
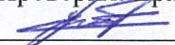
 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ АТӨКІМЕ АҚПАРАТ ЖӘНЕ ҚОҒАМ АРНАМА ҚИЗМЕТТЕРІ АЖАТ</small>	<b>АО «Национальная компания «КазМунайГаз»</b>	
<b>Наименование документа: Руководство по системе менеджмента информационной безопасности АО НК «КазМунайГаз»</b>		
<b>Тип документа: Руководство</b>	<b>Версия 4</b>	<b>стр. 1 из 16</b>
Разработал: Сагнаев Е.А.  <u>«20» февраля 2020 г.</u>	Проверил: Ермакбаев Е.К.  <u>«20» февраля 2020 г.</u>	Утверждено решением Правления АО НК «КазМунайГаз» от « <u>2</u> » <u>марта</u> 20 <u>20</u> года, Протокол № <u>8</u>

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ

### 1.1. Общие положения

АО НК «КазМунайГаз» (далее – КМГ) создано в соответствии с Указом Президента Республики Казахстан от 20 февраля 2002 г. № 811 «О мерах по дальнейшему обеспечению интересов государства в нефтегазовом секторе экономики страны» и постановлением Правительства Республики Казахстан от 25 февраля 2002 г. № 248 «О мерах по реализации Указа Президента Республики Казахстан от 20 февраля 2002 г. № 811».

Основные виды деятельности КМГ определяются Уставом КМГ, утвержденным решением лица, владеющего всеми голосующими акциями КМГ в лице АО «Самрук-Қазына».

В КМГ разработана и введена в действие система менеджмента информационной безопасности (далее – СМИБ), которая подтверждает способность КМГ обеспечить выбор адекватных и пропорциональных средств управления защитой информации, обеспечивающих безопасность информационных ресурсов при использовании их в деятельности КМГ. Принятие СМИБ является стратегическим решением для КМГ.


СМИБ разработана на основе требований международного стандарта ISO/IEC 27001:2013 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

СМИБ сохраняет конфиденциальность, целостность и доступность информации и обеспечивает уверенность заинтересованным сторонам в том, что риски управляются в достаточной мере.

СМИБ является частью общей структуры менеджмента, при этом информационная безопасность учитывается в течение всего цикла разработки информационных систем, а также в отношениях с поставщиками.

Руководство по системе менеджмента информационной безопасности (далее – Руководство) описывает вопросы реализации требований стандарта ISO/IEC 27001:2013, распределения полномочий и обязанностей работников КМГ, структурных подразделений, вовлеченных в процесс обеспечения информационной безопасности. При этом в целях качественной организации СМИБ противоречащие обязанности и ответственность разделяются.



 <b>ҚазМунайГаз</b> <small>NATIONAL COMPANY ҰЛТТЫҚ ҚОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

## 1.2. Применение СМИБ

Территориальные границы области применения СМИБ, включают в себя центральный офис КМГ, расположенный по адресу: г. Нур-Султан, ул. Кунаева 8.

Область применения СМИБ распространяется на все структурные подразделения КМГ.

В область применения СМИБ включены следующие типы ресурсов и технологии:

1) первичные ресурсы ИБ:

- информация (информационные активы);
- процессы;

2) вспомогательные ресурсы:

- аппаратное обеспечение;
- программное обеспечение;
- сервисы или бизнес-приложения;
- сеть и (или) сетевое оборудование;
- человеческие ресурсы;
- ресурсы, связанные с местоположением КМГ (помещения, зоны физической безопасности и системы безопасности, услуги телекоммуникации и обслуживания оборудования, системы жизнеобеспечения).

Область применения СМИБ применяется в отношении процессов:

«Консолидация бизнес-планов, финансовой и управленческой отчетности»;

«Управление геолого-геофизическими информационными системами».

Область применения СМИБ определена в соответствии с действующей версией Политики информационной безопасности АО НК «КазМунайГаз» (утверждена решением Правления АО НК «КазМунайГаз» от 10.11.2015 г., протокол №55 пункт 12) и может пересматриваться в случае необходимости. При этом допускается в рамках тестирования расширение области применения СМИБ с согласия курирующих руководителей.

## 2. Нормативные ссылки

При разработке СМИБ были использованы следующие международные стандарты:

ISO/IEC 27001:2013 - «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

ISO/IEC 27002:2013 - «Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации»;



ISO/IEC 27003:2017 - «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство»;

ISO/IEC 27004:2016 - «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, измерения, анализ и оценка»;

ISO/IEC 27005:2018 — «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

### 3. ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем Руководстве используются следующие определения и сокращения:

**Доступность информации**

- состояние информации, при котором субъекты, имеющие право доступа (право на использование, чтение, изменение, копирование, уничтожение информации), могут реализовывать их беспрепятственно

**Конфиденциальность информации**

- состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право

**Целостность информации (ресурсов)**

- состояние информации, при котором ее изменение осуществляется только преднамеренно субъектами, имеющими на это право

**Информационная безопасность (ИБ)**


- состояние защищенности информационного пространства КМГ, а также прав и интересов КМГ и каждого его работника в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается конфиденциальность, целостность и доступность информационных активов

**Информационный актив**

- информация и носители информации, имеющие ценность для КМГ, риск утери конфиденциальности/целостности/доступности которых, может привести к материальным или иным убыткам

**Инцидент ИБ**

- единичное событие или же ряд нежелательных или неожиданных событий в информационной

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҚАЗМҰНАЙ ГАЗ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

безопасности, которые подвергают большому риску бизнес-процессы или же угрожают информационной безопасности

**Система менеджмента информационной безопасности (СМИБ)** - часть общей системы управления, основанная на оценке рисков ИБ, которая предназначена для проектирования, внедрения, функционирования, мониторинга, анализа, сопровождения и улучшения ИБ

**Представитель руководства по СМИБ** - работник КМГ, назначаемый приказом председателя Правления КМГ из состава руководства, руководства функциональных блоков или из числа руководителей структурных подразделений, непосредственно подчиненных председателю Правления и отвечающих за информационную безопасность

**Ответственный за СМИБ** - работник ДКБ, ответственный за оперативное управление СМИБ

**Область применения СМИБ** - процессы, структурные подразделения и ресурсы в определенных территориальных границах, на которые распространяется действие СМИБ КМГ

**Декларация (заявление) о применимости средств управления СМИБ АО НК «КазМунайГаз»** Документ, описывающий средства управления, имеющие отношение к СМИБ КМГ. Составлен на основе приложения А стандарта ISO/IEC 27001:2013

**Пользователи СМИБ** - работники всех структурных подразделений КМГ (для целей настоящего Руководства)

**Риск ИБ** - потенциальная опасность нанесения ущерба КМГ при реализации угрозы ИБ (наступления инцидента ИБ) ввиду наличия уязвимости

**Рабочая группа по СМИБ** - создаваемый в КМГ постоянно действующий орган по управлению и поддержанию в рабочем состоянии СМИБ



<b>Угроза ИБ</b>	- потенциальная причина инцидента ИБ, который может нанести ущерб КМГ
<b>Уязвимость</b>	- недостаток или слабое место в информационной системе, процессе, которое может быть условием реализации угрозы ИБ
<b>Информационные системы (ИС)</b>	- совокупность методов, процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку и распространение информации
<b>Информационные технологии (ИТ)</b>	- система средств, способов, методов и моделей осуществления информационных процессов с помощью электронно-цифровых технологий и информационных систем
<b>Блок ИТ</b>	- структурные подразделения КМГ, отвечающие за информационные технологии
<b>КМГ</b>	- акционерное общество «Национальная компания «КазМунайГаз»
<b>ДКБ</b>	- департамент корпоративной безопасности

#### **4. Система менеджмента информационной безопасности**


##### **4.1. Общие требования**

В КМГ разработана, внедрена, функционирует, постоянно контролируется, анализируется, поддерживается в рабочем состоянии и улучшается СМИБ. Основные элементы СМИБ описаны в документации СМИБ.

Целями внедрения СМИБ в КМГ являются: обеспечение конфиденциальности, целостности и доступности информации, а так же обеспечение непрерывности ведения бизнес-процессов.

Основными задачами СМИБ являются:

- понимание всеми работниками КМГ и представителями третьих сторон, имеющим доступ к информационным ресурсам КМГ требований СМИБ;

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҰЛТТЫҚ КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

- внедрение и эксплуатация механизмов контроля для управления рисками СМИБ;
- мониторинг и проверка эффективности СМИБ;
- непрерывное совершенствование СМИБ на базе объективных измерений.

Для защиты информации, а также средств ее обработки от нарушения конфиденциальности, целостности и доступности ДКБ и Блок ИТ применяет организационные, физические, технические, программные и программно-аппаратные средства обеспечения СМИБ.

Мероприятия по обеспечению СМИБ соответствуют требованиям законодательства Республики Казахстан, требованиям заключенных КМГ договоров, а также требованиям, предъявляемым к защите информации КМГ.

К процедурам управления СМИБ применяется процессный подход, который заключается в последовательном выполнении следующих этапов:

- определение требований КМГ к СМИБ, а также политики и целей обеспечения СМИБ;

- осуществление управления информационными рисками (обеспечение выполнения требований к СМИБ) как части общего процесса управления всеми рисками КМГ;

- мониторинг и проверка выполнения процессов СМИБ;
- пересмотр требований к СМИБ (в соответствии с изменением бизнес-требований КМГ) и улучшение процедур управления СМИБ.

PDCA-модель (Plan – Do – Check – Act) в основном применима к структуре процессов СМИБ. Данная модель состоит из четырех последовательных этапов, которые выполняются для каждого процесса:

- планирование;
- внедрение;
- проверка функционирования;
- совершенствование.


Для эффективного функционирования процессов системы управления PDCA-модель применяется циклически, т.е. выполнение всех этапов регулярно повторяется. К процедурам управления при необходимости могут применяться и другие модели (или их элементы).

## **4.2. Создание и менеджмент СМИБ**

### **4.2.1. Создание СМИБ**

С целью создания СМИБ в КМГ реализованы следующие мероприятия:

- 1) определена область применения СМИБ;
- 2) разработана и утверждена Правлением КМГ Политика информационной безопасности АО НК «КазМунайГаз»;
- 3) определён подход к оценке рисков в КМГ, описана методология оценки рисков, критерии принятия рисков и определены приемлемые уровни

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҚАЗМУНАЙ ГАЗ КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

рисков в соответствии с Правилами управления рисками информационной безопасности АО НК «КазМунайГаз» (**KMG-PR-1752.3-22**);

4) выявлены риски КМГ. В Отчете об инвентаризации ресурсов (**KMG-F-1755.3-22/PR-1752.3-22**) и Каталоге угроз информационной безопасности (**KMG-F-1756.3-22/PR-1752.3-22**) указаны ценные ресурсы КМГ, владельцы ресурсов, потенциальные угрозы для этих ресурсов;

5) проанализированы риски и оценена значительность рисков, произведена оценка негативного влияния на организацию потери конфиденциальности, целостности или доступности ресурсов, вероятность случаев нарушения защиты ресурса, а также реализуемые на текущий момент средства управления и оценка уровня риска;

6) выявлены и оценены возможности для обработки рисков;

7) выбраны цели и средства управления для обработки рисков;

8) получено утверждение руководства предлагаемого остаточного риска;

9) получено разрешение руководства на внедрение и эксплуатацию СМИБ;

10) для достижения целей в области информационной безопасности разработаны планы, определяющие конкретные мероприятия, сроки, ответственных за выполнение, а также необходимые ресурсы;

11) разработана Декларация (заявление) о применимости средств управления СМИБ АО НК «КазМунайГаз».

#### **4.2.2. Эксплуатация СМИБ**


В целях обеспечения предотвращения или снижения рисков, а также постоянной способности СМИБ достигать запланированных результатов в КМГ сформулирован и реализуется план мероприятий по управлению рисками ИБ.

В КМГ разработаны и реализуются средства управления для достижения целей управления, которые соответствуют Политике информационной безопасности, а также результатам оценки рисков. Средства управления изложены в документах СМИБ.

#### **4.2.3. Постоянный контроль и анализ СМИБ**

Постоянный контроль и анализ СМИБ проводится в целях выявления и предотвращения инцидентов безопасности, а также определения эффективности мер, предпринимаемых для их устранения. Регистрируются все действия и события, которые могли бы негативно повлиять на результативность и функционирование СМИБ. При этом функции информационной безопасности и информационных технологий разделены.

Управление инцидентами ИБ осуществляется в соответствии с Рабочей инструкцией по управлению инцидентами системы менеджмента информационной безопасности АО НК «КазМунайГаз» (**KMG-RI-1946.2-22**).

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY УЛТТЫК КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

При этом осуществляется последовательный и результативный подход к управлению инцидентами информационной безопасности, включая информирование о событиях, связанных с безопасностью, и уязвимостях.

Ответственный за СМИБ формирует план с задачами проверок эффективности СМИБ и утверждает у представителя руководства по СМИБ КМГ. Анализ результативности и эффективности СМИБ осуществляется в соответствии с Рабочей инструкцией по оценке результативности выбранных средств управления и эффективности системы менеджмента информационной безопасности АО НК «КазМунайГаз» (КМГ-RI-1951.2-22), а также Положением о Совете по системам менеджмента АО НК «КазМунайГаз» (КМГ-PL-1093.7-59). По результатам оценки ответственный за СМИБ формирует отчет по оценке эффективности СМИБ и утверждает у представителя руководства по СМИБ.

Целью анализа информационной безопасности является подтверждение того, что информационная безопасность обеспечивается и управляется в соответствии с Политикой информационной безопасности и документами СМИБ.

Контроль выполнения применимых законодательных требований осуществляется в соответствии с Рабочей инструкцией по оценке соответствия законодательным и договорным требованиям системы менеджмента информационной безопасности в АО НК «КазМунайГаз» (КМГ-RI-2024.2-22).

#### **4.2.4. Поддержание в рабочем состоянии и улучшение СМИБ**

Ответственный за СМИБ:

1) на регулярной основе координирует работу по обеспечению работоспособности и улучшению СМИБ путем внедрения всех выявленных улучшений в СМИБ, применения опыта информационной защиты других организаций;

2) информирует все заинтересованные стороны обо всех действиях, направленных на улучшение показателей информационной безопасности, вкладе работников КМГ в результативность СМИБ, а также о возможных последствиях не соблюдения требований СМИБ.

#### **4.3. Требования к документации**

Документация СМИБ КМГ ведется в объеме, необходимом для эффективного функционирования СМИБ, включает записи управленческих решений, а также обеспечивает воспроизводимость результатов, демонстрируя взаимосвязь результатов процесса оценки и обработки риска от выбранных средств управления.

Документация СМИБ КМГ включает в себя:

- документированное заявление о политике и целях в области ИБ;





- описание области применения СМИБ;
- процедуры и средства управления в поддержку СМИБ согласно перечню документации СМИБ;
- описание методологии оценки рисков;
- отчет об оценке рисков;
- план обработки рисков.


Документация СМИБ управляется в соответствии с Правилами по управлению документами ИСУ (КМГ- PR-1.13-59).

## **5. Ответственность руководства**

### **5.1. Обязательства руководства**

Руководство КМГ приняло решение о создании, внедрении, эксплуатации, постоянному контролю, анализу, поддержанию в рабочем состоянии и улучшению СМИБ в соответствии с требованиями международного стандарта ISO/IEC 27001:2013, а также об интеграции требований данного стандарта с существующей в КМГ системой менеджмента. Это решение выражается в следующих действиях:

- утверждение Политики информационной безопасности, которая анализируется на адекватность и актуальность через запланированные промежутки времени или в случае значительных изменений системы управления КМГ;
- принятие решения о критериях принятия риска и приемлемых уровнях риска;
- утверждение планов непрерывности бизнеса, планов обработки рисков и т.п.;
- утверждение ролевой структуры СМИБ;
- стимулирование и поддержка работников КМГ, способствующих эффективности СМИБ;
- рассмотрение информационной безопасности в управлении проектами;
- обеспечение достаточного количества ресурсов, их доступности для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения СМИБ;
- проведение внутренних аудитов СМИБ, обеспечение достижения заданных результатов СМИБ;
- проведение анализа СМИБ со стороны руководства;
- постоянное взаимодействие с органами власти и организациями, по вопросам информационной безопасности, обобщение передового опыта;
- систематическое доведение до сведения всех работников КМГ и взаимодействующих организаций информации о важности выполнения целей защиты информации и соответствия Политики информационной безопасности АО НК «КазМунайГаз», ответственности КМГ в соответствии

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҰЛТТЫҚ КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

с законодательством Республики Казахстан и потребности КМГ в непрерывном улучшении СМИБ.

## 5.2. Менеджмент ресурсов


Руководство КМГ, понимая важность информационных ресурсов для функционирования всех бизнес-процессов, декларирует, что обеспечение работоспособности СМИБ входит в обязанности работников КМГ наряду с выполнением их должностных обязанностей.

Председатель Правления КМГ несёт ответственность за правильность применения всех реализованных средств управления СМИБ, которые включают в себя инициирование деятельности по обеспечению информационной безопасности КМГ, предоставление необходимых ресурсов для функционирования СМИБ для обеспечения поддержки требований бизнеса процедурами информационной безопасности, контроль над выполнением деятельности по обеспечению СМИБ, демонстрируя лидерство и приверженность относительно СМИБ.

СМИБ возглавляет председатель Правления КМГ, который управляет ею через представителя руководства по СМИБ. Представитель руководства по СМИБ назначается приказом председателя Правления КМГ из состава руководства или из числа руководителей структурных подразделений, непосредственно подчиненных председателю Правления и отвечающих за информационную безопасность.

Представитель руководства по СМИБ независимо от своих основных должностных обязанностей несет ответственность за:

- определение конкретных целей и текущих задач, для решения вопросов информационной безопасности;
- текущее управление, проведение единой политики и эффективное функционирование системы управления информационной безопасности;
- координацию взаимодействия с внешними организациями по вопросам, касающимся СМИБ;
- рассмотрение совместно с представителем руководства по интегрированной системе управления и принятие решений по проблемным вопросам СМИБ в пределах своей компетенции;
- проверку применения стандартов, политик и правил для обеспечения информационной безопасности и управления рисками в КМГ;
- консультирование руководства КМГ по вопросам информационной безопасности;
- периодическую оценку рисков информационной безопасности и соблюдение политик, процедур и правил;
- координирование обучения руководителей и работников КМГ вопросам информационной безопасности, доведение до сведения работников КМГ требований СМИБ;

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY УЛТТЫК КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

- контроль проведения тренировок и анализ результатов проведения тренировок по действиям в случае инцидентов, связанных с информационной безопасностью;

- обеспечение утверждения разработанных политик, задач, процедур и показателей для оценки информационной безопасности;

- изучение и анализ инцидентов в сфере информационной безопасности, реакции на инциденты в сфере информационной безопасности и разработку мер по улучшению сетевой и информационной безопасности;

- инициирование вопроса о привлечении работников КМГ к дисциплинарной ответственности за нарушение требований документации СМИБ;

- контроль выполнения утвержденных руководством КМГ документов, связанных с информационной безопасностью;

- организацию работы постоянно действующей рабочей группы по управлению и поддержанию в рабочем состоянии СМИБ АО НК «КазМунайГаз» (далее - Рабочая группа по СМИБ), а также привлечение структурных подразделений к мероприятиям по информационной безопасности по согласованию с курирующим руководителем;

- подготовку докладов с анализами произошедших инцидентов, связанных с информационной безопасностью, разработку мер для компенсаций последствий и предотвращению подобных инцидентов.

Представитель руководства по СМИБ в установленном порядке взаимодействует со всеми структурными подразделениями КМГ, дочерними организациями и зависимыми обществами КМГ, а также иными организациями и государственными органами в соответствии со своими полномочиями.

В случае временного отсутствия (болезнь, командировка, отпуск и т.д.) представителя руководства по СМИБ его функции выполняет лицо, назначенное приказом председателя Правления КМГ.

Оперативную работу по обеспечению функционирования СМИБ осуществляет ответственный за СМИБ при содействии владельцев процессов.


Ответственный за СМИБ несет ответственность за:

- разработку документов СМИБ;
- деятельность по разработке, внедрению, управлению и улучшению СМИБ;

- организацию внутренних аудитов СМИБ;

- информирование Представителя руководства по СМИБ по вопросам информационной безопасности;

- проведение периодической оценки рисков информационной безопасности и разработку планов по снижению рисков;

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

- документирование инцидентов, связанных с информационной безопасностью и немедленное информирование об этом Представителя руководства по СМИБ.

Все вопросы разработки, актуализации и функционирования СМИБ решаются в Рабочей группе по СМИБ, по представлению представителя руководства и членов Рабочей группы по СМИБ.

Рабочая группа по СМИБ несет ответственность за:

- экспертные консультации Представителя руководства по СМИБ и ответственного по СМИБ по конкретным вопросам, связанным с информационной безопасностью;

- выполнение специализированных оценок результативности СМИБ по заданиям Представителя руководства по СМИБ или ответственного за СМИБ;

- актуализацию документов СМИБ в части их касающейся;

- предложение улучшений в области информационной безопасности.

ДКБ несет ответственность за контроль безопасности программных и технических комплексов, обеспечивающих защиту информации КМГ, соблюдения требований безопасности по защите электронного документооборота, целевого использования ресурсов сети Интернет, мониторинг наличия инцидентов информационной безопасности.

Блок ИТ несет ответственность за контроль и обеспечение надлежащей и бесперебойной работы информационной и телекоммуникационной инфраструктуры КМГ.

Руководители структурных подразделений в области применения СМИБ несут ответственность за:

- успешное внедрение, обеспечение работоспособности и улучшения СМИБ в области действия их процессов;


- определение потребности в повышении квалификации работников своих подразделений, связанных с работой по информационной безопасности, информирование третьих лиц по вопросам информационной безопасности;

- соблюдение требований документов СМИБ работниками своих структурных подразделений и третьих лиц в соответствии с договорными соглашениями;

- доведение до сведения своих работников порядка раскрытия информации;

- немедленное информирование ответственного за СМИБ об установленных работниками инцидентах или отмеченных слабостях в области информационной безопасности;

- стимулирование и поддержку совместно с ДКБ своих работников, способствующих эффективности СМИБ, в соответствии с внутренними документами КМГ.

 <b>ҚазМұнайГаз</b> <small>NATIONAL COMPANY ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ АТӨКІМЕ ҚОҒАМЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

Работники КМГ в области применения СМИБ несут ответственность за:

- соблюдение требований документов СМИБ;
- соблюдение требований по обеспечению информационной безопасности на рабочем месте (политика «чистого экрана» и «чистого стола») и при работе с мобильными устройствами;
- немедленное информирование руководителя структурного подразделения об установленных инцидентах или отмеченных слабостях в области информационной безопасности.

В отношении работников КМГ, нарушивших требования информационной безопасности могут быть приняты меры дисциплинарного воздействия.

Порядок обеспечения подготовки, осведомленности и компетентности персонала в области ИБ описан в следующих документах:

Правила конкурсного отбора на занятие вакантных административных должностей АО НК «КазМунайГаз» (KMG-PR-838.7-47);

Правила трудового распорядка АО НК «КазМунайГаз» (KMG-PR-1167.3-6);

Правила обучения и развития работников АО НК «КазМунайГаз» (KMG-PR-434.8-6);

Рабочая инструкция о приеме, переводе, перемещении работников АО НК «КазМунайГаз» (KMG-RI-898.6-6).

## **6. Внутренние аудиты СМИБ**

В КМГ регулярно (не реже одного раза в год) проводится внутренний аудит СМИБ.

Внутренний аудит СМИБ организуется ответственным за СМИБ. Все операции, необходимые для проведения внутреннего аудита СМИБ, планируются с учетом требований к обеспечению конфиденциальности, целостности и доступности информационных ресурсов КМГ, а также непрерывности ведения бизнеса.


Внутренние аудиты СМИБ проводятся в соответствии с Правилами по проведению аудита процессов АО НК «КазМунайГаз» (KMG-PR-147.8-59).

## **7. Анализ СМИБ со стороны руководства**

### **7.1 Общие положения**

Председатель Правления с периодичностью не реже 1 раза в год, рассматривает результативность СМИБ, чтобы обеспечить ее пригодность, адекватность и результативность, а также соответствие требованиям стандарта ISO 27001:2013 и внутренним требованиям КМГ.

Этот анализ должен включать в себя оценку возможностей для улучшения и потребности в изменениях СМИБ, включая политику защиты

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҚАЗМҰНАЙ ГАЗ КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

информации и цели защиты информации. При этом анализ технического соответствия ИС должен регулярно проводиться ответственными работниками Блока ИТ.

Председатель Правления совместно с представителем руководства по СМИБ определяют дату проведения Совета по системам менеджмента АО НК «КазМунайГаз» по вопросам обеспечения безопасности для анализа СМИБ.

В случае необходимости, по предложению одного из членов Совета по ИСУ и СМИБ могут проводиться внеплановые заседания, посвященные анализу СМИБ.

В результате анализа оценивается текущий статус и уровень выполнения требований СМИБ, на основе которого председатель Правления принимает решения по дальнейшему совершенствованию системы.

В работе заседания по анализу СМИБ принимают участие все члены Совета по ИСУ и СМИБ, связанные с вопросами обеспечения безопасности, а также иные заинтересованные работники.

Повестка дня заседания подготавливается ответственным за СМИБ по согласованию с представителем руководства по СМИБ, рассматривается председателем Правления и сообщается всем участникам совещания не позднее 2-х рабочих дней до его проведения в соответствии с Положением о Совете по системам менеджмента АО НК «КазМунайГаз» (КМГ-PL-1093.7-59).


## **7.2 Входные данные для анализа**

Для проведения анализа СМИБ со стороны руководства представитель руководства по СМИБ организует работу по подготовке отчета о функционировании СМИБ и состоянии ИБ в КМГ.

Руководители структурных подразделений обязаны предоставить информацию, относящуюся к подготовке отчета ответственному за СМИБ в определенные сроки.

В отчете должна содержаться следующая информация о:

- последующих действиях, вытекающих из предыдущего анализа со стороны руководства;
- уязвимых местах или угрозах, адекватно не рассмотренных в предыдущих оценках риска;
- результатах аудитов и анализа СМИБ;
- устранения несоответствий, выявленных в результате аудитов и проверок, статусе корректирующих действий;
- методиках, продуктах или процедурах, а также любых изменениях которые можно было бы использовать в КМГ для улучшения качества работы и результативности СМИБ;

 <b>КазМунайГаз</b> <small>NATIONAL COMPANY ҚАЗТАН КОМПАНИЯСЫ</small>	<b>Руководство по системе менеджмента  информационной безопасности АО НК «КазМунайГаз»</b>	
	<b>Руководство</b>	<b>Версия 4</b>

- результатах измерений результативности и рекомендации по улучшению СМИБ.

### 7.3. Результаты анализа

Результатом анализа со стороны руководства КМГ являются решения, связанные с совершенствованием системы, процессов, процедур необходимых для наибольшей результативности СМИБ. В результате анализа устанавливается необходимость в изменении политики и целей СМИБ, а также потребность в ресурсах, необходимых для дальнейшего улучшения СМИБ.


Решения, принимаемые в результате проведения анализа со стороны руководства должны быть направлены на:

- улучшение результативности СМИБ;
- обновление оценки риска и плана обработки риска;
- изменения процедур и средств управления, которые влияют на защиту информации, если это необходимо, для того чтобы среагировать на внутренние или внешние события, которые могли негативно повлиять на СМИБ. К этим событиям относятся: деловые требования, требования защиты, деловые процессы, влияющие на существующие деловые требования, нормативные или законодательные требования, договорные обязательства, уровни риска и (или) критерии принятия риска;
- обеспечение необходимыми ресурсами;
- улучшение в том, как измеряется результативность средств управления.

Решения, принятые по итогам анализа со стороны руководства КМГ, документируются в протоколе заседаний Совета по системам менеджмента АО НК «КазМунайГаз» с указанием ответственных исполнителей и сроков исполнения.

## 8. Улучшение СМИБ

Руководство КМГ обеспечивает необходимую компетентность лиц, от которых зависит эффективность информационной безопасности посредством соответствующего обучения. На основании решений, принятых по итогам анализа со стороны руководства КМГ, утверждается план корректирующих действий и совершенствования СМИБ. Постоянное улучшение СМИБ обеспечивается систематическим выполнением корректирующих и предупреждающих действий в соответствии с Правилами по проведению аудита процессов АО НК «КазМунайГаз» (KMG-PR-147.8-59).

 <b>КазМунайГаз</b> NATIONAL COMPANY ҰЛТТЫҚ КОМПАНИЯСЫ	<b>Руководство по системе менеджмента информационной безопасности АО НК «КазМунайГаз»</b>	
<b>Руководство</b>	<b>Версия 4</b>	<b>стр. 16 из 16</b>

## **9. Применимые средства управления для обеспечения информационной безопасности**

Цели управления и применимые средства управления указаны в Декларации о применимости средств управления СМИБ АО НК «КазМунайГаз».

## **10. Заключительные положения**

Настоящее Руководство, а также все изменения и дополнения к нему утверждаются Правлением КМГ.



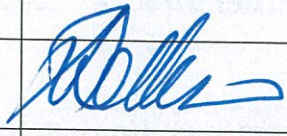

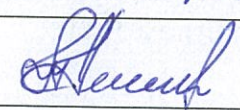


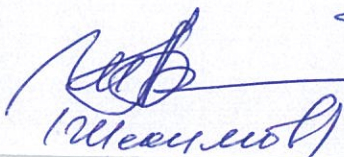
Лист согласования к Руководству по системе менеджмента  
информационной безопасности АО НК «КазМунайГаз»,  
Версия 4

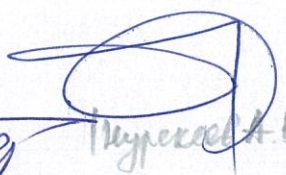
Форма ИСУ

KMG-F-235.13-8/ RG-6.13-8

стр. 1 из 1

Должность	Виза, дата	ФИО
Управляющий директор по правовому обеспечению	 24.02.2025	М. Сәулебай
Управляющий директор по стратегии		Э. Карымсаков
Директор по корпоративной безопасности		Т. Алиаскаров

  
19.02.2025

  
19.02.2025