«Қазақстан темір жолы»
ұлттық компаниясы» акционерлік қоғамы

Акционерное общество
«Национальная компания «Қазақстан темір жолы»

Утверждена
решением Правления
акционерного общества
«Национальная компания
«Қазақстан темір жолы»
от 17 апреля 2023 года № 02/10
вопрос № 8

Политика информационной безопасности акционерного общества «Национальная компания «Қазақстан темір жолы»

Версия 4.0

Группа документов:	Основополагающая документация
Разработчик:	Служба корпоративной безопасности
Ответственный за анализ и актуализацию документа:	Служба корпоративной безопасности

Астана 2023

Содержание

1 Общие положения

1. Настоящая Политика информационной безопасности акционерного общества «Национальная компания «Қазақстан темір жолы» (далее - Политика) разработана в соответствии с требованиями международного стандарта ISO 27001:2013 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью - Требования».

2. Политика является внутренним документом акционерного общества «Национальная компания «Қазақстан темір жолы» (далее – АО «НК «ҚТЖ»).

3. Действие настоящей Политики распространяется на группу компаний АО «НК «ҚТЖ» (акционерное общество «Национальная компания «Қазақстан темір жолы») и его дочерние организации (далее – ДО), сто процентов голосующих акций (долей участия) которых прямо принадлежат АО «НК «ҚТЖ» на праве собственности или доверительного управления и сторонние организации (в рамках заключенных договоров), действующие в интересах группы компаний АО «НК «ҚТЖ».

4. Руководство АО «НК «ҚТЖ» осознает важность и осуществляет управление информационной безопасностью, обеспечивая необходимые условия развития, совершенствования мер и средств защиты информационных активов в контексте угроз информационной безопасности, развития законодательства и норм регулирования деятельности АО «НК «ҚТЖ».

5. АО «НК «ҚТЖ» является транспортно-логистической компанией государственного значения, входящей в состав активов Акционерного общества «Самрук-Қазына». Осуществление указанной деятельности связано с управлением информацией, в том числе передаваемой государством, являющейся важным активом АО «НК «ҚТЖ» и зависит от обеспечения информационной безопасности, под которой понимается конфиденциальность, целостность и доступность активов согласно Правилам идентификации, классификации и маркировки активов, связанных со средствами обработки информации, утвержденных отдельным локальным актом.

6. АО «НК «ҚТЖ» уделяет особое внимание вопросам обеспечения информационной безопасности, постоянно совершенствует систему управления информационной безопасностью (далее - СУИБ), применяемые средства и способы защиты от угроз информационной безопасности, а также осуществляет непрерывное обучение работников АО «НК «ҚТЖ» для поддержания компетенции в области защиты информации на высоком уровне.

7. СУИБ является частью системы управления АО «НК «ҚТЖ». Положения Политики учитывают ожидания всех заинтересованных сторон и обязательны для исполнения всеми работниками АО «НК «ҚТЖ» и ДО в процессе формирования портфеля инвестиционных проектов, а также доводятся до сведения клиентов и иных третьих лиц, имеющих доступ к информационным

системам и документам АО «НК «ҚТЖ», в той части, которая непосредственно взаимосвязана с АО «НК «ҚТЖ» и ее деятельностью.

8. Политика предусматривает основные цели, принципы и требования по защите информации.

9. Политика разработана в соответствии с законодательством Республики Казахстан по вопросам использования информационных систем и информационной безопасности, а также требованиями международных стандартов управления информационной безопасности.

10. Политика охватывает все информационные системы и документы, владельцем и пользователем которых является АО «НК «ҚТЖ» и ДО. Обеспечение информационной безопасности является необходимым условием для осуществления деятельности АО «НК «ҚТЖ».

2 Цели, требования и основные принципы

11. Основной целью Политики является минимизация ущерба от событий, представляющих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

12. В основе СУИБ предусмотрен риск-ориентированный подход, направленный на снижение вероятности реализации событий информационной безопасности.

13. Обеспечение информационной безопасности необходимо для снижения рисков и экономических потерь, связанных с различными угрозами имеющимся информационным ресурсам АО «НК «ҚТЖ» и ДО. С этой целью необходимо поддерживать главные свойства информации, а именно:

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

2) конфиденциальность – свойство, указывающее, что доступ к информации может иметь только ограниченный круг лиц, определенный её владельцами;

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

14. В целях обеспечения достаточно надежной системы информационной безопасности, необходима постоянная переоценка 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 этой связи, определяются следующие этапы цикла управления информационной безопасности:

1) планирование (разработка) – анализ рисков, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии со Стратегией развития АО «НК «ҚТЖ» до 2029 года, утвержденной решением Совета директоров АО «НК «ҚТЖ» от 6 сентября 2019 года (протокол №13);

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

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

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

15. Построение системы обеспечения информационной безопасности АО «НК «ҚТЖ» и ДО, а также ее функционирование должны осуществляться в соответствии со следующими принципами:

1) законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются в рамках законодательства Республики Казахстан, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации АО «НК «ҚТЖ и ДО»;

2) ориентированность на бизнес – информационной безопасности рассматривается, как процесс поддержки основной деятельности. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьёзных препятствий деятельности АО «НК «ҚТЖ» и ДО;

3) непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты АО «НК «ҚТЖ» и ДО должны осуществляться без прерывания или остановки текущих бизнес-процессов АО «НК «ҚТЖ» и ДО;

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

5) обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам.

Во всех случаях стоимость мер и систем информационной безопасности должна быть меньше размера возможного ущерба от любых видов риска.

6) приоритетность – категорирование (ранжирование) всех информационных ресурсов АО «НК «ҚТЖ» и ДО по степени важности при оценке реальных, а также потенциальных угроз информационной безопасности;

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 информационной безопасности должны осуществляться профессионально подготовленными специалистами;

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

10) взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений АО «НК «ҚТЖ» и ДО, 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 – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

3 Объекты защиты

16. Основными объектами защиты обеспечения информационной безопасности в АО «НК «ҚТЖ» и ДО являются следующие элементы:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и локальными актами АО «НК «ҚТЖ» и ДО к коммерческой, служебной или иной охраняемой законом тайне, в том числе информационные ресурсы, входящие в проекты программ «Цифровая железная дорога» и программы Трансформации в АО «НК «ҚТЖ» (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) автоматизированных систем АО «НК «ҚТЖ» и ДО, с помощью которых производится обработка защищаемой информации;

4) процессы АО «НК «ҚТЖ» и ДО, связанные с управлением и использованием информационных ресурсов;

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

6) рабочие помещения и кабинеты работников АО «НК «ҚТЖ» и ДО, помещения АО «НК «ҚТЖ» и ДО, предназначенные для ведения закрытых переговоров и совещаний;

7) работники АО «НК «ҚТЖ» и ДО, имеющие доступ к защищаемой информации;

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

9) виртуальные среды (вычислительные ресурсы или их логическое объединение, абстрагированное от аппаратной реализации, обеспечивающие логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе) при использовании серверной инфраструктуры.

17. Защищаемая информация может:

1) размещаться на бумажных носителях;

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

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

4) присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

4 Угрозы информационной безопасности

18. Под угрозами информационной безопасности понимается потенциально возможное событие, процесс или явление, которые посредством воздействия на информацию или компоненты информационной системы, или ресурса могут прямо или косвенно привести к нанесению ущерба интересам владельцев и пользователей.

19. Угрозы информационной безопасности подразделяются на:

1) случайные, которые могут быть обусловлены следующими факторами:

стихийные бедствия;

ошибки по невниманию;

ошибки аппаратных и программных средств;

низкая осведомленность работников в области информационной безопасности;

недостаточное физическое обеспечение периметра информационной безопасности;

2) преднамеренные, которые могут быть обусловлены следующими факторами:

фальсификация или уничтожение данных;

неправомерное использование данных;

неправомерный доступ к информации;

компьютерные атаки (целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно-аппаратных средств, или протоколов межсетевых взаимодействия);

20. К числу угроз информационной безопасности АО «НК «ҚТЖ» и ДО относятся (но не ограничены ими):

1) утрата защищаемой информации;

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

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

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

5) недоступность информации в результате ее блокирования, сбоя оборудования, систем управления баз данных, распределённых вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств, и злонамеренных действий.

21. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности АО «НК «ҚТЖ» и ДО на нормальное функционирование:

1) чрезвычайные происшествия, связанные с безопасностью движения;

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 АО «НК «ҚТЖ» и ДО потери, связанные с невозможностью выполнения своих обязательств;

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

6) ущерб от отсутствия у руководства АО «НК «ҚТЖ» и ДО объективной информации;

7) ущерб, нанесённый репутации АО «НК «ҚТЖ» и ДО;

8) иной вид ущерба.

Для проведения идентификации угроз информационной безопасности, определения вероятности реализации угроз информационной безопасности, необходимо руководствоваться Методикой оценки рисков информационной безопасности по группе компаний АО «НК «ҚТЖ», утвержденной отдельным локальным актом.

5 Меры обеспечения информационной безопасности

22. Основными мерами по обеспечению информационной безопасности АО «НК «ҚТЖ» и ДО являются:

1) административно-правовые и организационные меры;

2) меры физической безопасности;

3) программно-технические меры.

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

1) контроль исполнения требований законодательства РК и внутренних документов АО «НК «ҚТЖ» и ДО;

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

3) контроль соответствия бизнес-процессов АО «НК «ҚТЖ» и ДО требованиям Политики;

4) информирование и обучение работников АО «НК «ҚТЖ» и ДО работе с информационными системами и требованиям информационной безопасности;

5) реагирование на каналы несанкционированной утечки информации, инциденты, связанные с этим, локализацию и минимизацию последствий;

6) анализ новых рисков информационной безопасности;

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

8) определение действий при возникновении чрезвычайных ситуаций;

9) проведение профилактических мер при приеме на работу и увольнении работников АО «НК «ҚТЖ»;

10) мероприятия по контролю правомерности использования ПО.

24. 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 АО «НК «ҚТЖ» и ДО в режимные помещения и помещения ограниченного доступа.

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

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

2) использование средств защиты периметра (firewall, IPS и т.п.);

3) применение комплексной антивирусной защиты;

4) использование средств информационной безопасности, встроенных в информационные системы;

5) обеспечение регулярного резервного копирования информации;

6) контроль за правами и действиями пользователей, в первую очередь, привилегированных;

7) применение средств криптографической защиты информации в порядке, установленном нормативными правовыми актами;

8) обеспечение безотказной работы аппаратных средств;

9) мониторинг состояния критичных элементов информационной системы.

6 Ответственность и соответствие требованиям законодательства

26. В АО «НК «ҚТЖ» и ДО внедрены соответствующие процессы для обеспечения соблюдения требований нормативных правовых актов, соблюдения прав интеллектуальной собственности, защиты охраняемой законом персональной информации, соблюдения ограничений по использованию криптографических средств.

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

28. При разработке и применении средств и методов информационной безопасности учитываются требования договорных обязательств и контрактов, заключенных АО «НК «ҚТЖ» и ДО с третьими сторонами.

29. Доступ третьей стороны к информационным ресурсам АО «НК «ҚТЖ» и ДО осуществляются только после анализа рисков, которые могут возникнуть при предоставлении такого доступа, и принятия адекватных защитных мер. В случае необходимости (в частности, при наличии требований нормативных правовых актов или международных стандартов), АО «НК «ҚТЖ» и ДО проводит проверку контрагентов (поставщиков товаров и услуг) на соответствие определенным требованиям.

30. На основании Политики разрабатываются локальные акты, регламентирующие порядок и методы обеспечения информационной безопасности, стандартов и т.п.

31.Ответственность за соблюдение настоящей Политики возлагается на работников АО «НК «ҚТЖ» и ДО.

7 Пересмотр Политики

32. Политика пересматривается по мере необходимости, но не реже одного раза в 24 месяца.