Утверждена
Решением Правления
НАО «Фонд социального
медицинского страхования»
«23» апреля
2021 г. (протокол № 13)

Политика информационной безопасности НАО «Фонд социального медицинского страхования»

Нур-Султан, 2021 год

Содержание

1. Общие положения

1. Политика информационной безопасности (далее – ПИБ) НАО «Фонд социального медицинского страхования» (далее – Фонд) является документом первого уровня, определяющим цели, задачи, руководящие принципы и практические приемы в области обеспечения информационной безопасности (далее – ИБ).

2. Настоящая Политика разработана в соответствии с:

1) Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации»;

2) Едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденными постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее – Единые требования);

3) серией международных стандартов по информационной безопасности ISO/IEC 27000, COBIT, ITIL, современным состоянием и ближайшими перспективами развития информационной инфраструктуры Фонда, а также возможности современных организационно-технических методов защиты информации.

3. Положения ПИБ обязательны для исполнения всеми работниками Фонда, стажерами, практикантами, а также должны доводиться до сведения иных третьих лиц, имеющих доступ к информационным системам и документам Фонда, в той их части, которая непосредственно взаимосвязана с Фондом и их деятельностью.

4. ПИБ охватывает все информационные системы и документы, владельцем и пользователем которых является Фонд.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Фонда. Информация является одним из важнейших активов Фонда.

5. ИБ Фонда – это состояние устойчивости (защиты) его информационных активов к случайным или преднамеренным воздействиям, которые могут привести к материальному ущербу, нанести ущерб репутации Фонда или повлечь нанесение иного ущерба Фонда, работникам или клиентам.

6. Требования ИБ, которые предъявляются Фондом, соответствуют Стратегии развития НАО «Фонд социального медицинского страхования» на 2020 – 2025 годы (далее - Стратегия Фонда) и предназначены для снижения рисков, связанных с ИБ, до приемлемого уровня. Наличие рисков в сфере ИБ Фонда имеют отношение к ее корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Наличие рисков в сфере ИБ Фонда составляют часть операционных рисков Фонда, тем самым влияющих на основную деятельность Фонда.

7. Руководство Фонда стремится обеспечить эффективную и стабильную

работу Фонда, а также поддержать уверенность всех заинтересованных сторон в надежности и стабильности работы Фонда, в защищенности их интересов от воздействия различных неблагоприятных факторов.

8. Руководство осознает, что ИБ является одним из критичных факторов успешной и стабильной работы Фонда и намерено оказывать необходимое содействие и демонстрировать приверженность целям и принципам обеспечения ИБ. Руководство Фонда также оставляет за собой общий контроль за процессом управления ИБ.

2. Цель и задачи политики информационной безопасности

9. Основные цели построения и совершенствования ПИБ:

1) обеспечение надлежащей защиты информации в зависимости от ее значения для Фонда;

2) обеспечение конфиденциальности, подлинности, целостности информации, защита персональных данных;

3) предотвращение несанкционированного физического доступа, повреждения и вмешательства в информацию и в средства обработки информации Фонда;

4) обеспечение информационной безопасности как неотъемлемой части информационных систем в течение всего их жизненного цикла;

5) обеспечение бесперебойного и результативного подхода к управлению инцидентами информационной безопасности, включая сообщения о событиях безопасности и слабые стороны.

10. В целях успешной реализации Политики необходимо успешное выполнение следующих задач:

1) инвентаризация и классификация информационных активов Фонда;

2) определение рисков ИБ и потенциальных возможностей данных рисков;

3) определение и документирование основных требований и процедур обеспечения ИБ;

4) внедрение и настройка средств защиты информации;

5) обучение персонала Фонда в области ИБ;

6) своевременное выявление и устранение уязвимостей активов Фонда и тем самым предупреждение возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов Фонда в результате реализации угроз ИБ;

7) уменьшение до приемлемого уровня возможного ущерба Фонда при реализации угроз ИБ, в том числе сокращение времени восстановления бизнес-процессов после возможных прерываний;

8) мониторинг и обработка событий и инцидентов ИБ;

9) планирование и оптимизация затрат на обеспечение информационной

безопасности Фонда.

11. Планирование, реализация и контроль комплекса организационных и технических мер по обеспечению ИБ на основе оценки рисков Фонда в сфере информационных технологий (далее - ИТ), направленных на:

1) обеспечение непрерывной доступности информационных активов Фонда для поддержки его бизнес-процессов;

2) обеспечение целостности информационных активов Фонда в целях поддержки высокого качества бизнес-процессов;

3) обеспечение конфиденциальности подлинности, целостности информации, защита персональных данных;

4) обеспечение соответствия предпринимаемых мер по информационной безопасности, применяемых в Фонде, требованиям законодательства, а также требованиям регулирующих и надзорных организаций.

12. Объектами, подлежащими защите, являются:

1) информационные активы, необходимые для работы Фонда, независимо от формы и вида их представления;

2) информационные системы, включая информационные технологии, технические и программные средства формирования, обработки, передачи, хранения (в том числе архивированные) и использования информации,

3) элементы ИТ-инфраструктуры, включая компьютерную технику, библиотеки, архивы, базы данных, сервера, включая физические и виртуальные в центральном аппарате и филиалах, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены защищаемые элементы ИТ-инфраструктуры Фонда;

4) структурные подразделения Фонда, включая центральный аппарат и филиалы,

5) процессы, регламенты и процедуры обработки информации в Фонде;

6) персональные данные работников и рекизиты поставщиков Фонда.

13. Фонду принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством Республики Казахстан. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Фонда, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Фонда.

3. Руководящие принципы обеспечения информационной безопасности

14. Настоящая Политика основывается на принципах:

1) обеспечения ИБ путем сохранения конфиденциальности, целостности и доступности информации;

2) конфиденциальности путем предоставления доступа к информации только авторизованным лицам;

3) целостности путем внесения исключительно авторизованных изменений в общедоступные электронные информационные ресурсы (данные находящиеся на персональных компьютерах, в корпоративной электронной почте, СЭД и т.д.)

4) доступности путем предоставления авторизованным лицам доступа в общедоступные электронные информационные ресурсы (данные находящиеся на персональных компьютерах, в корпоративной электронной почте, СЭД и т.д.) для выполнения их служебных обязанностей.

4. Практические приемы обеспечения информационной безопасности

15. Общее руководство в вопросах ИБ Фонда осуществляет руководство Фонда, в обязанности которого в контексте ИБ входит:

1) обеспечение целей ИБ в соответствии с законодательством Республики Казахстан в области информационно-коммуникационных технологий и информационной безопасности их в соответствующих процессах;

2) утверждение ПИБ;

3) осуществление координации внедрения мероприятий по управлению ИБ в Фонде;

4) обеспечение четкого управления и реальной поддержки инициатив в области ИБ;

5) выделение необходимых ресурсов для обеспечения ИБ;

6) утверждение распределения основных обязанностей и функций в отношении ИБ;

16. В целях разграничения ответственности и функций в сфере обеспечения ИБ создается подразделение ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определяется должностное лицо, ответственное за обеспечение ИБ, которые осуществляют:

1) контроль исполнения требований технической документации по ИБ;

2) контроль за документальным оформлением ИБ;

3) контроль за управлением активами в части обеспечения ИБ;

4) контроль правомерности использования ПО;

5) контроль за управлением рисками в области ИБ;
6) контроль за регистрацией событий ИБ;
7) проведение внутреннего аудита ИБ;
8) контроль за организацией внешнего аудита ИБ;
9) контроль за обеспечением непрерывности бизнес-процессов, использующих ИКТ;
10) контроль соблюдения требований ИБ при управлении персоналом;

5. Заключительные положения

17. Руководство Фонда, его филиалов несет ответственность за деятельность по обеспечению ИБ, декларирует свою приверженность вышеуказанным целям и принципам.

18. Работники Фонда, его филиалов несут ответственность за соблюдение требований ПИБ и должны своевременно сообщать обо всех выявленных нарушениях в области ИБ.

19. Пересмотр положений настоящей Политики осуществляется на регулярной основе, но не реже одного раза в два года.

20. Внеплановый пересмотр настоящей Политики осуществляется в случае:

1) изменения нормативных правовых актов Республики Казахстан, внутренних документов Фонда, определяющих требования информационной безопасности;

2) выявления снижения общего уровня информационной безопасности Фонда (по результатам внутреннего или внешнего аудита);

3) существенных изменений организационной и/или инфраструктуры, ресурсов и бизнес-процессов Фонда;

4) выявления существенных недостатков при выполнении мероприятий, регламентированных настоящей Политикой, а также противоречий ее положений с другими внутренними документами Фонда.

21. Пересмотр настоящей Политики, а также внесение в нее изменений выполняется в соответствии с порядком, установленным внутренними документами Фонда.