрозами информационных ресурсов МИС «Надежда».

Политика разработана на основании стандарта ИСО/МЭК 27001:2008 «Методы и средства обеспечения безопасности системы управления информационной безопасностью» и нормативно правовых документов, устанавливающих требования и меры обеспечения ИБ.

Работники, и другие лица, допущенные к информационным ресурсам МИС «Надежда», несут ответственность за рациональное использование и соблюдение требований настоящей Политики. Доступ к информационным ресурсам МИС «Надежда» предоставляется, только после ознакомления с настоящей Политикой и подписания обязательств о неразглашении сведений, документов, составляющих защищаемую информацию.

Положение настоящего документа относится ко всем штатным и временным работникам, имеющих доступ к информационной системе. Ответственность за соблюдение информационной безопасности несет каждый работник и пользователь МИС «Надежда». Политика ИБ распространяется на функционирование МИС «Надежда» в целом и обязательна для исполнения всеми пользователями, работающими в МИС «Надежда»

3. Цели и задачи обеспечения ИБ

Цель настоящей Политики является обеспечение безопасности от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных, а также повышение общего уровня конфиденциальности, целостности, доступности, непрерывности, осведомленности и повышения уровня эффективности, контролируемости мер защиты информации в МИС «Надежда».

Для достижения основных целей, ИС должна обеспечивать эффективное решение следующих задач:

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

– защита от вмешательства в процессе функционирования МИС персональных данных посторонних лиц (использования системы и доступ к ее ресурсам должны иметь только зарегистрированные установленные порядком пользователи);

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

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

– разработка нормативных документов для обеспечения ИБ МИС «Надежда»;

– защита информации от НСД и утечки по техническим каналам связи;

– создание механизма и условий оперативного мониторинга и реагирования на нарушения.

4. Основные принципы обеспечения информационной безопасности

Основным принципом обеспечения ИБ является защита МИС «Надежда». Для предотвращения угроз и инцидентов в информационной системе были определены основные принципы защиты обеспечения ИБ:

– защита от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного

несанкционированного вмешательства в процесс функционирования или НСД к циркулирующей в ней информации и ее незаконного использования;

– постоянный мониторинг и анализ автоматизированных систем и трудового процесса с целью выявления уязвимостей и предотвращения угроз в МИС «Надежда»;

– распределение ролей и обязанностей между сотрудниками и пользователями МИС «Надежда» для обеспечения ИБ и выявления ответственности за совершаемые операции;

– прогнозирование и выявление уязвимостей, способствующих повлиять на ИБ МИС «Надежда»;

– своевременный анализ и оценка рисков в ИС МИС «Надежда»;

– разработка и внедрение мер по защите ИБ.

Обеспечение защиты МИС «Надежда» достигается посредством постоянного поддержания целостности и аутентичности хранимой и обрабатываемой информации, доступности обрабатываемой информации и обеспечения конфиденциальности информации, хранимой и обрабатываемой средствами вычислительной техники, передаваемой по каналам связи.

Для обеспечения указанных свойств необходимо обеспечить 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 НСД 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, 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.

5. Координация вопросов в информационной безопасности

Действия по обеспечению ИБ должны координироваться руководством Компании в соответствии с их компетенцией и должностным положением.

Координация ИБ поддерживает взаимосвязь и сотрудничество между пользователями, администратором, разработчиками прикладного программного обеспечения и квалифицированных специалистов регулирующие вопросы по обеспечению ИБ в МИС «Надежда»

Основными задачами по координации и обеспечению ИБ являются:

– определение конкретных функций и обязанностей в области ИБ;

– согласование методик и процедур по обеспечению ИБ, такие как оценка рисков, классификация информации с точки зрения требований безопасности;

– определение мероприятий по обеспечению ИБ в случае её несоответствия политике ИБ;

– выявление изменений угроз ИБ, степень уязвимости и средств обработки информации к угрозам ИБ;

– координирование применяемых решений по реализации мер контроля ИБ;

– повышение профессионального уровня пользователей за счет обучения, подготовке по ИБ и осведомленности о ней;

– оценка информации, полученная от мониторинга и просмотра инцидентов по ИБ и рекомендации соответствующих мероприятий в ответ на идентифицированные инциденты ИБ;

– выполнение соответствующих мероприятий по обеспечению ИБ и Политике ИБ.

6. Управление инцидентами

В случае обнаружения нарушений Политики информационной безопасности следует незамедлительно доложить ответственному по информационной безопасности МИС «Надежда».

Сотрудники, подрядчики и пользователи МИС «Надежда» обязаны незамедлительно доложить ответственному по информационной безопасности и по возможности обеспечить минимизацию ущерба.

Ответственному по информационной безопасности МИС «Надежда» при аварийной ситуации необходимо руководствоваться внутренними нормативными документами, регламентирующие правила по устранению нарушений.

В МИС «Надежда» должны быть установлены меры дисциплинарной ответственности сотрудников, нарушающих требования безопасности. Для того чтобы иметь возможность реагировать на инциденты нарушения информационной безопасности должным образом, необходимо собирать свидетельства и доказательства незамедлительно после обнаружения инцидента.

7. Управление непрерывностью бизнеса

Основной целью управления непрерывностью работы МИС «Надежда» является противодействие прерывания работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

ИБ МИС «Надежда» должна быть встроена в систему непрерывности бизнеса компании. Для этого необходимо:

– Внедрить процесс управления непрерывностью бизнеса с целью минимизации влияния на деятельность Компании и восстановления после потери информационных активов (которые могут быть результатом отказов оборудования, несчастных случаев, и преднамеренных не преднамеренных действий сотрудников и стихийных бедствий) 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 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. ИБ 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.

Организация должна поддерживать и постоянно улучшать систему управления непрерывности бизнеса, включая необходимые процессы и их взаимодействия, в соответствии с установленными требованиями.

8. Анализ и оценка рисков

Основной целью анализа и оценки рисков является предоставление отчета на основе объективных свидетельств информации, необходимых для принятия обоснованного решения относительно способов обработки 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.

9. Обучение и осведомленность в вопросах ИБ

Все сотрудники должны проходить периодический инструктаж в области Политики и процедур ИБ, принятых в МИС «Надежда».

Основной целью обучения сотрудников и пользователей МИС «Надежда» является, обеспечение уверенности в компетентности сотрудников и пользователей об угрозах и проблемах, связанных с ИБ, об ответственности в соответствии с законодательством.

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 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.

10. Распределение обязанностей по обеспечению ИБ

Руководство Компании обязано активно осуществлять комплекс мероприятий по поддержанию МИС «Надежда» посредством дачи ясных указаний, демонстрированных обязательств, четких постановок задач и осведомленности работников об обязанностях по обеспечению ИБ.

Руководство обязано обеспечить:

– формирование и контроль выполнения всех пунктов данной политики;

– пересмотр эффективность реализации политики ИБ;

– четкое управление и зримую поддержку инициатив в области поддержки Системы;

– обеспечить координацию мер контроля за ИБ в МИС «Надежда»;

– предоставить ресурсы для обеспечения ИБ;

– утверждать распределение специфических ролей и обязанностей по ИБ;

– 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».

11. 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, регулярно проводит собрания, посвящённые проблемам обеспечения ИБ с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

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

Планирование и контроль состояния ИБ в МИС «Надежда» несет Ответственный за обеспечение 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.

12. Удаленный доступ

Управление удаленным доступом МИС «Надежда» определяет перечень правил:

Сотрудники получают право удаленного доступа к информационным ресурсам организации только для выполнения должностных обязанностей в МИС «Надежда».

Сотрудники, использующие в работе портативные компьютеры организации, может быть предоставлен удаленный доступ к сетевым

ресурсам организации в соответствии с правами доступа к корпоративной информационной системе.

Сотрудникам, работающим за пределами организации с использованием компьютера, не принадлежащего организации, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети организации, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

13. Пересмотр политики информационной безопасности

Пересмотр политики ИБ производится не реже одного раза в три года и имеет целью проведения определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации. 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.

14. Список источников

Настоящий документ разработан в соответствии со следующими нормативно-правовыми 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».

– Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 27001:2013 «Методы обеспечения безопасности. Системы менеджмента информационной безопасности»

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