Приложение
к Приказу АО «Казахтелеком»
от «29» __июля_____ 2021 года
№ 207___

Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2022 года
№ _____

Политика безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств АО "Казахтелеком"

Алматы, 2022

Оглавление

1 Термины, сокращения и определения

Администратор ИС – привилегированный пользователь, имеющий расширенные полномочия (привилегии) по настройке и эксплуатации ИС, а так же по управлению доступом к ИС;
АЭД – архив электронных документов;
ИБ – информационная безопасность. Состояние защищённости информационных ресурсов и систем, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность, что достигается целым комплексом организационных и технических мер, направленных на защиту данных;
ИР – информационный ресурс (актив). В рамках настоящей Политики понимается упорядоченная совокупность информации, представленная в электронном виде (файлы, базы данных, алгоритмы, компьютерные программы, приложения и т.д.) и содержащаяся, хранящаяся, обрабатываемая, передаваемая и используемая в информационных системах Общества (сети передачи данных, системы хранения, обработки, передачи, визуализации информации и т.п.);
ИС – информационная система. Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением соответствующих организационных ресурсов (человеческих, технических, финансовых и т. д.);
ИТ – информационные технологии. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
РД – регламентирующая документация Общества (политики, стандарты, приказы, регламенты, руководства, инструкции и т.п.);
Общество – Акционерное Общество «Казахтелеком»;
ОЭ – опытная эксплуатация;
Паспорт СВТ – документ, содержащий полный перечень оборудования и программного обеспечения СВТ;
Перечень ПО – документ «Перечень разрешенного к использованию ПО». Содержит перечень коммерческого и свободно распространяемого ПО, разрешенного к использованию в Обществе на установленный период. Должен утверждаться приказом или иным распорядительным документом, имеющий соответствующую силу.
ПО – программное обеспечение;
Политика – утвержденная в Обществе настоящая Политика безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств АО "Казахтелеком";
Пользователь – работник Общества или представитель третьей стороны, работающий с ИС Общества и использующий её ИР в соответствии с установленными правами и правилами доступа к информации;
ПЭ – промышленная (производственная) эксплуатация;
СВТ – средства вычислительной техники (стационарные компьютеры или рабочие станции, переносные компьютеры или ноутбуки и т.п.);

СП – структурное подразделение Общества;
СП ИТ – структурное подразделение Общества, ответственное за ИТ, технические обслуживание и эксплуатацию ИР и ИС Общества;
СП ТП – структурное подразделение Общества либо подразделение (или организация), привлекаемое для выполнения данных функций, которое выполняет техническую поддержку пользователей и СВТ в Обществе;
ТЗ – техническое задание;
ТП – техническая поддержка;
Третья сторона, третье лицо – физическое или юридическое лицо, подрядчик, поставщик, партнер, контрагент, контрактник, и т.п., взаимодействующие с Обществом на основании договорных соглашений и не являющееся штатным работником Общества;
ЧТЗ – частное техническое задание;
ЭДО – система электронного документооборота Общества;
РоС – Proof-of-concept («пилотный» проект, тестирование концепта и т.п.). Демонстрация практической осуществимости какого-либо метода, идеи, технологии, реализуемости с целью доказательства факта, что метод, идея или технология работают.

2 Назначение Политики и область ее действия

1. Настоящая Политика регламентирует процессы приобретения, разработки, тестирования, внедрения и эксплуатации ПО в ИС Общества.
2. Политика является руководящим документом и предназначена для обязательного использования в Обществе.
3. Требования Политики минимизируют вероятность возникновения негативных последствий и угроз безопасности для ИС Общества вследствие нарушений требований к процессам приобретения, разработки, тестирования и эксплуатации ПО.
4. Негативные последствия могут включать в себя вероятность повреждения ПО и ИС, появление уязвимостей ПО и ИС, внедрения вредоносного ПО в ИС, раскрытие или утрату чувствительной и конфиденциальной информации, кражу интеллектуальной собственности, репутационные последствия, а также влияние на важные внутренние системы и бизнес-процессы Общества.
5. Настоящая Политика применяется к любому ПО, работающему на ресурсах ИС Общества.
6. Политика устанавливает ответственность всех работников Общества и третьих лиц, использующих ИР и ИС Общества, разрабатывающих, приобретающих, тестирующих, использующих, эксплуатирующих и сопровождающих ПО в интересах Общества, и является обязательной для исполнения.
7. Политика предназначена для распространения внутри Общества и предоставления всем Руководителям, Работникам Общества и прочим заинтересованным лицам – участникам бизнес-процессов Общества.
8. Все исключения из правил и требований настоящей Политики должны быть согласованы со СП ИБ.

3 Общие положения и требования политики

9. Политика разработана в соответствии с законодательством Республики Казахстан в сфере ИБ, РД регулятора (регулирующих и надзорных органов), Политикой ИБ Общества, Концепцией ИБ Общества, серией международных стандартов по ИБ ISO/IEC 27000, COBIT, ITIL, современным состоянием и ближайшими перспективами развития информационной структуры Общества и возможности современных организационно-технических методов защиты информации.

10. Пересмотр положений Политики осуществляется на постоянной основе, но не реже одного раза в два года.

11. Внеплановый пересмотр Политики осуществляется в случае:

1) изменения нормативных правовых документов Республики Казахстан, РД регулятора (регулирующих и надзорных органов), определяющих требования ИБ;

2) выявления снижения общего и/или частного уровня ИБ Общества (по результатам внутреннего или внешнего аудита);

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

4) выявления существенных недостатков или противоречий положений Политики с другими внутренними документами Общества.

12. Положения Политики, могут дополняться, но не отменяться (заменяться), положениями других частных политик ИБ Общества и документами, разработанными на их основе.

13. Дополнительную информацию о безопасной работе и защите информации в ИС Общества можно получить из других частных политик ИБ Общества.

14. Любое ПО, используемое для осуществления деятельности Общества, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым), использоваться строго в соответствии с лицензионным соглашением, быть утвержденным в Перечне ПО и приобретаться непосредственно у разработчиков или официальных представителей и поставщиков. Случаи хранения и/или использования ПО, не являющегося лицензионным, должны быть исключены.

15. Все процессы и процедуры, связанные с приобретением, внедрением, тестированием, сдачей в эксплуатацию, эксплуатацией, поддержкой, обслуживанием, администрированием, устранением неисправностей и т.д. ПО должны выполняться в установленном порядке, в строгом соответствии с требованиями положений настоящей Политики и других внутренних РД Общества.

16. Во исполнение требований настоящей Политики в Обществе должен быть разработан и внедрен Перечень ПО (см. Приложение 1 к настоящей Политике), содержащий список категорий ПО и требований для них. Для категорий должны быть определены:

1) описания;

2) требования (критерии) допустимости установки и использования.

17. Для списка категорий применимы следующие условия:

1) ПО тех или иных категорий может быть запрещено полностью;

2) допускается использование лишь отдельного ПО какой-либо категории;

3) запрещается отдельное ПО категории, все остальное – разрешено;

4) требования могут дополняться и комбинироваться.

18. Цели разработки Перечня ПО следующие:

1) защита СВТ, ИР и ИС Общества от вредоносного ПО, вирусных атак и иных угроз безопасности;

2) снижение вероятности (риска) утечки информации Общества;

3) снижение вероятности (риска) передачи внутренней информации Общества (в том числе категорированной) через общедоступные, внешние и/или запрещенные серверы (сервисы);

4) повышение управляемости и подконтрольности используемого ПО применяемыми и перспективными средствами защиты информации и мониторинга.

19. При разработке Перечня ПО должны применяться следующие принципы:

1) запрет на использование ПО не должен препятствовать исполнению должностных, функциональных обязанностей, работающих с ним лиц (если реальных альтернатив ПО нет);

2) для распределенного ПО, преимущество в максимальной степени должно отдаваться тому, чьи серверы располагаются в сетях Общества, на территории Республики Казахстан;

3) во всех остальных случаях, при необходимости использования внешних ресурсов для функционирования ПО Общества и отсутствия иного (альтернативного) допустимого решения, должно быть обосновано такое использование и приняты соответствующие риски ИБ, также должно обеспечиваться применение повышенных требований к обеспечению ИБ на всех этапах внедрения, использования и мониторинга такого ПО.

20. Перечень ПО должен разрабатываться, вестись и актуализироваться уполномоченным СП ИТ при согласовании со стороны СП ИБ.

21. Любые СП, инициирующие приобретение, разработку, внедрение и т.п. нового ПО, должны в обязательном порядке официально уведомлять уполномоченное СП ИТ о данных фактах с целью актуализации Перечня ПО.

22. Сведения о вновь приобретенном ПО вносятся в Перечень ПО в виде дополнения и/или изменения.

23. В целях соблюдения актуального состояния перечня ПО, при выведении из эксплуатации (использования) того или иного ПО, необходимо своевременно вносить соответствующие поправки (изменения) в Перечень ПО.

24. В случае, если нормативными правовыми актами Республики Казахстан предъявляются особые требования к ПО (например, требование по сертификации такого ПО уполномоченными органами и т.п.) необходимо обеспечить выполнение таких требований.

25. На СВТ и ИС должен устанавливаться комплект только разрешенного ПО из Перечня ПО, необходимый и достаточный для выполнения на них поставленных задач.

26. Описание конфигурации СВТ и перечень установленного на нем ПО должен фиксироваться в Паспорте СВТ (см. Приложение 2 к настоящей Политике), который должен подписываться уполномоченным работником СП ТП, руководителем СП ТП, пользователем СВТ и его непосредственным руководителем. Тем самым подтверждается согласие сторон:

1) с указанной в Паспорте СВТ комплектацией оборудования СВТ и перечнем установленного ПО;

2) с фактом передачи от Общества к работнику (пользователю СВТ) ответственности за использование любого нелицензионного ПО, самовольное изменение конфигурации СВТ и несанкционированную установку любого ПО на вверенном данному пользователю СВТ.

27. Все операции по установке, сопровождению и поддержке, удалению ПО СВТ должны выполняться непосредственно (при участии) уполномоченными работниками СП ТП.

28. Разрешение использовать то или иное ПО (особенно касается такого ПО, как Google Drive, Yadex.Disk и т.п.) не свидетельствует о разрешении передавать через него информацию, которая является собственностью Общества, доступ к которой категорирован, ограничен требованиями законодательства Республики Казахстан, требованиями регулятора, а также требованиями положений РД Общества.

29. Договоры на закупку и разработку ПО должны включать обязательства поставщиков по сопровождению, обновлению версий, устранению и/или замене ПО при выявлении ошибок и/или неправильной работы ПО.

30. По возможности, а для специализированного ПО – обязательно, ПО должно поставляться вместе с исходными текстами (кодами).

31. При эксплуатации ПО необходимо:

1) соблюдать требования настоящей Политики;

2) использовать имеющееся в распоряжении ПО исключительно для выполнения своих служебных, должностных, функциональных и т.п. обязанностей;

3) обеспечивать сохранность переданных в составе СВТ носителей с ключевой информацией, сертификатов подлинности коммерческого ПО и т.п., наклеенных на корпус системного блока СВТ;

4) содействовать уполномоченным работникам СП ТП (при необходимости СП ИТ и СП ИБ) в выполнении работ по установке, настройке, устранению неисправностей и аудиту (учету) и др. установленного ПО;

5) ставить в известность уполномоченных работников СП ТП (при необходимости СП ИТ и СП ИБ) о любых фактах нарушения требований настоящей Политики.

32. При эксплуатации ПО, пользователям запрещено:

1) незаконное (нелицензионное) использование и хранение на жестких дисках СВТ и ИС Общества информации, являющейся объектом авторского права (программное обеспечение, фотографии, музыкальные файлы, игры и т.п.);

2) самостоятельно устанавливать ПО на СВТ и другие средства обработки информации;

3) самостоятельно вносить изменения в конструкцию, конфигурацию, размещение СВТ и другого оборудования ИС Общества;

4) изменять состав установленного на СВТ ПО (устанавливать новое ПО, изменять состав компонент пакетов ПО и удалять ПО);

5) использовать СВТ с установленным ПО не по назначению;

6) использовать установленное ПО, не предназначенное для исполнения ими функциональных обязанностей, в том числе системные утилиты и программы;

7) приносить на внешних носителях и несанкционированно запускать на своем или другом СВТ любые системные или прикладные программы, не указанные в Паспорте СВТ.

33. Защита операционных систем и прикладного ПО от известных технических уязвимостей должна поддерживаться своевременной установкой критических обновлений безопасности.

34. Для обеспечения корректной работы ПО рекомендуется применять системы автоматического обновления ПО. Критичные обновления безопасности ПО подлежат обязательному распространению во всех ИС Общества.

35. При внесении изменений в операционные системы, в том числе после установки обновлений, со стороны СП ТП должна быть проведена проверка корректности работы критичных приложений.

36. СП ИБ необходимо регулярно проверять установленное в Обществе ПО на предмет соблюдения авторских и смежных прав на интеллектуальную собственность в соответствии с установленными требованиями.

37. Требования к представителям третьих сторон, использующих в своей деятельности ПО Общества, должны соответствовать требованиям положений настоящей Политики и включаться в соответствующие положения договоров и соглашений.

38. ПО, установленное или используемое в Обществе в нарушение настоящей Политики, должно быть заблокировано и/или удалено уполномоченными и ответственными лицами соответствующих СП.

39. Любые инициативы и действия в отношении ПО (приобретение, внедрение, учет, хранение, использование и т.п.) должны выполняться в соответствии с установленными и принятыми в Обществе порядке и форме, при соблюдении требований положений настоящей Политики, разработанных на её основе документов.

40. Решение о потребности, необходимости приобретения и внедрения ПО в рамках различных инициатив (проектирование, модернизация, расширение и т.п.), необходимых для деятельности Общества и функционирования его бизнес-процессов, должно приниматься инициирующим заинтересованным СП (СП-заказчик).

41. Процедуры по экспертному рассмотрению, рецензированию и согласованию того или иного ПО в рамках инициативного решения на предмет целесообразности его применения, соответствия нормам и требованиям РД, соблюдения правил внедрения, интеграции и использования в ИС Общества, проверки технических и технологических аспектов и т.п., должны выполняться уполномоченным коллегиальным органом (рабочая группа, совет, комитет и т.п.), которые должны рассматривать подобные инициативы.

42. В состав такого уполномоченного коллегиального органа должны входить компетентные работники СП ИТ и СП ИБ (также, при необходимости, возможно привлечение работников и из других СП), которые должны обладать высоким уровнем экспертизы в рассматриваемых вопросах и направлениях.

43. Утверждать принятые уполномоченным коллегиальным органом решения должен Генеральный директор ДИТ (замещающее лицо).

44. Инициатором приобретения и внедрения нового ПО могут выступать:

1) руководители СП, осуществляющих обслуживание, эксплуатацию, поддержку СВТ, ИР и ИС Общества;

2) руководители СП, осуществляющих проектную и иную деятельность в Обществе, направленную на внедрение, развитие, усовершенствование, оптимизацию и т.п. СВТ, ИР и ИС Общества;

3) руководители СП, осуществляющих развитие и внедрение новых направлений бизнеса, бизнес-систем и т.п.;

4) руководители СП, являющиеся бизнес-владельцами ИР (ИС) либо лица, действующие в их интересах.

45. Инициатор должен подготовить служебную записку на имя Главного директора по ИТ Общества (замещающего лица), содержащую:

1) обоснование необходимости использования нового ПО;

2) функциональные требования к ПО;

3) перечень задач, для решения которых предназначено ПО;

4) степень критичности входной и выходной информации.

46. Служебная записка должна быть подготовлена в электронном виде в системе ЭДО.

47. Служебная записка должна согласовываться с руководством СП ИТ и СП ИБ.

48. Служебная записка поступает на рассмотрение и согласование к Главному директору по ИТ Общества (замещающему лицу), который на основании предоставляемых данных и проведенном анализе принимает решение о целесообразности использования нового ПО и согласовывает инициирование проекта для проведения работ по внедрению ПО.

49. Все работы, связанные с подготовкой проекта, оформлением необходимых документов и рассмотрением проекта на Проектном комитете, осуществляются в соответствии с внутренними документами Общества, регламентирующими порядок управления проектами.

50. В ходе подготовки проекта уполномоченными работниками СП ИТ должны быть изучены предложения на рынке программных средств, проведены иные необходимые исследования для принятия решения о целесообразности приобретения или разработки ПО.

51. Проведение исследований в части механизмов защиты ПО и соблюдения ИБ должно осуществляться уполномоченными работниками СП ИБ.

52. Решение о разработке или приобретении ПО должно максимально отвечать выдвинутым функциональным требованиям и общим требованиям ИБ в ИС Общества.

53. После концептуального принятия решения о приобретении или разработке ПО должны быть определены детальные требования к новому ПО.

54. Функциональные требования предъявляют работники инициатора внедрения ПО (СП-заказчика).

55. В отношении приобретаемого и внедряемого ПО должны предъявляться необходимые и достаточные требования для его работы и соответствия требованиям РД.

56. Требования в части технической реализации ПО предъявляются со стороны СП ИТ.

57. Требования в части механизмов ИБ и защиты ПО предъявляются со стороны СП ИБ.

58. Определение требований к новому ПО в рамках ИБ должно производиться с учетом:

1) требований национальных и международных стандартов в области ИБ;

2) требований законодательства Республики Казахстан;

3) требований регулятора;

4) внутренних документов по обеспечению ИБ;

5) степени критичности обрабатываемой информации, включая уровень конфиденциальности;

6) дополнительных требований в области ИБ.

59. В рамках требований ИБ должна быть определена необходимость включения в состав ПО следующих функциональных возможностей:

1) идентификация и аутентификация;

2) управление доступом к данным и действиями над ними;

3) регистрация, хранение и обработка событий безопасности;

4) контроль целостности файлов и программной среды;

5) криптографическая защита информации при ее хранении в ИС Общества и передаче по сетям и каналам связи;

6) использование грифов конфиденциальности данных, экранных и печатных форм в соответствии с требованиями положений РД Общества;

7) иное.

60. После определения детальных требований инициируется процесс приобретения или разработки ПО.

61. Приобретение ПО должно осуществляться согласно действующим в Обществе формам и правилам закупок.

62. В работе конкурсной комиссии в качестве технических экспертов должны принимать участие СП ИБ и СП ИТ.

4 Порядок действий при приобретении ПО

63. В рамках приобретения ПО должен соблюдаться следующий рекомендуемый порядок действий:

1) в случае принятия решения о приобретении ПО должна быть составлена Техническая спецификация, определяющая состав, количество и стоимость закупаемых средств;

2) Техническая спецификация должна готовиться уполномоченным лицом в Обществе, в роли которого может быть СП ИТ или уполномоченный коллегиальный орган (рабочая группа, совет, комитет и т.п.) с возможностью привлечения необходимых компетенции из числа работников СП Общества, для получения необходимых консультаций и помощи в работе либо это может быть внешняя организация (компания), предоставляющая необходимые услуги.

3) Техническая спецификация должна согласовываться руководством СП ИТ, СП ИБ и утверждаться Генеральным директором ДИТ;

4) после утверждения Технической спецификации на приобретение ПО должен быть проведен ее полный анализ путем проведения PoC. Для этого со стороны поставщика ПО должна предоставляться демонстрационная версия ПО (в том числе, лицензии на ПО и т.п.) и квалифицированная техподдержка на период проведения PoC;

5) порядок процедуры анализа нового ПО приведен в соответствующих пунктах настоящей Политики. По завершении анализа нового ПО в рамках проведения PoC должен быть составлен Акт приема-сдачи ПО в ОЭ с результатами и рекомендациями (см. Приложение 3 к настоящей Политике);

6) если в ходе анализа ПО было выявлено частичное и/или полное несоответствие ПО предъявленным к нему требованиям, должно быть принято решение о приобретении дополнительных программных средств для реализации требований или об отказе от использования данного ПО в ИС Общества;

7) на основании согласованного Акта приема-сдачи ПО в ОЭ по поручению Главного директора по ИТ может осуществляться дальнейшая процедура закупки полноценного пакета ПО;

8) после приобретения (закупки и получения) и перед промышленным использованием, ПО должно вводится в ОЭ. Порядок проведения ОЭ определен соответствующими пунктами настоящей Политики.

5 Порядок действий при разработке ПО

64. В рамках разработки ПО должен соблюдаться следующий рекомендуемый порядок действий:

1) на основании определенных требований к новому ПО должно быть составлено ТЗ на разработку ПО либо документ, его заменяющий;

2) ТЗ должно готовиться уполномоченным лицом в Обществе, в роли которого может быть СП ИТ или уполномоченный коллегиальный орган (рабочая группа, совет, комитет и т.п.) с возможностью привлечения необходимых компетенции из числа работников СП Общества, для получения необходимых консультаций и помощи в работе либо это может быть внешняя организация (компания), предоставляющая необходимые услуги.

3) при составлении ТЗ должны быть определены:

перечень СП Общества, в которых планируется внедрить ПО;

необходимые сведения о технологии обработки информации;

сведения об информации, получаемой в результате решения задач (получатели информации, периодичность выдачи информации, образцы выходных и экранных форм);

степень критичности обрабатываемой информации.

4) ТЗ должно быть согласовано с руководством СП ИТ, с руководством СП ИБ на предмет наличия необходимых требований к функциональным возможностям по защите информации и утверждено Генеральным директором ДИТ;

5) после утверждения ТЗ, при необходимости, уполномоченными работниками СП ИТ должно быть разработано ЧТЗ на реализацию определенной части требований, включенных в ТЗ. ЧТЗ должно быть согласовано с руководством СП ИБ;

6) разработка ПО должна осуществляться внешней (сторонней) организацией-разработчиком, которая должна иметь лицензию на осуществление деятельности по разработке соответствующего ПО, на основании договора. В договоре должны быть определены:

требования к материалам, предоставляемым организацией-разработчиком ПО;

ответственность разработчика за качество выполненных работ, за соответствие программного продукта техническим и функциональным требованиям ТЗ;

ответственность разработчика за отсутствие в разработанном ПО недокументированных возможностей;

7) по окончании выполнения работ организация-разработчик должна предоставить Обществу:

готовый программный продукт;

исходные коды ПО;

полную эксплуатационную и техническую документацию на ПО.

8) после получения разработанного программного продукта (ПО), уполномоченными работниками СП ИТ должен быть проведен PoC для анализа ПО, порядок которого определен соответствующими пунктами настоящей Политики;

9) ошибки, обнаруженные в процессе испытаний, должны быть устранены организацией-разработчиком ПО в установленные сроки;

10) при невозможности оперативного устранения неисправностей в ПО организация-разработчик совместно с представителями СП ИТ должна подготовить предложения по их устранению в процессе ОЭ. В этом случае оформляется Акт приема-сдачи ПО в ОЭ, к которому прилагается перечень замечаний (неисправностей), подлежащих устранению в процессе ОЭ;

11) в случае невозможности устранения неисправностей в процессе ОЭ организацией-разработчиком готовятся предложения о дополнительной доработке ПО с соответствующим переносом срока окончания работ. Предложения представляются на

рассмотрение руководству СП ИТ и Главному директору по ИТ для принятия по ним окончательного решения.

6 Порядок действий при анализе ПО

65. В ходе проведения PoC для анализа нового ПО должна проводиться оценка следующих его параметров:

1) соответствие ПО функциональным требованиям ИС Общества;

2) соответствие требованиям по защите, хранимой и обрабатываемой в ИС Общества информации;

3) соответствие функциональных возможностей ПО нормам и стандартам обработки информации в ИС Общества;

4) возможность эффективной работы на программно-аппаратных платформах и телекоммуникационной инфраструктуре ИС Общества;

5) надежность функционирования;

6) гибкость технологических решений, базы данных, технологии обмена информацией, интеграционными возможностями и т.п.;

7) качество сопровождения, возможность получения и установки новых модификаций и изменений к продукту по мере их появления;

8) качество разработанной технической и пользовательской документации, сложность технического сопровождения, модернизации прикладных программных систем, модификации и администрирования ПО;

9) возможность адаптации к изменяющимся условиям функционирования ИС Общества, в том числе возможность сохранения необходимого уровня защищенности ресурсов ИС Общества;

10) отсутствие недокументированных возможностей.

66. Анализ ПО должен проводиться в соответствии с блок-схемой (см. Приложение 4 к настоящей Политике).

67. Для проведения PoC и испытания (анализа, тестирования) ПО уполномоченные работники СП ИТ должны разработать Программу и методику испытаний (тестирования) ПО, которые регламентируют порядок проведения и виды испытаний, и содержат:

1) описание объекта испытаний (наименование, область применения и обозначение испытуемой программы);

2) цель испытаний;

3) требования к программе (требования, подлежащие проверке во время испытаний и заданные в ТЗ на программу);

4) требования к программной документации (указывается состав программной документации, предъявляемой на испытания);

5) средства и порядок испытаний (указываются программные и технические средства, используемые во время испытаний, а также порядок проведения испытаний);

6) набор тестовых заданий (приводятся описания проверок с указанием ожидаемых результатов проведения испытаний).

68. Программа и методика испытаний ПО согласуются с:

1) руководством СП ИБ в части соблюдения требований ИБ;

2) руководством СП ИТ.

69. Программа и методика испытаний ПО утверждаются Генеральным директором ДИТ.

70. Набор тестовых заданий должен содержать перечень задач, позволяющих проверить выполнение всех требований ТЗ или ЧТЗ. Минимальный набор тестов должен включать проверку:

1) выполнения функциональных требований при использовании тестовых данных ИС Общества;

2) взаимодействие (интеграция) нового ПО с действующими компонентами ИС Общества;

3) совместимости с различными платформами и периферийными устройствами, используемыми в ИС Общества;

4) работоспособности ПО в критических условиях работы при большой нагрузке и при недостаточном объеме оперативной памяти, дискового пространства, при недостаточной скорости обмена в линиях и каналах связи, при отключении части линий электропитания, линий и каналов связи и т.п.;

5) уровня устойчивости ПО при воздействии на него различных киберугроз, в том числе, атак на отказ, эксплуатация уязвимостей в коде и т.п.;

6) корректности работы внутренних алгоритмов калькуляции переменных и защиты от некорректного ввода/вывода;

7) документации и справочных файлов;

8) корректности работы штатных механизмов защиты информации в ПО;

9) степени соответствия требованиям стандартов в области защиты информации, законодательства Республики Казахстан, требований регулятора, а также внутренних документов ИБ Общества.

71. Проверка функциональных возможностей нового ПО в рамках PoC, должна проводиться на специально оборудованном стенде (тестовой зоне, пилотной зоне и т.п.). Стенд должен быть физически и логически изолирован от сетей и ИС Общества.

72. Проверка функциональных возможностей ПО должна проводиться совместно с:

1) администраторами ИС, которые будут осуществлять сопровождение данного ПО;

2) уполномоченными работниками СП ИБ;

3) уполномоченными работниками СП ИТ;

4) уполномоченными работниками СП, инициировавшего внедрение ПО;

5) при необходимости – с привлечением компетентных специалистов от организаций-разработчиков и/или поставщиков ПО.

73. Данные для тестирования должны быть предоставлены СП, которое будет эксплуатировать новое ПО (будет пользователем ПО). Данные должны соответствовать информации, которую планируется обрабатывать в новой подсистеме ИС Общества, но при этом не содержать конфиденциальной информации.

74. Критерием корректного выполнения тестов является соответствие результатов тестирования требованиям, описанным в ТЗ.

75. Все результаты проведения испытаний должны фиксироваться в Протоколе испытаний, который должен подписываться всеми участниками испытаний и утверждаться Генеральным директором ДИТ.

76. В случае полного соответствия ПО требованиям ТЗ принимается решение о вводе ПО в ОЭ.

77. На основании результата анализа Генеральный директор ДИТ принимает решение о возможности использования ПО в ИС Общества и о его вводе в ПЭ.

7 Порядок действий при проведении ОЭ

78. При проведении ОЭ должен соблюдаться следующий рекомендуемый порядок действий:

1) на основании Акта приема-сдачи ПО в ОЭ проводится ОЭ нового ПО совместно с:

администраторами ИС (при необходимости с привлечением СП ИБ);

уполномоченными работниками СП, которое будет эксплуатировать новое ПО (будет пользователем ПО);

2) продолжительность проведения ОЭ ПО должна быть не менее одного месяца;

3) по завершении ОЭ ПО должен быть составлен Акт ввода ПО в ПЭ (см. Приложение 5 к настоящей Политике), который подписывают руководители всех СП, участвовавших в проведении ОЭ. Аудитор СП ИБ должен проконтролировать корректность и правильность составления Акта. На основании Акта новое ПО вводится в ПЭ.

8 Порядок действий при хранении дистрибутивов, лицензий и документации ПО

79. При хранении дистрибутивов, лицензий и документации ПО должен соблюдаться следующий рекомендуемый порядок действий:

1) у руководства СП ИТ и/или СП ИБ должна храниться документация в бумажном и/или электронном виде на ПО, сопровождение которого осуществляет соответствующее подразделение;

2) при необходимости документация в бумажном и/или электронном виде может храниться в СП, эксплуатирующем (являющимся пользователем ПО) и/или являющимся бизнес-владельцем данного ПО. В этом случае руководитель такого СП должен назначить работника, ответственного за хранение документации. Доступ к документации может предоставляться только с разрешения руководителя СП;

3) должен быть создан единый АЭД для хранения дистрибутивов и документации на ПО. Управление АЭД должно быть возложено на уполномоченного работника СП ИТ;

4) после приобретения и/или разработки нового ПО, работниками СП ИТ должен быть оформлен Паспорт ПО в бумажном и/или электронном видах (см. Приложение 6 к настоящей Политике);

5) дистрибутивы ПО, коды программ, документация и Паспорт ПО в электронном виде должны передаваться в АЭД;

6) доступ к АЭД должен быть ограничен и предоставляться в порядке, определенном Политикой управления доступом к ИР;

7) документы, подтверждающие покупку ПО, должны храниться в СП, ответственном за финансовую отчетность (бухгалтерия и т.п.) на протяжении всего времени использования ПО и лицензий в деятельности Общества, копии указанных документов должны храниться в СП ИТ;

8) лицензионные соглашения на ПО, ключи защиты программного обеспечения, дистрибутивы ПО и т.п. должны храниться в СП ИТ.

9 Порядок эксплуатации ПО

80. В рамках эксплуатации ПО должен соблюдаться следующий рекомендуемый порядок действий:

1) установка и настройка нового ПО осуществляется в соответствии с установленными требованиями положений внутренних РД (например, Правилами внесения изменений в конфигурации программно-аппаратных средств ИС Общества и т.п.);

2) запрещается установка дистрибутивов ПО не из АЭД и не внесенных в Перечень ПО;

3) постоянная эксплуатация ПО должна проводиться в соответствии с требованиями лицензионного соглашения;

4) в состав ПО к моменту начала его промышленной эксплуатации в ИС Общества не должны входить средства отладки программ.

10 Порядок контроля установленного ПО

81. В целях контроля установленного ПО должен соблюдаться следующий рекомендуемый порядок действий:

1) уполномоченный представитель СП ИТ должен проводить контроль установленного ПО:

выборочно на 5% СВТ пользователей ИС Общества – два раза в год;

на всех серверах и сетевом оборудовании ИС Общества – один раз в год;

2) после проведения мероприятий по контролю, уполномоченный представитель СП ИТ должен в установленном порядке подготовить и направить отчет с результатами контроля в СП ИБ;

3) СП ИБ должно выполнить анализ отчетной информации и в случае выявления несоответствий установленного ПО Паспортам СВТ, формулярам серверов и заявкам на установку ПО, ответственный сотрудник СП ИБ должен действовать в соответствии с установленными правилами в части расследования инцидентов ИБ;

4) со стороны СП ИБ должна осуществляться проверка соблюдения требований положений Политик ИБ при внедрении ПО и осуществляться проверка правильности внедрения программных средств (ПО).

11 Роли и ответственность

82. Контроль за выполнением требований и правил Политики возлагается на СП ИБ, Руководителей СП, Руководителей филиалов Общества.

83. Ответственность за контроль исполнения и актуальность Политики, а также внесение в нее изменений возлагается на СП ИБ.

84. Ответственность за обеспечение должного исполнения требований и правил Политики возлагается на все заинтересованные СП в рамках их полномочий и в соответствии с положениями, установленными Политикой и разработанными на ее основе документами.

85. Руководители СП несут ответственность за своевременное доведение требований Политики до работников их подразделений и/или представителей третьих сторон в части их касающейся и за выполнение работниками их подразделений и/или представителями третьих сторон требований Политики.

86. Ответственность за организационное и методическое обеспечение процессов использования программных средств ИС Общества возлагается на СП ИБ.

87. Контроль за действиями администраторов ИС при использовании программно-аппаратных средств возлагается на руководство СП в соответствии с требованиями положений настоящей Политики.

88. В случае выявления нарушений требований настоящей Политики пользователем ИС (администратором ИС), которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, руководство СП должно в обязательном порядке уведомлять о произошедшем СП ИБ и должно инициироваться, и вестись служебное расследование с привлечением заинтересованных СП и в соответствии с утверждённым Порядком расследования инцидентов ИБ.

89. Нарушение положений Политики или разработанных в поддержку Политики документов, включая любое преднамеренное действие, предпринимаемое с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области ИБ, может привести к административному или уголовному наказанию в соответствии с действующим законодательством, а также РД по управлению персоналом Общества.

90. Решение о применении и выборе мер ответственности принимается руководством Общества по результатам проведенного служебного расследования в зависимости от целесообразности применения рассматриваемых мер, а также от сведений об умышленности нарушения.

Приложение 1
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

Перечень разрешенного к использованию ПО

п/п №	Дата включения в Перечень	Категория ПО	Описание			Кол-во лицензий и особенности лицензирования	Требования
			Производитель ПО	Название ПО	Область применения		
1	2	3	4	5	6	7	8
1	01.01.2021	Антивирусное ПО	Kaspersky	KAV	СВТ, серверы	1000	Использование разрешено
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

Приложение 2
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

Паспорт СВТ

Номер_____

Компьютер:

Имя:		Инв. номер:	
Модель:		Серийный номер:	
Домен:		IP-адрес:	

Пользователь:

ФИО:		Номер:	
E-mail:		Учетная запись:	
Группа:		СП:	
Телефон:		Примечание:	

Операционная система:

Название:	Серийный номер:

Программное обеспечение:

Издатель:	Продукт:	Серийный номер:

Примечание:

_____

Дата:	
Администратор:	
Владелец:	

Работник СП ТП _____
(подпись) (ФИО работника)

Руководитель СП _____
(подпись) (ФИО работника)

Работник СП (пользователь СВТ) _____
(подпись) (ФИО работника)

Приложение 3
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

АКТ
приема-сдачи ПО в опытную эксплуатацию

«___» _____ 20__ года № _____

Настоящий акт составлен в том, что
_____
(название организации разработчика/ поставщика)

разработала/предоставила ПО
_____,

состоящее из комплекса задач (задачи)___ _____

Основание для выполнения работы_____

Сдаваемая работа представлена в виде_____
(наименование документации)

В результате испытаний установлено
_____
(в данном разделе отражаются конкретные замечания по функционированию программы, сбои, ошибки, обнаруженные в процессе испытаний, с указанием причин их возникновения, приводятся замеченные нарушения, отмечаются отклонения от ТЗ. При отсутствии замечаний устанавливается, что ПО прошло приемо-сдаточные испытания, отвечает требованиям подразделения–заказчика и принимается в опытную эксплуатацию)
_____

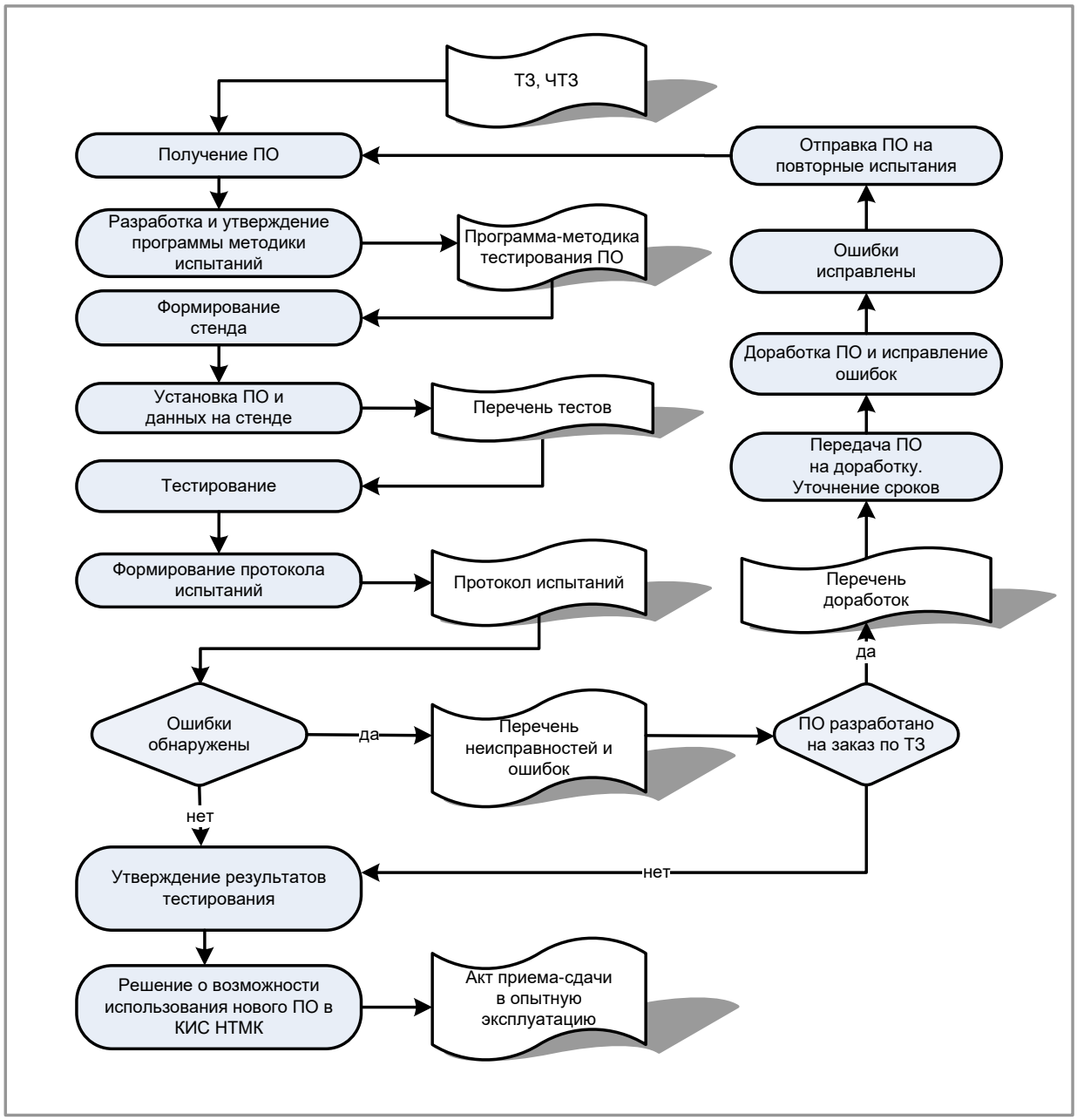
Генеральный директор ДИТ
_____
«___» _____ 20__ года

Руководитель СП ИБ
_____
«___» _____ 20__ года

Руководитель СП ИТ
_____
«___» _____ 20__ года

Приложение 4
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

Блок-схема порядка анализа нового ПО



Приложение 5
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

АКТ
ввода ПО в промышленную эксплуатацию

«___» _____ 20__ года № _____

Настоящий акт составлен в том, что ПО_____
_____,

состоящее из комплекса задач (задачи)_____
_____,

прошло приемо-сдаточные испытания и опытную эксплуатацию, отвечает требованиям подразделения-заказчика и принимается в промышленную эксплуатацию.

Основание для выполнения работы_____

Сдаваемая работа представлена в виде_____
(наименование документации)

Генеральный директор ДИТ
_____
«___» _____ 20__ года

Руководитель СП ИБ
_____
«___» _____ 20__ года

Руководитель СП ИТ
_____
«___» _____ 20__ года

Приложение 6
к Политике безопасности при приобретении, разработке, эксплуатации ПО и программно-аппаратных средств

Паспорт ПО

Номер_____

Наименование	Описание
Название программного обеспечения /модуля	
Тип	Общее/специальное
Функциональное назначение	
Описание поставляемого программного обеспечения /модуля	
Разработчик/поставщик	Название_____ Адрес_____ Контактная информация_____
Форма поддержки	Отсутствует Горячая линия_____ № Договора на обслуживание Другое _____
Количество лицензий	_____
Список документации на программное обеспечение	Функциональное описание Руководство пользователя Описание технической архитектуры Инструкция по установке Описание баз данных Схема межмодульного взаимодействия Инструкция администратора Описание диагностических сообщений Другая документация _____
Наименование подразделения, купившего (заказавшего) программное обеспечение	
Расположение места хранения дистрибутива и документации	
Ответственный за хранение	
Дата приема ПО	
Ответственный за сопровождение	Ф.И.О._____ Контактная информация_____

Требования к программно-аппаратному обеспечению

Наименование	Описание
Тип процессора	
Оперативная память	
Объем на диске	

Перечень модулей ИС, с которыми взаимодействует ПО

Название модуля	Описание взаимодействия

Руководитель СП, использующего ПО _____ «___» _____ 20__ года

Работник, ответственный за сопровождение ПО _____ «___» _____ 20__ года

Работник, ответственный за хранение дистрибутивов _____ «___» _____ 20__ года