Выписка из протокола № 6
очного заседания Совета директоров акционерного общества
«Центр развития города Алматы»

г. Алматы «27» сентября 2022 года

Наименование и место нахождения исполнительного органа акционерного общества: Правление АО «Центр развития города Алматы» *(далее - Общество)*, Республика Казахстан, город Алматы, улица Абая, дом 90.

Место проведения заседания Совета директоров Общества:
Республика Казахстан, город Алматы, улица Айтеке би, 67.

Дата и время проведения заседания Совета директоров Общества:
Открыто в 12.00 часов 27 сентября 2022 года;
Закрыто в 13.00 часов 27 сентября 2022 года.

На момент проведения очного заседания Совета директоров Общества количественный состав Совета директоров составляет 6 человек. Присутствовали 5 членов Совета директоров. Отсутствует по уважительной причине Конирбаев Б.К. *(находится в командировке)*.

Кворум для принятия решений имеется.

Повестка дня очного заседания Совета директоров

3. Об утверждении Политики информационной безопасности АО «Центр развития города Алматы».

В соответствии с подпунктами 13) пункта 31 Устава АО «Центр развития города Алматы», **Совет директоров РЕШИЛ**:

1. Утвердить проект Политики информационной безопасности АО «Центр развития города Алматы» согласно приложению №4 к настоящему протоколу;

2. Признать утратившим силу Политику информационной безопасности АО «Центр развития города Алматы», утверждённую решением Совета директоров Общества, протокол №1 от 06 января 2021 года.

3. Исполнительному органу АО «Центр развития города Алматы» принять необходимые меры, вытекающие из настоящего решения.

Председатель
Совета директоров [подпись] Е. Досаев

Корпоративный секретарь [подпись] Н. Барлыбаев

Корпоративный секретарь **Н.Барлыбаев**

Утверждена
решением Совета директоров
АО «Центр развития города Алматы»
от «27» 05 2022 года
протокол №6
приложение №4

Политика информационной безопасности
АО «Центр развития города Алматы»

г. Алматы

Содержание

1. Общие положения

1. Настоящая Политика информационной безопасности АО «Центр развития города Алматы» (далее - Политика) предназначена для определения целей и требований обеспечения информационной безопасности АО «Центр развития города Алматы».

2. Под обеспечением информационной безопасности или защитой информации понимается сохранение её конфиденциальности, целостности и доступности.

Конфиденциальность информации обеспечивается предоставлением доступа к информационным ресурсам только авторизованным пользователям, целостность – обеспечивается в случае внесения изменений в данные авторизованными пользователями, доступность – в обеспечении возможности доступа к информационным ресурсам авторизованным пользователям в нужное для них время.

3. В Политике используются следующие основные понятия и сокращения:

1) Общество – АО «Центр развития города Алматы»;

2) информационная безопасность (далее – ИБ) – комплекс правовых, технических и организационных мероприятий Общества, направленных на обеспечение защиты информационных ресурсов от несанкционированного доступа, преднамеренного или случайного искажения и разрушения, физического разрушения, в том числе в результате воздействий техногенного и природного характера, а также состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

3) подразделение ИТ (далее – ПИТ) – структурное подразделение Общества, ответственное за системно-техническое обслуживание информационно-коммуникационной инфраструктуры Общества, либо персонал Общества, привлеченный к данной деятельности;

4) менеджер по ИБ – работник Общества, ответственный за ИБ Общества;

5) пользователь – штатные и внештатные работники Общества, стажеры, практиканты и лица, оказывающие услуги гражданско-правового характера, использующее информационные ресурсы Общества;

6) контрагент - физическое или юридическое лицо, с которым Обществом заключен договор;

7) информационная система (далее – ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

8) электронные информационные ресурсы (далее – ЭИР) – информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

9) ИТ-администратор – работник Общества, ответственный за настройку, администрирование, поддержку, сопровождение и обеспечение бесперебойного функционирования ИС Общества;

10) конфиденциальность информации – обеспечение предоставления информации только авторизированным лицам;

11) целостность информации – состояние информации (информационных ресурсов ИС), при котором её (их) изменение осуществляется только авторизованными пользователями;

12) система управления информационной безопасностью (далее – СУИБ) – часть общей системы управления Общества, основанная на оценке рисков ИБ и предназначенная для разработки, реализации, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ;

13) Руководство Общества – Правление Общества;

14) доступность – обеспечение возможности доступа авторизованным пользователям к информационным ресурсам ИС Общества.

2. Нормативные документы

4. Настоящий документ разработан в соответствии со следующими правовыми актами и документами:

1) Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;

2) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

3) Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 г. № 111/НҚ «Об утверждении методики и правил проведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности»;

4) СТ РК ISO/IEC 27001-2015 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью»;

5) СТ РК ISO/IEC 27002-2015 «Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасности».

3. Цели и задачи обеспечения ИБ

5. Целями настоящей Политики являются:

1) предотвращение и минимизация ущерба от реализации угроз ИБ;

2) повышение (увеличение) защиты конфиденциальности, целостности и доступности информации Общества.

6. Для достижения указанных целей необходимо решение следующих задач:

1) обеспечение непрерывности деятельности Общества, организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты активов посредством комбинации предупреждающих и восстанавливающих мер и мероприятий;

2) управление рисками ИБ в целях недопущения или снижения вероятности возникновения внештатных ситуаций;

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

4) создание механизма постоянного мониторинга и реагирования на нарушения;

5) защита конфиденциальности, целостности и доступности всех значимых для Общества активов.

4. Основные принципы обеспечения ИБ

7. Основным принципом является защита ИС и ЭИР Общества от возможного нанесения материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования или несанкционированного доступа к циркулирующей в ней информации и её незаконного использования.

8. Защита ИС и ЭИР Общества достигается посредством обеспечения и постоянного поддержания следующих свойств:

1) доступности обрабатываемой информации;

2) обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники и передаваемой по каналам связи;

3) целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой и передаваемой по каналам связи.

9. Для обеспечения указанных свойств Общество должно обеспечивать эффективное решение следующих задач:

1) защиту от вмешательства в процесс функционирования посторонних лиц (возможность использования ИС и доступ к её ресурсам должны иметь только зарегистрированные пользователи, за исключением открытых данных);

2) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа: к информации, средствам вычислительной техники, аппаратным, программным и криптографическим средствам зашиты.

3) регистрация действий пользователей при использовании защищаемых ресурсов в системных журналах и периодический контроль корректности действий пользователей ИС путём анализа содержимого этих журналов ответственными работниками;

4) контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

5) защиту от несанкционированной модификации и контроль целостности ИС и ЭИР Общества, а также защиту ИС от внедрения несанкционированных программ, включая компьютерные вирусы;

6) защиту конфиденциальной информации, информации с ограниченным доступом, персональных данных от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи;

7) защиту конфиденциальной информации, персональных данных, информации с ограниченным доступом, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

8) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

9) своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам Общества, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

10) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

5. Область распространения

10. Действие настоящей Политики распространяется на всех работников Общества, а также контрагентов Общества, учитывается в договорных отношениях с последними, применяется ко всем информационным технологиям и телекоммуникационным ресурсам, используемым в Обществе, а также ко всем помещениям, в которых пользователь может получить доступ к ИС и информационно-коммуникационной инфраструктуре Общества.

11. В целях обеспечения выполнения требований настоящей Политики, необходимо обеспечить её соблюдение, как пользователями, так и контрагентами Общества. Поэтому, в соответствующих случаях, все договоры, заключаемые со сторонними юридическими и физическими лицами, должны содержать требование о соблюдении Политики и обеспечении ИБ. Вся деятельность, подразумевающая контакт контрагентов с данными, содержащимися в ИС и ЭИР Общества, должна осуществляться в соответствии с требованиями Политики. Выполнение данного требования является обязанностью структурного подразделения Общества, ответственного за подготовку договоров.

6. Распределение обязанностей по обеспечению ИБ

12. Руководство Общества, ПИТ и менеджер по ИБ реализуют комплекс мероприятий по поддержанию ИБ ИС и ЭИР Общества посредством дачи ясных указаний и чётких постановок задач работникам Общества, осведомлённости работников Общества об обязанностях по обеспечению ИБ:

1) менеджер по ИБ обеспечивает формирование и контроль выполнения всех пунктов данной Политики, отвечает за руководство разработкой, анализом Политики;

2) Руководство должно обеспечить чёткое управление и зримую поддержку инициатив по совершенствованию СУИБ, координацию мер контроля за ИБ в Обществе, предоставлять ресурсы для обеспечения ИБ, утверждать распределение специфических ролей и обязанностей по ИБ;

3) Руководство берет на себя обязательство о соответствии информационной системы действующим требованиям, связанным с информационной безопасностью, законодательным требованиям, в том числе требованиям по соблюдению прав на интеллектуальную собственность;

4) менеджер по ИБ совместно с ПИТ должен инициировать планы и программы по поддержанию осведомлённости об ИБ.

13. ИТ-администраторы действуют в строгом соответствии с зонами их ответственности, согласно утвержденному Руководству администратора по сопровождению объекта информатизации Общества.

14. Пользователи ИС Общества действуют в строгом соответствии с зонами их ответственности, согласно утвержденным должностным обязанностям, учётным ролям в ИС и Руководствам пользователя ИС Общества.

7. Координация ИБ

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

16. Координация ИБ должна включать взаимосвязь и сотрудничество, пользователей, ИТ-администраторов, разработчиков прикладного программного обеспечения и квалифицированных специалистов в таких областях, как кадровые ресурсы, информационные технологии и управление рисками. Эта деятельность должна:

1) обеспечивать соответствие выполнения мероприятий по обеспечению ИБ;

2) определять мероприятия по обеспечению ИБ в случае её несоответствия Политике;

3) утверждать методологии и процессы обеспечения ИБ, например, оценку рисков, классификацию информации;

4) идентифицировать все изменения угроз ИБ и степень уязвимости информации и средств обработки информации к угрозам ИБ;

5) оценивать адекватность принимаемых решений и координировать реализацию мер контроля ИБ;

6) повышать уровень подготовки пользователей в области ИБ и осведомлённости о ней;

7) оценивать информацию, полученную от мониторинга и просмотра инцидентов по ИБ и рекомендовать соответствующие мероприятия в ответ на идентифицированные инциденты ИБ.

8. Обучение и осведомлённость в вопросах ИБ

17. Требования к обучению и осведомлённости в вопросах ИБ:

1) пользователи, работники ПИТ, ИТ-администраторы Общества и контрагенты (в применимых случаях) должны быть ознакомлены с Политикой;

2) менеджер по ИБ Общества должен проводить первичный инструктаж по ИБ;

3) работники ПИТ и ИТ-администратор, обеспечивающие функционирование ИС Общества должны проходить регулярный инструктаж по соблюдению требований ИБ;

4) менеджер по ИБ по мере необходимости, но не менее одного раза в три года, проходит курсы по повышению квалификации по ИБ;

5) в целях обеспечения гарантированного уведомления менеджером по ИБ, всех заинтересованных сторон об инциденте и уязвимости ИБ по отношению к ИС Общества должны быть реализованы формальные процедуры по уведомлению об инциденте и проявлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры по сохранению ИБ;

6) менеджер по ИБ Общества должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, о наступлении которых или предпосылках к таковым необходимо отправить уведомление;

7) работники ПИТ и ИТ-администраторы Общества обязаны как можно быстрее сообщать о любых нарушениях в сфере ИБ менеджеру по ИБ;

8) менеджер по ИБ должен вести мониторинг посещения серверного помещения за работниками ПИТ.

9. Управление инцидентами

18. В случае обнаружения нарушения ИБ следует незамедлительно доложить менеджеру по ИБ.

19. Все работники, контрагенты и пользователи, пользующиеся ИС и ЭИР Общества обязаны незамедлительно доложить менеджеру по ИБ и по возможности обеспечить минимизацию ущерба.

20. В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях».

10. Управление непрерывностью бизнеса

21. Необходимо внедрить процесс управления непрерывностью бизнеса с целью минимизации влияния на деятельность Общества и восстановления после потери активов (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования, преднамеренных и непреднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению ИБ. Этот процесс должен идентифицировать важные бизнес-

процессы и интегрировать требования непрерывности бизнеса управления ИБ с другими требованиями непрерывности касательно таких аспектов, как операции, кадровое обеспечение, материалы, и оборудование.

22. Последствия бедствий, нарушений безопасности, отказов в обслуживании и доступность сервисов должны быть предметом анализа степени влияния на бизнес. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью возобновления важных операций в течение требуемого времени при их нарушении. ИБ должна быть составной частью общего процесса непрерывности бизнеса, и других процессов управления в Обществе.

23. Необходимо, чтобы обеспечение управления непрерывностью бизнеса включало мероприятия по управлению ИБ для идентификации и уменьшения рисков, в дополнение к общему процессу оценки степени риска, ограничения последствий разрушительных инцидентов, и обеспечения доступности информации, требуемой для процессов бизнеса.

24. Необходимо разработать и поддерживать управляемый процесс непрерывности бизнеса для всего Общества, который соответствует требованиям ИБ, необходимым для обеспечения непрерывности бизнеса.

25. В процессе должны быть собраны вместе следующие ключевые элементы управления непрерывности бизнеса:

1) понимание рисков, с которыми сталкивается Общество, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов;

2) определение всех активов, задействованных в критических бизнес-процессах;

3) понимание возможных последствий нарушения бизнес-процессов, вызванных инцидентами нарушения ИБ, в случае незначительных или существенных инцидентов, потенциально угрожающих деятельности Общества, а также выбора средств и способов обработки информации, соответствующих к целям бизнеса;

4) организация оптимального страхования результатов обработки информации, которое может быть частью общего процесса непрерывности бизнеса, а также частью управления операционным риском;

5) определение и рассмотрение вопроса реализации дополнительных превентивных и подавляющих средств контроля;

6) идентификация достаточных финансовых, организационных, технических ресурсов и ресурсов окружающей среды для соответствия идентифицированным требованиям ИБ;

7) обеспечение безопасности персонала и защиты средств обработки информации и собственности Общества;

8) формулирование и документирование планов обеспечения непрерывности бизнеса, удовлетворяющих требования ИБ в соответствии с согласованной стратегией;

9) регулярное тестирование и обновление планов развития информационных технологий и существующих процессов;

10) обеспечение органичного включения в процессы и структуру Общества планов управления непрерывностью бизнеса.

11. Анализ и оценка рисков

26. Требования к анализу и оценке рисков:

1) Политика первоначально должна основываться на данных, полученных в результате анализа и оценки рисков ИБ;

2) с целью совершенствования Политики должен проводиться ежегодный анализ и оценка рисков ИБ для ИС и ЭИР Общества;

3) анализ и оценка рисков должна проводиться в соответствии со стандартами, действующими на территории Республики Казахстан;

4) при оценке рисков должно учитываться влияние реализации угроз ИБ на количественные и качественные показатели. Реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению ИБ должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе.

12. Контроль изменений

27. В целях минимизации влияния инцидентов, связанных с изменениями, на качество предоставляемых услуг, работоспособности ИС, используются стандартные методы и процедуры для продуктивной и своевременной обработки изменений. Процедуры управления изменениями в операционной среде и в программных приложениях должны содержать следующие мероприятия:

1) утверждение предлагаемых изменений;

2) планирование и тестирование изменений;

3) оценка возможных последствий изменений;

4) информирование об изменениях всех заинтересованных лиц;

5) определение процедур и обязанностей по восстановлению работ средств и систем обработки информации в случаях возникновения сбоев по причине некорректных изменений;

6) регистрация изменений.

28. Для предотвращения отрицательного воздействия изменений на качество оказываемых публичных услуг необходимо заранее протестировать изменения.

29. Тестирование изменений должно учитывать следующие аспекты:

1) производительность;

2) безопасность;

3) возможность обслуживания;

4) версионную совместимость;

5) надежность и доступность;

6) функциональность.

30. Для обеспечения надлежащего контроля по всем изменениям в оборудовании, программном обеспечении или процедурах должны быть определены роли, ответственности и процедуры. Вся необходимая информация

об изменениях программного обеспечения должна фиксироваться и сохраняться в журнале регистрации изменений/обновлений.

31. В целях снижения риска несанкционированного доступа или изменения в ИС обеспечивается разделение средств разработки, тестирования и эксплуатации.

32. Должны быть определены и документированы процедуры передачи программного обеспечения из стадии разработки в стадии тестирования и эксплуатации.

33. Компиляторы, редакторы и другие системные утилиты не должны быть доступны в операционной среде без крайней необходимости.

34. Среда, в которой выполняется тестирование, должна быть как можно более близкой к среде рабочей системы.

35. Для снижения рисков возникновения ошибок пользователи должны использовать различные пользовательские профили в рабочей системе и в системе для тестирования. Меню на обеих системах должны отображать соответственно одинаковые идентификационные сообщения.

36. Тестирование должно выполняться на наборе данных, некритичных для ИБ.

37. Для выполнения требований по разграничению средств разработки, тестирования и эксплуатации необходимо использоваться отдельный тестовый стенд.

38. Любое новое программное обеспечение (в том числе продление лицензий) и аппаратные средства должны быть соответствующим образом одобрены со стороны Руководства, с учетом целей их использования и согласованы с менеджером по ИБ.

13. Пересмотр Политики

39. Общество является владельцем Политики. Менеджер по ИБ обеспечивает развитие, пересмотр и анализ эффективности Политики. Пересмотр должен включать возможности оценки для улучшения Политики и подход к управлению ИБ в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

40. При пересмотре Политики необходимо учитывать результаты мониторинга управления ИБ.

41. Входные данные для пересмотра управления ИБ должны включать информацию по:

1) обратной связи от заинтересованных сторон;
2) результатам независимых пересмотров;
3) статусу превентивных и корректирующих действий;
4) результатам предыдущих пересмотров;
5) характеристикам процесса и соответствию Политики
6) изменениям, которые могут повлиять на подход Общества к управлению ИБ, включая изменения в законодательстве Республики Казахстан, организационной среде, деловой ситуации, наличии ресурсов, договорных, регулятивных или юридических условиях, или в технической среде;

7) тенденции, связанные с угрозами и уязвимостями;
8) сообщённым инцидентам ИБ;
9) рекомендациям, представленным соответствующими учреждениями.

42. Выходные данные из пересмотра управления должны включать любые решения и действия, связанные с:

1) усовершенствованием подхода Общества к управлению ИБ и его процессами;
2) усовершенствованием целей и мер контроля;
3) улучшением распределения ресурсов и(или) обязанностей.

43. Пересмотр управления ИБ необходимо регистрировать.

44. Политика должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности, адекватности и эффективности управления ИБ.

45. Политика должна пересматриваться не реже одного раза в два года.

46. Пересмотренная Политика должна утверждаться Советом Директоров Общества.

14. Структура документации, регламентирующая обеспечение ИБ

47. Документация, регламентирующая обеспечение ИБ в Обществе делится на следующие уровни:

1) Политика, устанавливает основные принципы обеспечения ИБ Общества, является методологической основой при разработке документов нижних уровней;
2) правила и положения, устанавливают порядок осуществления ИБ, отражающий взаимодействие структурных подразделений Общества между собой и сторонними организациями, и детализирующие требования Политики;
3) инструкции и регламенты, определяющие вопросы осуществления ИБ в отдельных сферах деятельности Общества или описывающие процессы и процедуры обеспечения ИБ;
4) рабочие формы, применение которых является подтверждением проводимой работы в части обеспечения ИБ Общества (приказы, заявки, журналы, реестры, планы, отчеты и т.д.).

15. Ответственность

48. Ответственность за анализ эффективности реализации Политики и контроль соблюдения ее требований несет менеджер по ИБ.

49. Планирование и контроль за ИБ в Обществе несёт менеджер по ИБ.

50. В случае нарушения требований настоящей Политики все пользователи и контрагенты Общества несут ответственность в соответствии с действующим законодательством Республики Казахстан.