Рег. № 47
от « 22 » мая 2014 г.

Утверждена
протоколом Правления АО «ЕНПФ»
от « 22 » мая 2014 г. № 34

Политика
информационной безопасности АО «ЕНПФ»

Изменения и дополнения, утвержденные протоколом Правления АО «ЕНПФ»:

№	Внесены изменения, дополнения	Дата утверждения протокола	№ протокола	Рег. №
1	Протокол	от «__» _____ 20__ г.	№ _____	Рег. № _____
2	Протокол	от «__» _____ 20__ г.	№ _____	Рег. № _____
3	Протокол	от «__» _____ 20__ г.	№ _____	Рег. № _____
4	Протокол	от «__» _____ 20__ г.	№ _____	Рег. № _____

Признана утратившей силу протоколом Правления АО «ЕНПФ» от «____» _____ 201__ г. № ___

Глава 1. Общие положения

1. Настоящая Политика информационной безопасности АО «ЕНПФ» (далее – Политика) определяет систему взглядов на проблему обеспечения безопасности информации, излагает основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих внутренних документов АО «ЕНПФ» (далее – Фонд).

2. Нормативно-правовую основу Политики составляют положения законодательства Республики Казахстан по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.

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

4. Политика 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. Информационная безопасность Фонда (далее – ИБ) – есть 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 Фонду, его акционерам, работникам или клиентам.

6. Являясь элементом общей политики руководства Фонда, ИБ основывается на требованиях бизнеса, разрабатывается и реализуется в соответствии с общими правилами управления рисками в Фонде. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов.

7. Обеспечение ИБ включает в себя любую деятельность, направленную на защиту информации и поддерживающей ее инфраструктуры.

8. Неотъемлемой частью организации ИБ является непрерывный контроль эффективности предпринимаемых мер, определение для работников перечня недопустимых действий (бездействия), возможных последствий и ответственности.

Глава 2. Цели, требования и основные принципы

9. Основной целью, на достижение которой направлены все положения Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

10. ИБ не является самоцелью, ее обеспечение необходимо для снижения рисков и экономических потерь, связанных со всевозможными угрозами имеющимся информационным ресурсам Фонда. С этой целью необходимо поддерживать главные свойства информации, а именно:

1) доступность – свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия;

2) конфиденциальность – свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

3) целостность – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

11. Процесс создания надежной информационной защиты никогда не бывает законченным. В целях обеспечения достаточно надежной системы ИБ, необходима постоянная регулировка ее параметров, адаптация для отражения новых опасностей, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Политику по мере возникновения такой необходимости.

В соответствии с данным положением, определяются следующие этапы цикла управления ИБ (модель PDCA: Plan-Do-Check-Act):

1) Plan – Планирование (разработка) – анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию ИБ для получения результатов в соответствии с общей стратегией и целями Фонда;

2) Do – Реализация (внедрение и эксплуатация) – внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно-аппаратных средств;

3) Check – Проверка (мониторинг и анализ) – оценка и там, где это применимо, –измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;

4) Act – Корректировка (сопровождение и совершенствование) – принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния ИБ, требований со стороны руководства, иных факторов, в целях обеспечения непрерывного совершенствования системы ИБ.

12. Построение системы обеспечения ИБ Фонда и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1) законность – любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Фонда;

2) ориентированность на бизнес – ИБ рассматривается как процесс поддержки основной деятельности. Любые меры по обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Фонда;

3) непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Фонда должны осуществляться без прерывания или остановки текущих бизнес-процессов Фонда;

4) комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

5) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер и систем ИБ должна быть меньше размера возможного ущерба от любых видов риска;

6) приоритетность – категорирование (ранжирование) всех информационных ресурсов Фонда по степени важности при оценке реальных, а также потенциальных угроз ИБ;

7) необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация – эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными специалистами Фонда;

9) информированность и персональная ответственность – руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;

10) взаимодействие и координация – меры ИБ осуществляются на основе взаимосвязи соответствующих структурных подразделений Фонда, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11) подтверждаемость – важная документация и все записи – документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Глава 3. Объекты защиты, область применения

13. Основными объектами обеспечения ИБ в Фонде признаются следующие элементы:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Фонда к конфиденциальной информации, коммерческой тайне Фонда, любая иная информация, необходимая для обеспечения нормального функционирования Фонда (далее – защищаемая информация);

2) средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы Фонда, с помощью которых производится обработка защищаемой информации;

4) процессы Фонда, связанные с управлением и использованием информационных ресурсов;

5) помещения, в которых расположены средства обработки защищаемой информации;

6) кабинеты работников и помещения Фонда;

7) персонал Фонда, имеющий доступ к защищаемой информации;

8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

14. Подлежащая защите информация может:

1) размещаться на бумажных носителях;

2) существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);

3) передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов.

15. Политика применяется ко всем работникам Фонда, стажерам, практикантам, контрагентам и иным лицам, так или иначе имеющим доступ к информационным ресурсам Фонда или вовлеченным в процессы информационного обмена.

Глава 4. Угрозы информационной безопасности

16. Под угрозами ИБ понимается потенциальная возможность нарушения главных свойств информации.

17. Угрозы ИБ подразделяются на:

1) случайные – стихийные бедствия, ошибки по невниманию, ошибки аппаратных и программных средств и т.д.;

2) преднамеренные, т.е. фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

18. К числу угроз ИБ относятся (но не ограничены ими):

1) утрата информации, составляющих коммерческую тайну Фонда и иную защищаемую информацию;

2) искажение (несанкционированная модификация, подделка) защищаемой информации;

3) утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);

5) недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств и злонамеренных действий.

19. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Фонда и его нормальное функционирование:

1) финансовые потери, связанные с утечкой или разглашением защищаемой информации;

2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3) ущерб от дезорганизации деятельности Фонда и потери, связанные с невозможностью выполнения им своих обязательств;

4) ущерб от принятия управленческих решений на основе необъективной информации;

5) ущерб от отсутствия у руководства Фонда объективной информации;

6) ущерб, нанесенный репутации Фонда;

7) иной вид ущерба.

Глава 5. Модели вероятного нарушителя

20. Нарушители ИБ классифицируются следующим образом:

1) внутренние нарушители – работники Фонда, неосознанно либо злонамеренно нарушающие режим ИБ;

2) внешние нарушители – лица, не связанные с Фондом трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Фонда.

21. Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.

22. Основные типы внутренних нарушителей:

1) «необученный/халатный работник» – работник Фонда, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;

2) «конкурирующий работник» – работник Фонда, по личной неприязни либо по иным причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и в целом Фонд;

3) «заинтересованный нарушитель» – работник Фонда, который заинтересован в неправомерных действиях по отношении к Фонду третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Фондом трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение – утечка информации (в случае заинтересованности собственной выгодой – финансовые мошенничества);

4) «внедренный злоумышленник» – работник Фонда, поступивший на работу с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Фондом;

5) «увольняющийся работник» – работник Фонда, прекращающий с ним трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел непосредственный доступ;

6) «обиженный работник» – работник Фонда, резко неудовлетворенный параметрами трудовой деятельности либо, как вариант, руководство Фонда явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений.

23. Основные типы внешних нарушителей (в данном разделе используется терминология, принятая на настоящий момент в сообществе специалистов по ИБ):

1) «Начинающий» – лицо, интересующееся взломом любого информационного ресурса, имеющего общеизвестные уязвимости. Не нацелен на взлом информационных ресурсов именно Фонда, легко прекращает атаку в случае обнаружения серьезных средств защиты. Как правило, использует широко распространенные методы взлома, не разрабатывает собственных средств;

2) «Черный хакер» – в отличие от «Начинающего» более упорен во взломе конкретного ресурса, обход систем защиты считает «делом чести», может разрабатывать простые атакующие средства. Действует с целью самоутверждения или для извлечения личной выгоды, может продавать свои услуги криминальным структурам;

3) «Гуру» – высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае

будет нацелен на проведение финансового мошенничества, во втором – либо на утечку информации, либо на недоступность серверов и компрометацию Фонда в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;

4) «Партнер» – работник организации-партнера либо дочерней организации, имеющих доступ к информационным системам Фонда. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях ИБ, принятых в Фонде;

5) «Консультант» – работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;

6) «Стажер/практикант» – как правило, ограничен в доступе к информации и информационным системам, однако постоянно находится на территории Фонда и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Фонда, курирующего данного стажера/практиканта;

7) «Клиент» – клиент Фонда, имеющий доступ к его сервисам дистанционного обслуживания. Может нанести урон при неправильном использовании данных сервисов, утере идентификационных данных либо действовать как первые три типа внешних нарушителей, имея – пусть и ограниченный – доступ к информационным ресурсам.

Глава 6. Меры по обеспечению информационной безопасности

24. Основными мерами по обеспечению ИБ Фонда являются:

1) административно-правовые и организационные меры;

2) меры физической безопасности;

3) программно-технические меры.

25. Административно-правовые и организационные меры включают (но не ограничены ими):

1) контроль исполнения требований законодательства РК и внутренних документов;

2) разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;

3) контроль соответствия бизнес-процессов требованиям Политики;

4) информирование и обучение работников Фонда работе с информационными системами и требованиям ИБ;

5) реагирование на инциденты, локализацию и минимизацию последствий;

6) анализ новых рисков ИБ;

7) отслеживание и улучшение морально-делового климата в коллективе;

8) определение действий при возникновении чрезвычайных ситуаций;

9) проведение профилактических мер при приеме на работу и увольнении работников Фонда.

26. Меры физической безопасности включают (но не ограничены ими):

1) организацию пропускного и внутриобъектового режимов;

2) построение периметра безопасности защищаемых объектов;

3) организацию круглосуточной охраны охраняемых объектов, в том числе с использованием технических средств безопасности;

4) организацию противопожарной безопасности охраняемых объектов;

5) контроль доступа работников Фонда в помещения ограниченного доступа.

27. Программно-технические меры включают (но не ограничены ими):

1) использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

2) использование средств защиты периметра (firewall, Data Loss Prevention (DLP) и т.п.);

3) применение комплексной антивирусной защиты;

4) использование средств ИБ, встроенных в информационные системы;

5) использование специальных комплексов ИБ (как защита электронных информационных ресурсов, так и защита от утечки по электромагнитным и акустическим каналам);

6) обеспечение регулярного резервного копирования информации;

7) контроль за правами и действиями пользователей, в первую очередь, имеющих расширенные права доступа;

8) применение систем криптографической защиты информации;

9) обеспечение безотказной работы аппаратных средств;

10) мониторинг состояния критичных элементов информационной системы.

Глава 7. Разделение полномочий и ответственности

28. Основным принципом построения системы ИБ является то, что за успешную реализацию Политики ИБ отвечает каждый работник Фонда.

29. Руководство Фонда:

1) осуществляет стратегическое планирование;

2) утверждает нормативные документы;

3) определяет полномочия и ответственность подразделений в области ИБ;

4) координирует деятельность всех подразделений для организации и поддержания соответствующего уровня ИБ деятельности Фонда;

5) выделяет достаточные ресурсы для разработки, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования системы ИБ;

6) принимает решения о критериях принятия рисков и допустимом уровне риска;

7) обеспечивает проведение внешних и внутренних проверок состояния ИБ;

8) проводит ежегодный анализ состояния ИБ через департамент безопасности;

9) отвечает за общее состояние ИБ.

30. Департамент безопасности:

1) рассматривает стратегию развития ИБ в Фонде, а также проекты годовых бюджетов по обеспечению ИБ Фонда, осуществляет мониторинг развития и внедрения программно-технических решений по ИБ Фонда, внедряет организационные меры по ИБ Фонда, осуществляет отказ от действующих проектов по ИБ, потерявших свою актуальность;

2) осуществляет, при необходимости, промежуточный контроль реализации проектов по отчетам, предоставляемым руководителями проектов, а также вносит рекомендации руководству Фонда о поощрении работников за успешную реализацию проектов и привлечении к дисциплинарной ответственности за невыполнение решений департамента безопасности или срыв сроков выполнения проектов;

3) рассматривает и утверждает итоговые отчеты, касающиеся ИБ;

4) рассматривает отчеты по крупным инцидентам в области ИБ;

5) анализирует, вырабатывает и, при необходимости, дает на будущее рекомендации, направленные на избежание возникновения инцидентов ИБ;

6) рассматривает предложения структурных подразделений Фонда по изменению их организационной структуры, связанному с проектами в области ИБ. По результатам вносит предложения на рассмотрение руководства Фонда в установленном порядке;

7) реализует решения руководства Фонда, осуществляет общую организацию системы обеспечения ИБ, координирует и контролирует деятельность всех подразделений Фонда в сфере ИБ;

8) осуществляет методологическую поддержку процесса управления и обеспечения ИБ Фонда;

9) обеспечивает выбор средств и механизмов контроля, управления и обеспечения ИБ Фонда;

10) обеспечивает штатное функционирование комплекса средств ИБ Фонда;

11) организует процесс анализа и оценки угроз в области ИБ Фонда;

12) контролирует соблюдение требований ИБ всеми участниками информационного обмена;

13) совместно с департаментом поддержки пенсионных услуг и внутренних связей обеспечивает процесс обучения новых и действующих работников с первичными требованиями ИБ;

14) обеспечивает мониторинг состояния ИБ Фонда;

15) проводит обработку событий и инцидентов, связанных с нарушениями ИБ, подготавливает соответствующие заключения и рекомендации;

16) информирует руководство Фонда о состоянии системы обеспечения ИБ;

17) информирует департамент управления рисками о событиях и инцидентах в области ИБ Фонда в соответствии с принятыми в Фонде требованиями;

18) реализует меры физической и технической безопасности;

19) проводит профилактические меры при приеме на работу и увольнении работников Фонда.

31. Департамент управления рисками:

1) участвует в процессе оценки рисков ИБ;

2) организует систему регистрации событии и инцидентов, связанных с нарушениями ИБ в специализированной базе событий операционных рисков;

3) участвует в процессе анализа событий и инцидентов в области ИБ;

4) осуществляет методологическую поддержку процесса анализа и оценки рисков;

5) в рамках функционирования инструментов операционного риск-менеджмента совместно с Департаментом безопасности участвует в процессе идентификации и оценки рисков ИБ, а также принимает участие в постановке задач по минимизации данных рисков

32. Департамент информационных технологий:

1) обеспечивают предоставление доступа пользователям к информационным ресурсам Фонда в соответствии с принятыми в Фонде требованиями;

2) конфигурируют системное и прикладное программное обеспечение в соответствии с принятыми в Фонде требованиями;

3) обеспечивают непрерывное функционирование, целостность и доступность (включая архивирование и резервное копирование информации) информационных ресурсов Фонда, конфиденциальность обрабатываемой в них информации (администрирование встроенных механизмов безопасности).

33. Управление человеческих ресурсов:

1) осуществляет обязательный комплекс мероприятий по сбору первичных документов при приеме кандидатов на работу и подписанию с работниками Фонда, а также лицами, привлеченными на работу по договору, стажерами, практикантами соответствующих соглашений (трудовых договоров, договоров о прохождении стажировки, договоров подряда или возмездного оказания услуг, обязательств о неразглашении служебной, коммерческой тайны и т.д.);

2) по указаниям руководства Фонда обеспечивает наложение на работников Фонда дисциплинарных взысканий в случае нарушения Политики и правил ИБ.

34. Юридический департамент отвечает за соответствие внедряемых процессов, нормативных документов в области ИБ нормативным правовым актам (требованиям законодательства РК) при их согласовании.

35. Структурные подразделения Фонда:

1) отвечают за соблюдение требований ИБ при внедрении, модификации, предоставлении клиентам продуктов и услуг;

2) согласовывают права доступа к информационным системам/процессам, бизнес-владельцами которых они являются.

36. Руководители структурных подразделений Фонда:

1) обеспечивают ознакомление работников с текущими требованиями ИБ;

2) отвечают за обеспечение ИБ в подчиненных подразделениях.

37. Пользователи информационной системы:

1) отвечают за соблюдение требований настоящей Политики, а также иных внутренних нормативных документов по обеспечению безопасной работы в информационной системе;

2) контролируют исполнение требований ИБ, изложенных в настоящей Политике и других внутренних документах Фонда, третьими лицами, с которыми они контактируют в рамках своих должностных обязанностей, в том числе путем включения указанных требований в договоры с третьими лицами;

3) обязаны извещать непосредственного руководителя и подразделение информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными ресурсами.

Глава 8. Соответствие требованиям

38. Настоящая Политика и система ИБ в целом опираются на следующие нормативные правовые акты и международные стандарты (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы ИБ Фонда в целом; в то же время существует ряд документов, который либо описывает стратегические аспекты развития ИБ на государственном уровне, либо регламентирует правила по информационной защите отдельных приложений/ услуг):

1) Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;

2) Международный стандарт ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования» (СТ РК ИСО/МЭК 27001-2008);

3) Закон Республики Казахстан от 21 июня 2013 года № 105-V «О пенсионном обеспечении в Республике Казахстан»

4) Постановлением НБРК от 27 августа 2013 №240 «Правила формирования системы управления рисками и внутреннего контроля для единого накопительного фонда и добровольных накопительных фондов»

39. В Фонде должны быть внедрены соответствующие процессы для обеспечения соблюдения требований нормативных правовых актов, соблюдения прав интеллектуальной собственности, защиты охраняемой законом персональной информации, соблюдения ограничений по использованию криптографических средств.

40. Все требования и положения международного стандарта ISO/IEC 27001 являются обязательными для исполнения в области их применения, определяемой соответствующими документами.

41. При разработке и применении средств и методов ИБ должны учитываться требования договорных обязательств и контрактов, заключенных Фондом с третьими сторонами.

42. Положения настоящей Политики, законодательства Республики Казахстан в сфере информационной безопасности и международных стандартов ISO/IEC 27001 должны содержаться в должностных инструкциях работников Фонда, задействованных в реализации требований данных стандартов и в договорах на выполнение работ/ предоставление услуг, заключаемых со сторонними организациями и физическими лицами, задействованными в обслуживании и эксплуатации систем, на которые распространяется действие данных нормативных документов и стандартов. Доступ третьей стороны к информационным ресурсам Фонда осуществляется только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер.

43. В случае необходимости (в частности, при наличии требований нормативных правовых актов или международных стандартов), Фонд проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям.

44. На основании Политики разрабатывается ряд подчиненных внутренних нормативных документов, регламентирующих конкретные правила и методы обеспечения ИБ, частные политики в области действия стандартов и т.п. Указанные документы могут дополнять и расширять требования Политики, но не могут вступать с ними в противоречие.

Глава 9. Анализ и пересмотр

45. Анализ и оценка настоящей Политики, подчиненных документов, информационных систем и системы ИБ в целом производится как минимум ежегодно на основании результатов следующих мероприятий:

1) анализ состояния и эффективности системы ИБ руководством Фонда;

2) текущие проверки состояния ИБ департаментом безопасности;

3) сканирование информационных систем на предмет наличия уязвимостей, проведение тестов на проникновение, проводимых департаментом безопасности либо квалифицированными внешними аудиторами;

4) выявленные департаментом безопасности инциденты и нарушения требований ИБ.

5) проверки состояния ИБ при проведении аудиторских проверок.

6) иные аудиты и проверки системы ИБ.

46. Мероприятия по аудиту, требующие проведения проверок действующих систем, должны быть спланированы и согласованы таким образом, чтобы свести к минимуму риск прерывания бизнес-процессов.

47. Доступ к средствам и результатам аудита информационных систем должен быть защищен и ограничен с целью предотвращения возможного несанкционированного использования, компрометации или модификации.

48. Пересмотр настоящей Политики и подчиненных документов осуществляется по результатам процесса анализа и оценки в соответствии с пунктом 47 Политики, но не реже одного раза в год.

Глава 10. Заключительные положения

49. Несоблюдение порядка и правил использования информационных ресурсов и принятых в Фонде мер ИБ влечет за собой ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Фонда.

50. Положения Политики вступают в силу с момента их утверждения Советом директоров Фонда.

51. Настоящая Политика может быть пересмотрена с учетом изменений в деятельности Фонда, изменений в законодательстве Республики Казахстан и по мере необходимости.

52. Вопросы, не предусмотренные в положениях Политики, разрешаются в соответствии с законодательством Республики Казахстан, внутренними документами и решениями Совета директоров Фонда (при этом законодательство Республики Казахстан имеет превалирующую силу).

53. Департамент безопасности несет ответственность за актуальное содержание настоящих Правил.

Председатель Правления **Д. Медеушеева**

Лист согласования
Политики информационной безопасности АО «ЕНПФ»

Наименование должности	Инициал имени, фамилия	Подпись	Дата подписания	Примечание
Заместитель директора юридического департамента	М. Баратова			
Директор департамента информационных технологий	А. Ситников			
Директор департамента управления рисками	Ю. Баяндин			
Начальник подразделение стратегии и анализа	К. Фазылова			

Разработчик:
директор департамента безопасности
М. Мажитов _____ «___» _____ 201__ г.
(подпись)