ҚАЗАҚСТАН ХАЛЫҚ БАНКІНІҢ ЕНШІЛЕС ҰЙЫМЫ
HALYK
KAZTELEPORT
ДОЧЕРНЯЯ ОРГАНИЗАЦИЯ НАРОДНОГО БАНКА КАЗАХСТАНА

УТВЕРЖДЕНА
решением Совета Директоров АО «Казтелепорт»
Протокол № 28 от 20.06. 2025 года

Политика информационной безопасности АО «Казтелепорт»

Разработчик:	Департамент информационной безопасности
Бизнес-владелец:	Департамент информационной безопасности

г. Алматы, 2025 г.

Содержание

Глава 1. Общие положения

1. Политика информационной безопасности АО «Казтелепорт» (далее – Политика ИБ) определяет требования к организации информационной безопасности АО «Казтелепорт» и устанавливает цели, задачи и принципы в области информационной безопасности, которыми руководствуется АО «Казтелепорт» (далее – Компания) в своей деятельности.
2. Под информационной безопасностью или защитой информационных активов понимается принятие и выполнение необходимых мер от случайного или преднамеренного изменения, раскрытия или уничтожения информационных активов, а также обеспечение их конфиденциальности, целостности и доступности.
3. Успешная деятельность Компании напрямую зависит от уверенности клиентов в том, что оказываемые им услуги не нарушают их информационную безопасность, поэтому обеспечение информационной безопасности Компании и ее клиентов является ключевым видом деятельности для целей существования Компании.
4. Политика ИБ разработана с учётом требований и рекомендаций:
   1) СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»;
   2) СТ РК ISO/IEC 27002-2023 – «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью»;
   3) СТ РК ISO/IEC 27005-2022 – «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности»;
   4) Правил обеспечения информационной безопасности в Группе Халык.

Глава 2. Термины и сокращения

5. В Политике ИБ используются следующие термины и сокращения:
   1) актив - что-либо, что имеет ценность для Компании;
   2) владелец актива - руководитель структурного подразделения / уполномоченное лицо, которое утверждено, как ответственное за производство, разработку, обслуживание, использование и безопасность активов. Термин «владелец» не означает, что человек действительно имеет право собственности на активы;
   3) бизнес-владелец информационного актива – владелец бизнес-процесса, для обеспечения жизненного цикла которого используется информационный актив;
   4) ВНД – внутренний нормативный документ;
   5) доступность - свойство, определяющее возможность предоставления и использования по запросу авторизованного субъекта;
   6) защищаемый доступ - комплекс правовых, организационных и технических мер, направленных на предотвращение неправомерного доступа к информационным активам Компании, включая незаконные действия по получению, копированию, распространению, искажению, уничтожению или блокированию информации;
   7) ИА - информационный актив - совокупность информации и информационной инфраструктуры, имеющей ценность для Компании;
   8) ИБ – информационная безопасность;

9) информация - сведения о ком-либо или о чем-либо независимо от формы их представления;

10) информационная инфраструктура - совокупность информационных систем, систем связи, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации;

11) контролируемый доступ - система наблюдения и проверки процесса функционирования и фактического состояния управляемого доступа;

12) конфиденциальность - свойство, определяющее, что информация не может быть доступна или раскрыта для неавторизованного лица, организации или процесса;

13) минимально необходимые права доступа - ограниченные права доступа, достаточные для выполнения определенных (поставленных) задач;

14) обработка риска - процесс выбора и реализации мер по изменению риска;

15) оценка рисков - оценка угроз, их последствий, уязвимости информации и средств ее обработки, а также вероятности их возникновения;

16) риск – влияние неопределённости на цели;

17) система менеджмента информационной безопасности (СМИБ) – часть общей системы менеджмента, основанная на подходе менеджмента рисков, для создания, внедрения, применения, мониторинга, анализа, поддержания и улучшения информационной безопасности;

18) СИТ - служба информационных технологий – подразделения/работники Компании, в обязанности которых входит разработка, внедрение, сопровождение и поддержка информационной инфраструктуры Компании, предоставление, изменение и аннулирование прав доступа, осуществление настроек информационной инфраструктуры Компании, в том числе обеспечивающих соответствие требованиям обеспечения информационной безопасности;

19) целостность - свойство, гарантирующее корректность и полноту активов;

20) ЦОД – центр обработки данных.

Глава 3. Цели и область применения Политики ИБ

6. Политика ИБ разработана с целью:

1) защиты информации Компании и ее клиентов от реальных и потенциальных угроз;

2) минимизации и локализации последствий при воздействии угроз;

3) создания и поддержания в актуальном состоянии СМИБ, обеспечивающей защиту информации, информационных активов и информационной инфраструктуры Компании от внешних и внутренних угроз информационной безопасности, реализация которых может привести к ущербу, и минимизацию ущерба в случае реализации этих угроз;

4) обеспечения соответствия СМИБ Компании требованиям стандарта СТ РК ISO/IEC 27001-2023 и получения/подтверждения соответствующего сертификата соответствия.

7. Политика ИБ разработана с учётом бизнес-целей Компании, внешних и внутренних факторов, имеющих отношение к деятельности Компании и оказывающих влияние на ее способность достигать ожидаемых результатов от СМИБ, требований заинтересованных сторон.

8. Областью применения СМИБ в Компании является менеджмент информационной безопасности при оказании услуг:

   1) телекоммуникационных;

   2) услуг центров обработки данных;

   3) услуг по монтажу и техническому обслуживанию структурированных кабельных сетей, систем видеонаблюдения, систем охранно-пожарной сигнализации, систем контроля доступа;

   4) услуг по информационной безопасности, в том числе в ЦОДах, и защиты периметра от внешних сетевых угроз;

   5) услуг по сопровождению программного обеспечения 1С Предприятие, в том числе услуг «Облачная 1С»;

   6) аутсорсинговых;

   7) услуг технического обслуживания систем гермозоны;

   8) реализации товаров и услуг;

   9) услуг технического обслуживания электрозарядных устройств.

9. Границами применения СМИБ являются все структурные подразделения Компании, ЦОДы, серверные Компании, размещенные в г. Алматы, г.Актау и г. Астана.

10. Политика ИБ обязательна для исполнения всеми сотрудниками Компании, служебные функции которых входят в область применения и границы СМИБ.

11. Политика ИБ является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

Глава 4. Задачи по достижению целей Политики ИБ

12. Цели Политики ИБ достигаются посредством обеспечения и постоянного поддержания следующих задач:

   1) создание организационной структуры, которая будет обеспечивать работоспособность СМИБ;

   2) разработка ВНД для обеспечения четкого управления и поддержки Политики ИБ со стороны Руководства Компании;

   3) обеспечение управляемого, защищаемого и контролируемого доступа к активам Компании;

   4) проведение регулярной оценки и анализа рисков информационной безопасности и разработка мер по их снижению в соответствии с СТ РК ISO/IEC 27005-2022;

   5) предотвращение событий, которые могут повлиять на непрерывность бизнеса, и разработка предупреждающих мер;

   6) разработка и внедрение системы управления инцидентами ИБ.

Глава 5. Принципы Политики ИБ

13. Для достижения поставленных целей и при выполнении задач Компания намерена руководствоваться следующими принципами:

   1) **Соответствие законодательным и иным принятым на себя обязательствам.** Реализация мер обеспечения информационной безопасности осуществляется в строгом соответствии с действующим законодательством Республики Казахстан,

требованиями акционера – АО «Народный Банк Казахстана» и договорными обязательствами;

2) **Управление процессом обеспечения информационной безопасности Руководством Компании.** Деятельность по обеспечению информационной безопасности инициирована и контролируется Председателем Правления Компании. Координация деятельности по обеспечению информационной безопасности осуществляется ответственным за СМИБ, который назначается приказом Председателем Правления Компании;

3) **Постоянное улучшение СМИБ.** Постоянное улучшение СМИБ, включая все необходимые процессы и их взаимодействие, в соответствии с требованиями СТ РК ISO/IEC 27001-2023. Информацию о возможностях улучшения Компания получает из:

   a) результатов мониторинга СМИБ;

   b) результатов аудитов;

   c) анализа СМИБ со стороны руководства.

   На основании полученной информации актуализируются Цели ИБ и разрабатываются необходимые мероприятия по их реализации;

4) **Управление рисками.** Управление рисками информационной безопасности выражается в поддержке регулярной деятельности по следующим направлениям:

   a) идентификация активов, подлежащих защите, и определение «владельцев» этих активов;

   b) своевременное выявление и прогнозирование угроз информационной безопасности в отношении идентифицированных активов;

   c) оценка и обработка рисков информационной безопасности;

   d) оценка эффективности применяемых методов и средств обеспечения информационной безопасности, в том числе с привлечением внутренних и внешних аудиторов;

5) **Согласованность действий.** Действия по обеспечению информационной и физической безопасности осуществляются на основе четкого взаимодействия подразделений Компании и согласованы между собой по целям, задачам, принципам, методам и средствам;

6) **Экономическая целесообразность.** Выбор мер обеспечения информационной безопасности осуществляется с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации;

7) **Управление персоналом.** Тщательный подбор персонала (работников), выработка и поддержание корпоративной этики, создающей благоприятную среду для деятельности Компании и снижения рисков информационной безопасности;

8) **Документированность требований информационной безопасности.** Все требования информационной безопасности фиксируются во внутренних нормативных документах, которые утверждаются уполномоченными органами / лицами Компании;

9) **Осведомленность в вопросах обеспечения информационной безопасности.** Документированные требования в области информационной безопасности доводятся до сведения всех работников Компании и контрагентов в части, их

касающейся. Компания на периодической основе осуществляет информирование и обучение работников вопросам обеспечения информационной безопасности;

10) **Управление изменениями конфигураций.** С целью предотвращения системных сбоев и инцидентов информационной безопасности все действия по изменению конфигураций в средствах и системах обработки информации надлежащим образом контролируются и документируются;

11) **Реагирование на инциденты информационной безопасности.** Выявление, регистрация и оперативное реагирование на действительные, предпринимаемые и вероятные нарушения информационной безопасности;

12) **Персональная ответственность.** Требования по соблюдению информационной безопасности устанавливаются ВНД Компании. Обязанности по соблюдению требований информационной безопасности включаются в трудовые договоры и должностные инструкции работников. За неисполнение или ненадлежащее исполнение обязанностей по обеспечению и соблюдению требований информационной безопасности на работников могут налагаться дисциплинарные взыскания в порядке, предусмотренном Трудовым кодексом Республики Казахстан и ВНД Компании;

13) **Предоставление минимально необходимых прав доступа.** Работникам Компании и контрагентам предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств;

14) **Регулярность проведения аудитов информационной безопасности.** Проведение аудитов с периодичностью не реже одного раза в год выполняется для проверки действенности политик и других внутренних нормативных документов Компании, касающихся информационной безопасности. По итогам аудитов могут быть актуализированы цели и задачи в отношении информационной безопасности Компании;

15) **Учет требований информационной безопасности в проектной деятельности.** Требования информационной безопасности учитываются в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации;

16) **Применение процедур дисциплинарной практики.** За неумышленное и умышленное невыполнение требований внутренних документов СМИБ, к персоналу применяются процедуры дисциплинарной ответственности в соответствии с законодательством Республики Казахстан. Данный принцип в обязательном порядке доводится до всего персонала Компании.

Глава 6. Реализация принципов Политики ИБ

14. Принципы Политики ИБ реализуются посредством:

1) применения средств управления, утверждаемых и вводимых в действие решением Правления АО «Казтелепорт»;

2) тематических политик, входящих в структуру Политики ИБ Компании, в том числе, но не ограничиваясь:

a) Политика управления доступом;

b) Политика сетевой безопасности;

c) Политика передачи информации;

d) Политика в отношении мобильных конечных устройств и удаленной работы;

e) Политика физической безопасности;

f) Политика использования криптографии;

g) Политика чистого стола и чистого экрана;

h) Политика информационной безопасности для отношений с поставщиками;

i) Политика резервного копирования;

j) Политика управления изменениями.

15. **Политика управления доступом.**
Цель политики - обеспечить доступ персонала только к тем информационным активам, которые необходимы для выполнения служебных обязанностей.

16. **Политика сетевой безопасности.**
Цель политики - обезопасить сетевые сервисы от несанкционированного доступа персонала и посторонних лиц.

17. **Политика передачи информации.**
Цель политики - обеспечить безопасности информации, передаваемой внутри Компании и любой внешней заинтересованной стороне.

18. **Политика в отношении мобильных конечных устройств и удаленной работы.**
Цель политики - защита информации от рисков, возникающих при использовании мобильных устройств и при удаленной работе персонала.

19. **Политика физической безопасности;**
Цель политики - предотвращение несанкционированного физического доступа, повреждения и перемещения информации и других связанных с ней активов.

20. **Политика использования криптографии.**
Цель политики – обеспечить надлежащее и эффективное использование криптографии для защиты конфиденциальности, подлинности или целостности информации в соответствии с требованиями бизнеса и информационной безопасности, а также с учетом юридических, законодательных, нормативных и договорных требований, связанных с криптографией.

21. **Политика чистого стола и чистого экрана.**
Цель политики – исключить риски несанкционированного доступа, потери и повреждения информации на столах, экранах и в других доступных местах в рабочее и нерабочее время.

22. **Политика информационной безопасности для отношений с поставщиками.**
Цель политики – поддерживать согласованный уровень информационной безопасности в отношениях с поставщиками.

23. **Политика резервного копирования.**
Цель политики - обеспечение возможности восстановления после потери данных или систем.

24. **Политика управления изменениями.**
Цель политики – организация процесса управления изменениями, гарантирующего обеспечение конфиденциальности, целостности и доступности информации в средствах обработки информации и информационных системах в течение всего жизненного цикла системы, начиная с ранних этапов проектирования и заканчивая всеми последующими усилиями по обслуживанию.

25. Для реализации тематических политик разрабатываются и вводятся в действие соответствующие ВНД Компании.

Глава 7. Угрозы информационной безопасности

26. Под угрозами ИБ понимается совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности.
27. Угрозы ИБ подразделяются на:
    1) случайные – стихийные бедствия (природные источники угроз – землетрясение, пожары, осадки, наводнения и т.д.), непреднамеренные ошибочные действия со стороны работников Компании и третьих лиц, взаимодействующих с информационными активами Компании, ошибки аппаратных и программных средств и т.д.;
    2) преднамеренные, т.е. умышленная фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.
28. К числу угроз ИБ относятся (но не ограничены ими):
    1) утрата информации, составляющей коммерческую тайну Компании и иную охраняемую законом информацию;
    2) искажение (несанкционированная модификация, подделка) защищаемой информации;
    3) утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение, передача и т.д.);
    4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);
    5) недоступность информации в результате ее блокирования, отказа и сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств и злонамеренных действий.
29. В результате реализации указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Компании и ее нормальное функционирование:
    1) финансовые потери, связанные с утечкой, разглашением или несанкционированной модификацией защищаемой информации;
    2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;
    3) финансовые потери, связанные с несанкционированными действиями в информационных ресурсах Компании;
    4) ущерб от дезорганизации деятельности Компании, финансовые и репутационные потери, связанные с невозможностью выполнения Компанией своих обязательств;
    5) ущерб от принятия управленческих решений на основе необъективной информации;
    6) ущерб от отсутствия у руководства Компании объективной информации;
    7) ущерб, нанесенный репутации Компании;
    8) иные виды ущерба.

Глава 8. Модели вероятного нарушителя

30. В Компании принята следующая классификация моделей вероятных нарушителей ИБ:
    1) внутренние нарушители – работники Компании, неосознанно либо злонамеренно нарушающие режим ИБ;

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

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

32. Основные типы внутренних нарушителей:

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

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

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

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

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

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

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

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

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

3) «Elite hacker», или «Гуру» – высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае будет нацелен на проведение финансового мошенничества, во втором – либо на утечку информации,

либо на недоступность серверов и компрометацию Компании в глазах клиентов. В арсенале имеет полный спектр специального программно-технического обеспечения, а также использует методы социальной инженерии;

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

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

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

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

Глава 9. Участники СМИБ, их полномочия и ответственность

34. Совет Директоров Компании утверждает настоящую Политику ИБ, изменения и дополнения в нее, а также утверждает Правила определения коммерческой тайны Компании и Перечень сведений, составляющих коммерческую тайну Компании.

35. Председатель Правления Компании несет ответственность за реализацию настоящей Политики ИБ.

36. Правление Компании обеспечивает достаточность ресурсов для разработки, внедрения, эксплуатации, сопровождения и совершенствования СМИБ, определяет полномочия и ответственность подразделений и работников в области ИБ.

37. Подразделение информационной безопасности осуществляет планирование мероприятий по реализации положений настоящей Политики ИБ, координирует и контролирует деятельность функциональных блоков и структурных подразделений Компании по обеспечению ИБ, по созданию, внедрению и поддержанию СМИБ, несет ответственность за достижение поставленных целей СМИБ.

38. Руководители функциональных блоков, структурных подразделений, работники Компании несут ответственность за безусловное полное выполнение своих обязанностей по обеспечению информационной безопасности в соответствии с настоящей Политикой ИБ и ВНД Компании.

39. Ответственность за несоблюдение информационной безопасности в Компании, а также за невыполнение положений настоящей Политики ИБ несет каждый сотрудник Компании в соответствии с действующим законодательством Республики Казахстан и ВНД Компании.

40. Ответственность за поддержание Политики ИБ в актуальном состоянии несет подразделение информационной безопасности.

Глава 10. Заключительные положения

41. Пересмотр настоящей Политики ИБ осуществляется по мере необходимости, но не реже одного раза в пять лет. Пересмотр осуществляется на основе результатов анализа СМИБ со стороны руководства Компании.
42. Политика ИБ размещается на официальном веб-сайте Компании и доступна для всех заинтересованных лиц.
43. Политика ИБ доводится до персонала Компании, должна быть им понята и принята для исполнения.