

УТВЕРЖДЕНА  
решением Совета Директоров АО «Казтелепорт»  
Протокол № 20 от 24 июня 2021 года

**Политика системы менеджмента информационной безопасности  
АО «Казтелепорт»**

(с изменениями от 02 сентября 2022г.  
(протокол заочного заседания Совета Директоров АО «Казтелепорт» №34)

Разработчик:	Управление информационной безопасности
Бизнес-владелец:	Управление защиты ресурсов ЦОД

г. Алматы, 2021 г.

## Содержание

Глава 1. Общие положения .....	3
Глава 2. Термины и сокращения .....	3
Глава 3. Цели и область применения СМИБ .....	4
Глава 4. Задачи по достижению целей Политики СМИБ .....	5
Глава 5. Принципы Политики СМИБ .....	5
Глава 6. Реализация принципов политики СМИБ .....	7
Глава 7. Ответственность .....	12
Глава 8. Заключительные положения.....	12

## Глава 1. Общие положения

1. Политика системы менеджмента информационной безопасности АО «Казтелепорт» (далее – Политика СМИБ) определяет требования к организации системы менеджмента информационной безопасности АО «Казтелепорт» и устанавливает цели, задачи и принципы в области менеджмента информационной безопасности, которыми руководствуется АО «Казтелепорт» в своей деятельности, разработана в соответствии с требованиями пункта 5.2 СТ РК ИСО/МЭК 27001-2015.
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. Политика СМИБ разработана с учётом требований:
  - 1) СТ РК ISO/IEC 27001-2015 «Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности – Требования»;
  - 2) СТ РК ISO/IEC 27002:2015 – «Информационные технологии – Методы защиты – Свод рекомендуемых правил для управления информационной безопасностью»;
  - 3) СТ РК ISO/IEC 27005:2013 – «Информационные технологии – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности»;
  - 4) Концепции информационной безопасности АО «Казтелепорт», утвержденной решением Совета директоров АО «Казтелепорт» (Протокол №20 от 24 июня 2021г.).

## Глава 2. Термины и сокращения

4. В Политике СМИБ 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<sup>1</sup> – владелец основного 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;

---

<sup>1</sup> Постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 23 ноября 2020 года № 111 Об утверждении Методики оценки рисков информационной безопасности, включая порядок ранжирования финансовых организаций по степени подверженности рискам информационной безопасности

- 8) информация - сведения о ком-либо или о чем-либо независимо от формы их представления;
- 9) информационная инфраструктура - совокупность информационных систем, систем связи, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации;
- 10) Компания – АО «Казтелепорт»;
- 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) угроза - потенциальная причина инцидента, который может нанести ущерб информационной инфраструктуре Компании или Компании в целом;
- 21) [УЗРЦОД – Управление защиты ресурсов ЦОД](#).

### **Глава 3. Цели и область применения СМИБ**

5. Политика СМИБ разработана с целью:
  - 1) создания системы обеспечения защиты информации, информационных ресурсов и информационной инфраструктуры Компании от внешних и внутренних угроз информационной безопасности, реализация которых может привести к ущербу, и его минимизации в случае реализации этих угроз;
  - 2) подготовки к оценке соответствия СМИБ Компании и получению сертификата на соответствие требованиям стандарта СТ РК ИСО/МЭК 27001-2015.
6. Политика СМИБ разработана с учётом организационной среды Компании, требований и пожеланий заинтересованных сторон.
7. Областью применения СМИБ в Компании является менеджмент информационной безопасности при оказании услуг:
  - 1) телекоммуникационных;

- 2) услуг центров обработки данных (ЦОД);
  - 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 технической поддержке устройств самообслуживания, технической поддержки платёжных терминалов;~~
  - 6) услуг по сопровождению программного обеспечения 1С Предприятие, в том числе услуг «Облачная 1С»;
  - 7) аутсорсинговых;
  - 8) услуг технического обслуживания систем гермозоны;
  - 9) реализации товаров и услуг.
8. Границами применения СМИБ являются все структурные подразделения Компании, гермозоны Компании, размещенные в г. Алматы и г. Нур-Султан.
9. Политика СМИБ обязательна для исполнения всеми сотрудниками Компании, служебные функции которых входят в область применения и границы СМИБ.
10. Политика СМИБ является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

#### Глава 4. Задачи по достижению целей Политики СМИБ

11. Цели Политики СМИБ достигаются посредством обеспечения и постоянного поддержания следующих задач:
- 1) создание организационной структуры, которая будет обеспечивать работоспособность системы информационной безопасности;
  - 2) разработка ВНД для обеспечения четкого управления и поддержки Политики СМИБ 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 27005:2013;
  - 5) предотвращение событий, которые могут повлиять на непрерывность бизнеса и разработка предупреждающих мер;
  - 6) разработка и внедрение системы управления инцидентами.

#### Глава 5. Принципы Политики СМИБ

12. Для достижения поставленных целей и при выполнении задач Компания намерена руководствоваться следующими принципами:
- 1) **Постоянное улучшение СМИБ.** 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 СМИБ и разрабатываются необходимые мероприятия по их реализации;

- 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 по СМИБ, который назначается приказом Председателем Правления Компании;
- 3) **Соответствие законодательным и иным принятым на себя обязательствам.** Компания реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством Республики Казахстан, требованиями акционера – АО «Народный Банк Казахстана» и договорными обязательствами;
- 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.** Компания стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации;
- 7) **Управление персоналом.** Компания стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности Компании и снижает риски информационной безопасности;
- 8) **Документированность требований информационной безопасности.** Компания стремится, чтобы все требования информационной безопасности были зафиксированы во внутренних нормативных документах и утверждены Правлением Компании. Система менеджмента информационной безопасности в Компании строится на основе требований стандарта СТ РК ISO/МЭК 27001:2015;
- 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 нарушения информационной безопасности, Компания

стремится надлежащим образом контролировать и документировать действия по изменению конфигураций в средствах и системах обработки информации;

- 11) **Реагирование на инциденты информационной безопасности.** Компания стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности;
- 12) **Персональная ответственность.** Требования по соблюдению информационной безопасности устанавливаются внутренними нормативными документами. 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.** Помимо повседневной (операционной) деятельности, Компания стремится учитывать требования информационной безопасности 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 доведён до персонала Компании.

#### **Глава 6. Реализация принципов политики СМИБ**

13. Принципы Политики СМИБ реализуются посредством:

- 1) Политики информационной безопасности, утверждаемой и вводимой в действие решением Совета Директоров АО «Казтелепорт»;
- 2) применения средств управления, утверждаемых и вводимых в действие решением Правления АО «Казтелепорт»;
- 3) частных политик, входящих в структуру Политики СМИБ Компании и требуемых СТ РК ИСО/МЭК 27001-2015:
  - a) Политика управления доступом;
  - b) Политика использования сетевых сервисов;
  - c) Политика мобильных вычислений и коммуникаций, дистанционной работы;
  - d) Политика использования средств криптографической защиты информации;

- e) Политика резервного копирования;
- f) Политика «Чистого стола» и «Чистого экрана»;
- g) Политика управления изменениями.

**14. Политика управления доступом.**

Цель политики - обеспечить доступ персонала только к тем информационным активам, которые необходимы для выполнения служебных обязанностей.

Требования политики:

- 1) Управление доступом осуществляется на основании формализованного и утвержденного процесса, с учетом обеспечения требований безопасности, нормативных и договорных требований. Доступ персоналу предоставляется в пределах необходимых для выполнения возложенных на них функций;
- 2) Все сотрудники должны авторизоваться перед получением доступа к ресурсам Компании;
- 3) Сотрудники не должны иметь прав на удаление объектов других пользователей в каталогах общего доступа;
- 4) Доступ уровня администратора домена могут иметь только специально назначенные работники Компании;
- 5) Предоставление прав доступа и изменение прав доступа осуществляет СИТ.

**15. Политика использования сетевых сервисов.**

Цель политики - обезопасить сетевые сервисы от несанкционированного доступа персонала и посторонних лиц.

Требования политики:

- 1) Использование сетевых сервисов осуществляется на основании формализованного и утвержденного процесса, с учетом обеспечения требований безопасности, нормативных и договорных требований;
- 2) В Компании разрешен доступ в корпоративную сеть из-за пределов периметра сети и работа в дистанционном режиме;
- 3) Важные сетевые узлы корпоративной сети Компании должны вести протоколы событий. Протоколы должны регулярно анализироваться СИТ на наличие уязвимостей;
- 4) Физическая и логическая конфигурация корпоративной сети, должна быть документирована. Документирование и актуализацию осуществляет СИТ;
- 5) Защита сетевого периметра осуществляется техническими и организационными методами. Выбор методов и средств обеспечения сетевой безопасности осуществляет СИТ.

**16. Политика мобильных вычислений и коммуникаций, дистанционной работы.**

Цель политики - устранить возможную утечку информации и угрозы сетевым сервисам через мобильные устройства персонала и при использовании удаленного доступа.

В Компании разрешено использование мобильных устройств (в том числе личных) и режима дистанционной работы с информационными активами Компании, при этом должны выполняться следующие требования:

- 1) Мобильное устройство должно быть защищено паролем;
- 2) Сотрудник Компании, использующий личное мобильное устройство, даёт согласие на блокировку мобильного устройства в случае его потери;



- 3) Осуществляется двухфакторная аутентификация пользователя;
- 4) Удаленный доступ должен предоставляться с использованием технологии VPN (Virtual Private Network);
- 5) На всех стационарных и мобильных устройствах, подключаемых посредством удаленного доступа к информационным ресурсам Компании, в обязательном порядке устанавливается специальное программное обеспечение, выполняющее в том числе и функции межсетевое экрана и антивирусной защиты.

**17. Политика использования средств криптографической защиты информации.**

Цель политики – обеспечить безопасное использование криптографических средств защиты.

Требования политики:

- 1) Криптографические ключи должны быть персонифицированы;
- 2) Сотрудники Компании допускаются к работе со средствами криптографической защиты информации только после прохождения инструктажа по мерам безопасности при работе с криптографическими ключами в СИТ;
- 3) Сотрудники Компании, владеющие криптографическими ключами средств защиты информации, должны ограничить доступ к ключам посторонних лиц;
- 4) Категорически запрещается:
  - a) использовать внешний носитель ключа не по назначению;
  - b) выводить ключевую информацию на экран монитора или принтер;
  - c) преднамеренно вносить изменения в ключи;
  - d) снимать несанкционированные копии ключей;
  - e) разглашать данные в отношении ключей и/или порядка их хранения, а также передавать ключи лицам, не имеющим права их использования;
  - f) записывать постороннюю информацию на внешний носитель ключей.

**18. Политика «Чистого стола» и «Чистого экрана».**

Цель политики – исключить утечку информации из-за ненадлежащего хранения документов, содержащих конфиденциальные сведения и из-за бесконтрольного использования персональных компьютеров.

Требования политики:

- 1) Персоналу Компании запрещается оставлять в легкодоступных местах в свое отсутствие или в нерабочее время документы, содержащие конфиденциальные сведения;
- 2) В отсутствие сотрудника на своем рабочем месте или в нерабочее время все документы, содержащие конфиденциальные сведения, должны храниться в ящиках, шкафах, сейфах и/или других приспособлениях, исключающих возможность их визуального просмотра и/или доступа посторонними лицами;
- 3) Во время работы с конфиденциальной информацией в присутствии посторонних лиц, сотрудники обязаны предпринимать меры по защите от визуального просмотра и/или доступа к этим документам;
- 4) Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги;

- 5) Пользователям персональных компьютеров и серверов запрещается оставлять без присмотра разблокированный персональный компьютер, ноутбук или сервер. В случае отсутствия на рабочем месте, пользователи обязаны выйти из системы и/или активизировать системные средства защиты от несанкционированного доступа (временная блокировка экрана);
- 6) Пользователи перед уходом должны выключать все компьютеры, ноутбуки или сервера, которые не будут использоваться в нерабочее время;
- 7) Во время обработки конфиденциальной информации в присутствии посторонних лиц, пользователи обязаны предпринимать меры по защите экрана монитора от просмотра посторонними лицами;
- 8) Также, для предотвращения просмотра электронных документов посторонними лицами, пользователям запрещается сохранять электронные документы, содержащие конфиденциальные сведения, на «рабочем столе» персонального компьютера или сервера.

19. **Политика резервного копирования.**

Цель политики - обеспечение отказоустойчивости информационных активов за счет создания копии (резервное копирование или резервирование) информационных массивов и других необходимых данных и размещения ее в другом месте.

- 1) Резервирование обеспечивается применением системы резервного копирования, с указанием используемых инструментов проведения процедур резервирования, архивирования, хранения и восстановления информации с учетом выбранных способов, методов и типов:
  - a) Методы резервирования (холодное, горячее);
  - b) Типы резервирования (полный, инкрементальный, смешанный);
  - c) Способ резервирования (автоматический, ручной).
- 2) При построении системы резервного копирования определяются места хранения копий, соответствующих требованиям, предъявляемым к такого рода помещениям. Обеспечивается наличие в данном помещении соответствующей системы резервного копирования.
- 3) При проведении процедур резервирования обязательно выполнение следующих требований:
  - a) Определение количества дублирующих (одинаковых) копий и количества процедур последовательного создания и хранения копий информации, изменяющихся по содержанию со времени создания наиболее ранних копий;
  - b) Описание обозначения копий информации, подлежащих хранению;
  - c) Ведение «Журнала создания копий».
- 4) На всех этапах резервирования, архивирования, хранения и восстановления копий должен вестись мониторинг правильности выполнения процедур, в том числе должно проводиться периодическое тестовое восстановление информации, особенно архивной информации.
- 5) Должны быть указаны ответственные работники за процессы резервирования и восстановления с указанием наименований резервируемых данных. Необходимо обеспечить шифрование носителей информации при их транспортировке.
- 6) При администрировании системы резервного копирования необходимо регламентировать расписание и время, в течение которого непосредственно происходит создание резервных копий.

- 7) Администратор системы резервного копирования должен согласовать с бизнес-владельцем ИА параметры резервного копирования (состав резервируемых данных, время проведения процедур резервирования и восстановления, объем копируемой информации, место размещения резервных копий).
- 8) Необходимо учитывать влияние не только информации, но и сопутствующих данных, подлежащих резервированию, хранению и восстановлению – сопутствующее программное обеспечение, без которого невозможно использовать саму информацию, а также обеспечивать синхронность версий программного обеспечения и информации.
- 9) В описании используемой системы резервного копирования должно быть указано ее влияние на выбранные способы, методы, типы, количество дублирующих и архивных копий.
- 10) Выбранные настройки системы резервного копирования должны согласовываться с владельцами информационных активов.

## **20. Политика управления изменениями.**

Цель политики – организация процесса управления изменениями, гарантирующего осуществление контролируемой оценки, утверждения, внедрения и обзора изменений.

Требования политики:

- 1) Изменения сервисов и инфраструктуры должны иметь четко определённый и задокументированный охват;
  - 2) Все запросы на изменения должны быть записаны и классифицированы, например, срочные, значительные, несущественные. Для запросов на изменение должна производиться оценка рисков, влияния и выгод для бизнеса;
  - 3) Процесс управления изменениями должен включать в себя способ отмены или исправления изменения в случае неудачи;
  - 4) Изменения должны утверждаться, проверяться, внедряться контролируемым способом. Для всех изменений должен производиться обзор успешности внедрения, а также любых предпринятых после внедрения действий;
  - 5) Должны применяться политики и процедуры контроля авторизации и внедрения срочных изменений;
  - 6) Запланированные сроки внедрения изменений должны использоваться как основа для планирования изменений и релизов. График, содержащий информацию обо всех изменениях, утверждённых к внедрению, и информацию о предполагаемых сроках внедрения, должен поддерживаться заинтересованными сторонами;
  - 7) Записи об изменениях должны регулярно анализироваться для обнаружения роста количества изменений повторяющихся типов, намечающихся тенденций и другой значимой информации;
  - 8) Результаты и выводы анализа изменений должны быть записаны;
  - 9) Действия по улучшению, выявленные в рамках этого процесса, должны быть записаны и использоваться в качестве входных данных для плана улучшения услуг.
21. Для реализации частных политик разрабатываются и вводятся в действие соответствующие ВНД Компании.

## **Глава 7. Ответственность**

22. Ответственность за реализацию настоящей Политики СМИБ возлагается на Председателя Правления Компании.
23. **УЗРЦОД** несет ответственность за достижение поставленных целей СМИБ, осуществляет планирование мероприятий по реализации положений настоящей Политики СМИБ, координирует деятельность функциональных блоков и структурных подразделений Компании по созданию, внедрению и поддержанию СМИБ.
24. Руководители функциональных блоков, структурных подразделений, работники Компании несут ответственность за безусловное полное выполнение своих обязанностей по обеспечению информационной безопасности в соответствии с настоящей Политикой СМИБ и ВНД Компании.
25. Ответственность за несоблюдение информационной безопасности в Компании, а также за невыполнение положений настоящей Политики СМИБ несет каждый сотрудник Компании в соответствии с действующим законодательством Республики Казахстан и ВНД Компании.
26. Ответственность за поддержание Политики СМИБ в актуальном состоянии несет **УЗРЦОД**.

## **Глава 8. Заключительные положения**

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