Рег. № 19
от «01» февраля 202_ г.

Утверждена протоколом
Совета директоров АО «ЕНПФ»
от «26» января 2024 г. № 2

Политика
информационной безопасности АО «ЕНПФ»

Изменения и дополнения, утвержденные протоколом Совета директоров АО «ЕНПФ»:

№	Внесены изменения, дополнения	Дата утверждения	№ 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 Совета директоров АО «ЕНПФ» от «____» _____ 202__ г. № ___

Глава 1. Общие положения

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

2. Нормативную 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 вкладчиков обязательных пенсионных взносов (ОПВ), физических лиц, за которых перечислены обязательные пенсионные взносы работодателя (ОПВР), обязательные профессиональные пенсионные взносы (ОППВ), добровольные пенсионные взносы (ДПВ), получателей пенсионных выплат, получателей целевых требований 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. Требования настоящей Политики распространяются на 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. Под информационной безопасностью Фонда в настоящей Политике понимается состояние защищенности электронных информационных ресурсов, информации относящейся к коммерческой и (или) иной охраняемой законами тайне (конфиденциальная информация), информационных систем и информационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному и репутационному ущербу Фонда.

6. Политика информационной безопасности направлена на защиту персональных данных, информации по вкладчикам ОПВ, физическим лицам, за которых перечислены ОПВР, ОППВ, ДПВ, получателям пенсионных выплат, а также участникам целевых требований, получателей целевых требований и других заинтересованных сторон.

7. В настоящей Политике используются следующие термины, определения и сокращения:

1) администраторы ресурсов ИС – работники Департамента цифровизации и Департамента развития и поддержки инфраструктуры Фонда, осуществляющие администрирование информационных систем;

2) заинтересованные стороны – поставщики товаров/работ/услуг, управляющие компании по управлению пенсионными и (или) собственными активами, поставщики внешних информационных данных и другие деловые контрагенты, с которыми взаимодействует Фонд при реализации своих функций и задач;

3) ИБ - информационная безопасность;

4) инцидент ИБ - непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации;

5) ИС – информационная система;

6) ИТ-инфраструктура - это комплекс взаимосвязанных информационных систем и сервисов, обеспечивающих функционирование и развитие средств информационного взаимодействия Фонда;

7) кибератака - совокупность преднамеренных действий злоумышленника, направленных на нарушение одного из трех свойств информации — доступности, целостности или конфиденциальности;

8) компрометация корпоративных данных - факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа;

9) ОЦИБ - оперативный центр информационной безопасности, комплексное решение, позволяющее получать информацию о состоянии информационной безопасности в информационной и ИТ инфраструктуре путем централизованного сбора событий и сетевой активности в режиме реального времени, получать исчерпывающую информации о потенциально небезопасных и подозрительных активностях, представляющих риск для организации, проводить комплексный анализ и осуществлять выявление инцидентов в ИТ инфраструктуре в режиме 24/7/365.

Глава 2. Соответствие требованиям

8. Настоящая Политика и система ИБ в целом опираются на следующие нормативные правовые акты и международные стандарты (в данном разделе указаны основные нормативные акты,1 непосредственно влияющие на процесс создания системы ИБ Фонда в целом; в то же время существует ряд документов, которые либо описывают стратегические аспекты развития ИБ на государственном уровне, либо регламентируют правила по информационной защите отдельных приложений/услуг):

1) Социальный Кодекс Республики Казахстан от 20 апреля 2023 года № 224-VII ЗРК;

2) Закон Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам начисления детям средств из Национального фонда Республики Казахстан, их выплат и использования» от 16 ноября 2023 года № 40-VIII ЗРК;

3) Закон Республики Казахстан "О персональных данных и их защите" от 21.05.2013 № 94-V;

4) Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее – Единые требования);

5) Правила формирования системы управления рисками и внутреннего контроля единого накопительного пенсионного фонда, добровольных накопительных пенсионных фондов, утвержденные Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 7 июня 2023 года №40;

6) Требования к автоматизированным информационным системам для учета пенсионных активов и накоплений, утвержденные Постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 26 июня 2023 года №60;

7) Международный стандарт ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования» (СТ РК ИСО/МЭК 27001-2015);

8) Международный стандарт ISO/IEC 20000-1:2018 «Информационные технологии - Управление услугами – Часть1: Требования к системе управления услугами».

9. В Фонде соблюдаются требования нормативных правовых актов Республики Казахстан по защите права интеллектуальной собственности, персональных данных и ограничения по использованию криптографических средств.

10. Все требования и положения международного стандарта ISO/IEC 27001 и ISO/IEC 20000-1:2018 являются обязательными для исполнения в области их применения, определяемой соответствующими внутренними нормативными документами Фонда.

11. При разработке и применении средств и методов ИБ учитываются требования договорных обязательств Фонда с третьими лицами.

12. Положения настоящей Политики, законодательства Республики Казахстан в сфере информационной безопасности и международных стандартов ISO/IEC 27001 и ISO/IEC 20000-1:2018 содержатся в должностных инструкциях работников Фонда, задействованных в реализации требований данных стандартов и в договорах, заключаемых со сторонними

организациями и физическими лицами, задействованными в обслуживании и эксплуатации систем, на которые распространяется действие данных 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.

13. При наличии требований нормативных правовых актов Республики Казахстан или международных стандартов, Фонд проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям.

14. На основании Политики в Фонде утверждаются внутренние нормативные документы нижестоящего уровня, регламентирующие 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 3. Цели, задачи и основополагающие принципы построения ИБ

15. Основной целью ИБ является защита ИС Фонда, конфиденциальной информации, коммерческих и персональных данных от возможного нанесения ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня рисков. На достижение данной цели направлены все положения Политики для минимизации ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

16. Достижение поставленной цели обеспечивается выполнением следующих задач:

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).

17. В целях обеспечения информационной безопасности Фонда и соответствия Единым требованиям главной из основных задач ИБ является создание ОЦИБ на базе подразделения кибербезопасности.

18. В обязанности ОЦИБ входит мониторинг, анализ и противодействие сетевым атакам. ОЦИБ призван комплексно решить задачу по управлению уязвимостями, своевременно выявить попытки кибератак и обеспечить сохранность и конфиденциальность данных

19. ОЦИБ решает комплекс задач по оптимизации системы управления ИБ Фонда за счет:

1) регулярной коррекции и дополнения мер защиты;

2) уменьшения времени реакции на атаки и инциденты ИБ за счет использования готовых сценариев реагирования;

3) внедрения средств автоматизации для выявления инцидентов информационной безопасности и реагирования.

20. ОЦИБ отслеживает активность на рабочих станциях, серверах и в сетях, в приложениях, базах данных, на web-сайтах и других корпоративных интернет-ресурсах.

21. Задачи ОЦИБ:

1) обнаружить злонамеренные и аномальные действия;

2) идентифицировать угрозы;

3) провести анализ инцидентов информационной безопасности, и последующую оценку возникших рисков в области ИБ;

4) зарегистрировать и расследовать каждое из событий;

5) предотвратить компрометацию корпоративных данных.

22. Задачи ИБ, являются элементом общей политики руководства Фонда, основываются на требованиях деятельности Фонда, руководства и законодательства Республики Казахстан, разрабатываются и реализуются в соответствии с требованиями по управлению рисками в Фонде.

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

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

25. В целях обеспечения 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, представление 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.

26. Построение системы обеспечения ИБ Фонда и ее функционирование осуществляются в соответствии со следующими основными принципами:

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

2) ориентированность на деятельность Фонда – ИБ рассматривается как процесс поддержки основной деятельности Фонда. 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 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 реализовываются на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствуют 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 осуществляется профессионально подготовленными специалистами Фонда;

9) информированность и персональная ответственность – руководители всех уровней и все работники 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, создаются и хранятся с возможностью оперативного доступа и восстановления.

Глава 4. Объекты обеспечения информационной безопасности и защиты информации

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

1) информационные ресурсы, содержащие персональные данные и сведения, отнесенные в соответствии с действующим законодательством Республики Казахстан 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 иные 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.

28. 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 другим аналогичным устройствам в виде электрических сигналов.

Глава 5. Меры по обеспечению информационной безопасности

29. Основными мерами по обеспечению ИБ Фонда являются:

1) административно-правовые и организационные меры;
2) меры физической безопасности;
3) программно-технические меры.

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

1)установление процедур по обеспечению сохранности сведений, составляющих коммерческую тайну на рынке ценных бумаг, тайну пенсионных накоплений, условных пенсионных счетов, целевых накоплений и недопущению их использования в собственных интересах Фонда, их работников или третьих лиц;

2)установление перечня информации, относящейся к конфиденциальной информации, порядка составления, оформления, регистрации, учета и хранения документов, содержащих конфиденциальную информацию;

3)установление порядка допуска к конфиденциальной информации, с указанием должностных лиц;

4)установление механизмов предотвращения утечки конфиденциальной информации и искажения информационных данных, предусматривающие: перечень информационных данных, имеющих ограниченный доступ, порядок получения доступа, порядок контроля доступа к информационным данным и перечня должностей лиц, имеющих доступ к информационным данным;

5)выработка мероприятий по предотвращению несанкционированного доступа к базе данных посредством осуществления мониторинга и идентификации пользователей базы данных и обеспечения системой, позволяющей идентифицировать пользователя информационной системы;

6)контроль исполнения требований законодательства Республики Казахстан и внутренних нормативных документов Фонда;

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

8)контроль соответствия процессов требованиям Политики;

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

10) реагирование на инциденты, локализацию и минимизацию последствий;
11) анализ и оценка новых рисков ИБ;
12) отслеживание и улучшение морально-делового климата в коллективе;
13) определение действий при возникновении чрезвычайных ситуаций;
14) проведение профилактических мер при приеме на работу и увольнении работников Фонда.

31. 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;
6) выполнение плановых мероприятий.

32. 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) обеспечение регулярного резервного копирования информации;

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

7) использование криптографической защиты информации;

8) обеспечение безотказной работы аппаратных средств;

9) мониторинг состояния критичных элементов информационной системы.

Глава 6. Угрозы информационной безопасности

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

34. Угрозы ИБ подразделяются на (но не ограничиваясь ими):

1) случайные – стихийные бедствия, ошибки по невниманию, ошибки и сбои аппаратных и программных средств;

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

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

1) утрата информации, составляющей коммерческую тайну (конфиденциальную информацию) и иную защищаемую информацию;

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

3) утечка – несанкционированное ознакомление с защищаемой информацией посторонними лицами (несанкционированный доступ, копирование, хищение и другие правонарушения);

4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и другие правонарушения);

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 (чрезвычайных и кризисных ситуаций), иных форс-мажорных обстоятельств и злонамеренных действий.

36. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Фонда и его нормальное функционирование (включая, но не ограничиваясь):

1) применение к Фонду санкций, предписаний и иных мер регуляторного воздействия в связи с незаконным раскрытием тайны пенсионных накоплений, условных пенсионных счетов, целевых накоплений и иной защищаемой информации;

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

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

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

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

6) ущерб от отсутствия у руководства Фонда объективной информации;

7) репутационный ущерб Фонду;

8) иной вид ущерба

Глава 7. Разделение полномочий и ответственности

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

38. Руководство Фонда:

1) осуществляет стратегическое планирование;
2) утверждает внутренние 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 подразделение кибербезопасности;
9) отвечает за общее состояние ИБ.

39. Подразделение кибербезопасности:

1) как ОЦИБ получает информацию о состоянии ИБ путем централизованного сбора событий и сетевой активности в режиме реального времени, получает информацию о потенциально небезопасных и подозрительных активностях, представляющих риск для Фонда.
2) анализирует, вырабатывает и, при наличии оснований, дает рекомендации, направленные на предупреждение возникновения инцидентов ИБ;
3) реализует решения руководства Фонда и осуществляет общую организацию системы обеспечения ИБ, координирует и контролирует деятельность всех подразделений Фонда в сфере ИБ;
4) 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;
5) осуществляет 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 подразделения кибербезопасности или срыв сроков выполнения проектов;
6) осуществляет поддержку процесса управления и обеспечения ИБ Фонда;
7) осуществляет выбор средств и механизмов контроля, управления и обеспечения ИБ Фонда;
8) поддерживает штатное функционирование комплекса средств ИБ Фонда;
9) анализирует и оценивает угрозы в области ИБ Фонда;
10) контролирует соблюдение требований ИБ всеми участниками информационного обмена;
11) совместно с подразделением по управлению персоналом обеспечивает процесс обучения новых и действующих работников с требованиями ИБ, в части помощи по организации адаптационных/электронных/ежегодных курсов;
12) осуществляет мониторинг состояния ИБ Фонда;
13) проводит обработку событий и инцидентов, связанных с нарушениями ИБ, подготавливает соответствующие заключения и рекомендации;
14) информирует руководство Фонда о состоянии системы обеспечения ИБ, согласно регламента внутренних нормативных документов;
15) осуществляет методологическую поддержку процесса анализа и оценки рисков;
16) информирует подразделение по управлению рисками о событиях и инцидентах в области ИБ Фонда в соответствии с принятыми в Фонде требованиями внутренних документов по вопросам управления ключевыми и операционными рисками;
17) контролирует регистрацию событий и инцидентов, связанных с нарушениями ИБ, в соответствии с требованиями внутренних документов по вопросам управления ключевыми и операционными рисками;

18) обеспечивает функционирование процесса идентификации и оценки рисков ИБ с выработкой мер по обработке рисков и минимизации рисков ИБ в соответствии с Методикой оценки и обработки рисков системы управления информационной безопасностью АО «ЕНПФ»;

19) совместно с задействованными подразделениями принимает участие в осуществлении мероприятий, предусмотренных в Плане обеспечения непрерывности и восстановления деятельности АО "ЕНПФ", в том числе мероприятий, проводимых до возникновения чрезвычайных кризисных и/или не кризисных ситуаций.

40. Администраторы ресурсов ИС обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности:

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);

4) обеспечивают соответствующий уровень функционирования системы управления ИТ-услугами Фонда;

5) обеспечивают непрерывность всех процессов Фонда, минимизируют возможные потери и ущербы от нарушений в области ИТ- услуг Фонда.

41. Подразделение по управлению рисками проводит анализ зарегистрированных событий и инцидентов в области ИБ Фонда, результатов идентификации и оценки рисков ИБ, изучает план по обработке рисков ИБ и выработанные меры по минимизации рисков ИБ с целью определения целесообразности включения их в план по минимизации рисков для последующего мониторинга их исполнения в соответствии с требованиями внутренних нормативных документов по управлению ключевыми и операционными рисками в рамках функционирующей системы управления рисками Фонда.

42. Подразделение по управлению персоналом:

1) осуществляет обязательный комплекс мероприятий по сбору первичных документов при приеме кандидатов на работу и подписанию с работниками Фонда, а также со стажерами, практикантами соответствующих соглашений (трудовых договоров, договоров о прохождении стажировки, - обязательств о неразглашении служебной, коммерческой тайны (конфиденциальной информации));

2) по указанию руководства Фонда обеспечивает привлечение работников Фонда к дисциплинарной ответственности в случае нарушения Политики и внутренних нормативных документов по ИБ.

43. Юридический департамент проверяет проекты внутренних нормативных документов в области ИБ на предмет соблюдения общеустановленного порядка юридического оформления проекта внутреннего нормативного документа и соответствия законодательству Республики Казахстан.

44. Руководители структурных подразделений Фонда:

1) обеспечивают ознакомление работников с текущими требованиями ИБ;

2) отвечают за обеспечение ИБ во вверенных им подразделениях.

45. Структурные подразделения Фонда:

1) отвечают за соблюдение требований ИБ при внедрении, модификации, предоставлении услуг Фонда;

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

46. 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 кибербезопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными ресурсами.

Глава 8. Анализ и пересмотр

47. Анализ и оценка настоящей Политики, производных документов Фонда по информационной безопасности, информационных систем и системы ИБ пересматривается как минимум один раз в два года на основании результатов следующих мероприятий:

1) анализ состояния и эффективности системы ИБ руководством Фонда;

2) текущие проверки состояния ИБ подразделением кибербезопасности;

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

4) выявленные подразделением безопасности инциденты и нарушения требований ИБ.

5) проверки состояния ИБ при проведении аудиторских проверок.

6) иные аудиты и проверки системы ИБ.

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

49. Доступ к средствам и результатам аудита информационных систем защищается и ограничивается с целью предотвращения возможного несанкционированного использования, компрометации или модификации.

50. Пересмотр настоящей Политики и производных документов Фонда по информационной безопасности осуществляется по результатам процесса анализа и оценки в соответствии с пунктом 46 Политики.

Глава 9. Заключительные положения

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

51. Настоящая Политика пересматривается с учетом изменений в деятельности Фонда, изменений в законодательстве Республики Казахстан и по мере необходимости с учетом требований главы 2 настоящей Политики.

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. Подразделение кибербезопасности несет ответственность за актуальное содержание настоящей Политики.

54. Политика является публичным документом и может быть размещена на любых информационных ресурсах Фонда.

Председатель Правления **Ж. Курманов**

Лист согласования
Политики информационной безопасности АО «ЕНПФ»

Наименование должности	Инициал имени, фамилия	Подпись	Примечание
Управление антикоррупционного комплаенса	А. Жукенова		
Заместитель Директора Юридического департамента	А. Бимен		
Директор Департамента риск-менеджмента	Э. Талаева		
Заместитель Директора Департамента управления персоналом	Г. Жиеналина		
Директор Департамента организации выплат и информирования	Н. Рахимова		
Директор Департамента учета и отчетности пенсионных активов	А.Тусеева		
Директор Департамента развития и поддержки инфраструктуры	Р. Лосевской		

Настоящим подтверждаем, что производный документ на бумажном носителе соответствует документу, согласованному в электронном варианте.

Разработчик:
Директор
Департамента кибербезопасности

_____ Е.Алдабеков
(подпись)

Прошито и пронумеровано

на 13 (тринадцать) листах

Директор Департамента кибербезопасности

_____ Е. Алдабеков