«Утверждаю»

_____

«__» «_____» 20__ г.

РУКОВОДСТВО ПО

СИСТЕМЕ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

1 Назначение

Настоящее Руководство устанавливает единые требования к порядку управления информационной безопасностью в ТОО ПРИМЕР (далее-Компания), закрепляет полномочия и ответственность работников Компании, устанавливает общие направления и принципы деятельности для реализации в Компании системы менеджмента информационной безопасности (далее-СМИБ) в соответствии с требованиями международного стандарта ISO/IEC 27001:2022.

Настоящее Руководство вводится в действие со дня его утверждения.

2 Общие положения

2.1 Область применения

Требования настоящего Руководства распространяются на структурные подразделения Компании, к информационным активам и процессам, подпадающим в область действия СМИБ, описанной в документе «Область действия системы управления информационной безопасностью Компании.

Контроль за выполнением требований настоящего Руководства несет руководитель Рабочей группы СМИБ.

Ответственность за управление и соответствие требований настоящего Руководства требованиям нормативных правовых актов Республики Казахстан, нормативных документов несет Менеджер информационной безопасности.

Руководители структурных подразделений, входящих в Область действия СМИБ, несут ответственность за выполнение требований настоящего Руководства.

2 Нормативные ссылки

2.1 В настоящем Руководстве по СМИБ приведены ссылки на внешние и внутренние нормативные документы в соответствии с:

- Перечнями внешней нормативной документации компании и ее структурных подразделений;
- Контрольным перечнем основной документации СМИБ /Контрольным перечнем внутренних нормативных документов Компании.

3 Термины и определения, сокращения

В настоящем руководстве использованы термины в соответствии с определениями предусмотренными Глоссарием интегрированной системы менеджмента.

В дополнение к ним в настоящем руководстве предусмотрены следующие термины, определения и сокращения:

ВНД – внутренний нормативный документ;
ДУП - Департамент по управлению персоналом;
ИА – информационный актив;
ИБ – информационная безопасность;
ИС – информационная система;
КЦД – конфиденциальность, целостность, доступность;
РИБ – риски информационной безопасности**;**
СМИБ – система управления информационной безопасностью
ПРПД – цикл «Планирование-Реализация-Проверка-Действие».

4 Контекст организации

4.1 Описание контекста Компании

4.1.1 Внешняя среда организации.

Внешняя среда Компании рассматривается как совокупность двух относительно самостоятельных подсистем: макроокружения (внешняя макросреда) и непосредственного окружения (внешняя микросреда).

4.1.2 Внутренняя среда организации.

В компании определены элементы внутренней среды. К факторам внутренней среды отнесены: цели, оргструктура, ресурсы, персонал, технология, информационные системы, корпоративная культура компании.

Схема, описывающая среду организации приведена на рисунке 1.

Рисунок 1 - Контекст ТОО ПРИМЕР

4.2 Заинтересованные стороны. Потребности и ожидания.

4.2.1 Высшее руководство компании идентифицировало свои заинтересованные стороны, их интересы и поддерживает сбалансированное реагирование на их требования и ожидания.

4.2.2 К заинтересованным сторонам отнесены физические и юридические лица, создающие добавленную ценность для организации или так, или иначе заинтересованные в деятельности организации, или находящиеся под ее влиянием.

4.2.3 В компании определены основные группы заинтересованных лиц, их потребности и ожидания (таблица 1).

Таблица 1

Заинтересованная сторона	**Потребности и ожидания**
Потребители	Соблюдение всех условий договорных отношений, проявление уважения и добросовестности во взаимоотношениях.
Единственный акционер	Своевременное и полное доведение информации о деятельности компании, затрагивающей интересы компании
Филиалы	Стабильное финансовое развитие, прибыльность, повышение инвестиционной привлекательности компании.
Государственные структуры	Соблюдение принципов партнерства и уважения, с пониманием того, что все инициативы государственных органов и Компании должны быть направлены на развитие экономики страны и продвижение достойного труда; Компания должна быть ответственным и добросовестным налогоплательщиком; Социальное партнерство с региональными государственными органами; Выполнение законодательных и нормативных требований.
Общественные организации и местная общественность на территории присутствия	Информационная безопасность деятельности компании; Развитие инфраструктуры; Использование регионального промышленного кластера;
СМИ	Информационная открытость бизнеса, информация о ключевых событиях.
Персонал	Хорошие условия труда; Обеспечение обратной связи руководства организации с работниками компании;
Поставщики и партнеры	Взаимные выгоды и преемственность; Соблюдение всех условий договорных отношений, проявление уважения и добросовестности во взаимоотношениях;

4.3 Область действия системы менеджмента информационной безопасности

4.2.1 Областью действия СМИБ является обеспечение информационной безопасности Компании.

СМИБ распространяется на структурные подразделения, должностных лиц, информационные активы, задействованных в процессах Компании, указанных в Приложении 1 «Область действия Системы Менеджмента Информационной Безопасности ТОО ПРИМЕР.

К СМИБ применяются все требования, установленные разделами 4, 5, 6, 7, 8, 9 и 10 международного стандарта ISO/IEC 27001:2022.

В СМИБ применяются механизмы контроля из Приложения А международного стандарта ISO/IEC 27001:2022 согласно документу СМИБ «Положение о применимости». Все исключения механизмов контроля, принятые в СМИБ, указаны и обоснованы в «Положении о применимости».

4.4 Система менеджмента информационной безопасности

4.4.1 СМИБ Компании предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

4.4.2 В ТОО ПРИМЕР разработана, внедрена и поддерживается в рабочем состоянии СМИБ в соответствии с требованиями ISO/IEC 27001:2022.

4.4.3 В Компании применяется процессный подход к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СМИБ.

4.4.4 Процессный подход реализуется в соответствии с моделью ПРПД (Планирование–Реализация–Проверка–Действие), которая применима к структуре всех процессов СМИБ. Данная модель состоит из четырех последовательных фаз, которые выполняются для каждого процесса СМИБ:

Планирование (создание и управление СМИБ) – определение политики СМИБ, целей, процессов и процедур, относящихся к управлению рисками и совершенствованию информационной безопасности для получения результатов в соответствии с общими политиками и целями Компании.

Реализация (внедрение и эксплуатация СМИБ) – внедрение и применение политики ИБ, механизмов контроля, процессов и процедур в области ИБ.

Проверка (мониторинг и анализ СМИБ) – Оценка и, там где это применимо, измерение характеристик исполнения процесса в соответствии с политикой ИБ, целями и практическим опытом, и предоставление отчетов руководству Компании для соответствующего анализа.

Действие (сопровождение и совершенствование СМИБ) – принятие корректирующих и превентивных мер, основанных на результатах внутреннего аудита СМИБ, анализа со стороны руководства Компании или другой относящейся к делу информации, для обеспечения непрерывного совершенствования СМИБ.

Для эффективного функционирования процессов СМИБ модель ПРПД применяется циклически, т.е. выполнение всех этапов регулярно повторяется.

5 Лидерство

5.1 Лидерство и обязательства руководства

5.1.1 Руководство компании приняло на себя обязательства по разработке, внедрению и улучшению СМИБ, регламентированной стандартом ISO/IEC 27001:2022, которое подтверждается:

1) изданием соответствующих организационно-распорядительных документов, определяющих ответственность и полномочия должностных лиц:

- о создании рабочей группы по СМИБ для реализации мероприятий планов работ по разработке, внедрению, поддержанию и развитию СМИБ компании;
- о введении документации СМИБ в действие;
- о проведении внутренних аудитов СМИБ и др.

2) наличием планов мероприятий по разработке и внедрению (совершенствованию) СМИБ;

3) обучением сотрудников компании по стандартам и другим инструментам системного менеджмента;

4) проведением рабочих совещаний с членами рабочей группы по СМИБ, а также – общих собраний со всеми сотрудниками в целях доведения до персонала:

- важности и значения обеспечения и повышения эффективности СМИБ компании;
- необходимости удовлетворения требований и ожиданий, а также учета интересов заинтересованных сторон в области СМИБ;
- необходимости соблюдения законодательных и других нормативных требований, относящихся к основной деятельности компании, к деятельности в области СМИБ;
- необходимости повышения квалификации персонала с целью соответствия требованиям к выполняемым заданиям;

5) разработкой и утверждением Политики в области информационной безопасности;

6) установлением конкретных целей СМИБ;

7) проведением анализа СМИБ со стороны руководства;

8) обеспечением СМИБ необходимыми финансовыми ресурсами, в том числе для:

- повышения квалификации и компетентности кадров;
- обеспечения процессов необходимым оборудованием, информационными ресурсами;
- развития применяемых производственных и управленческих технологий;
- расширения партнерских связей.

5.2 Политика в области информационной безопасности

5.2.1 Политика в области информационной безопасности была сформирована и периодически пересматривается на основании и с учетом:

- обратной связи от заинтересованных сторон;
- результатов независимых проверок;
- состояния предупреждающих и корректирующих действий;
- результатов предыдущих проверок руководства;

- эффективности процессов и соответствия политики информационной безопасности;
- изменений, которые могут повлиять на подход организации к управлению информационной безопасностью, включая изменения организационного окружения, обстоятельств бизнеса, доступности ресурсов, договорных и нормативных условий;
- тенденции, связанные с угрозами и уязвимостями;
- отчетность об инцидентах информационной безопасности;
- соблюдения законодательных требований
- рекомендаций соответствующих государственных органов.

5.2.2 Политика в области информационной безопасности включает:
- цели и задачи в области информационной безопасности;
- обязательство непрерывного улучшения системы менеджмента информационной безопасности.

5.2.3 Политика СМИБ компании доведена до сведения сотрудников, доступна для заинтересованных сторон.

5.2.3.1 Документ «Политика СМИБ» в компании издается отдельным документом и управляется в соответствии с требованиями процедуры «Управление документацией».

5.2.3.2 Доступность Политики СМИБ персоналу, потребителям, общественности и другим заинтересованным внешним сторонам обеспечивается через сайт компании в Интернет сети.

5.2.4 Политика СМИБ разъясняется персоналу компании через систему внутреннего обучения и инструктирования.

5.2.5 Политика СМИБ компании анализируются и пересматриваются высшим руководством не реже одного раза в год в соответствии с процедурой «Анализ и оценка интегрированной системы менеджмента со стороны высшего руководства» с целью обеспечения их актуальности, адекватности и пригодности к применению.

5.3 Организационные функции, ответственность и полномочия

5.3.1 Высшее руководство компании несет прямую ответственность за состояние дел в области информационной безопасности, за рабочее состояние, результативное функционирование и постоянное совершенствование СМИБ компании. Высшее руководство компании демонстрирует свои обязательства в отношении вышесказанного посредством:

1) обеспечения наличия ресурсов, необходимых для разработки, внедрения, поддержания в актуальном состоянии и улучшения СМИБ;

2) определения и делегирования обязанностей и полномочий, установления ответственности и подотчетности в целях содействия эффективному менеджменту в области СМИБ.

5.3.2 Задачи, функции, ответственность и полномочия структурных подразделений компании, в том числе и в рамках СМИБ, установлены в рамках положений о структурных подразделениях.

5.3.3 Обязанности, ответственность и полномочия высшего руководства и других работников компании, в области СМИБ, определяются в целом – в рамках должностных инструкций, карт процессов и документированных процедур СМИБ компании.

5.3.4 Ответственность и полномочия работников компании определяются и доводятся до их сведения также на основе других внутренних регламентирующих документов: положений, правил, производственных и рабочих инструкций.

5.3.5 Ответственные лица по СМИБ.

5.3.5.1 К числу ответственных лиц (подразделений) по СМИБ компании относятся:

1) Представитель руководства по СМИБ – …….;

2) Уполномоченные представители руководства по СМИБ в подразделениях;

3) внутренние аудиторы, другие члены рабочих групп по СМИБ: Владельцы процессов, ответственные по СМИБ в подразделениях.

5.3.5.2 Обязанности и полномочия ответственных лиц, подразделений и коллегиальных органов по СМИБ документально оформлены соответствующими документами.

5.3.5.3 Обязанности и полномочия внутренних аудиторов установлены в процедуре «Внутренний аудит».

6 Планирование.

6.1 Действия по обработке рисков и реализации возможностей

6.1.1 Общие положения

6.1.1.1 Установление целей, задач и планов (программ) в СМИБ уровня компании производится на основе положений политик СМИБ с учетом требований законодательно-нормативных документов, требований стандарта ISO/IEC 27001:2022 к СМИБ компании и результатов анализа:

- исходного состояния и достижений в области информационной безопасности;
- финансовых, операционных, организационных условий, технологических вариантов, а также мнений заинтересованных сторон.

6.1.1.2 Систематическое определение рисков и потенциальных возможностей

Подход Компании к управлению рискам ИБ определен, утвержден и санкционирован Руководством Компании и применяется в процессах стратегического планирования деятельности Компании. Управление рисками ИБ предназначено для идентификации и оценки рисков ИБ, определения и оценки вариантов обработки этих рисков, выбора целей контроля и контрольных мер, снижающих эти риски до приемлемого уровня в контексте планирования деятельности, операционных требований, ограничений и целей национального и международного законодательства и регулирования.

Управление рисками ИБ заключается в оценке и обработке рисков ИБ и включает в себя следующие этапы: инвентаризация и определение владельцев информационных активов, категорирование информационных активов, определение критичности уязвимостей, оценка рисков ИБ, принятие решений по обработке рисков ИБ, реализация мер обработки рисков ИБ, проверка эффективности реализованных мер, определение и внесение улучшений.

6.1.2 Оценка рисков информационной безопасности

6.1.2.1 Идентификация рисков

Инвентаризация, определение владельцев и категорирование ИА осуществляется в соответствии с процедурой «Порядок инвентаризации и категорирования информационных активов и систем».

Определение критичности уязвимостей, оценка рисков ИБ, принятие решений по обработке рисков ИБ осуществляются в соответствии с процедурой «Порядок оценки и обработки рисков информационной безопасности». Реализация мер обработки РИБ осуществляется в соответствии с утвержденным Планом Обработки РИБ.

Компания регулярно осуществляет управление рисками ИБ не реже одного раза в год, а также при внедрении новых или внесении изменений в существующие информационные системы.

6.1.2.2 Анализ и оценка рисков ИБ.

Оценка рисков ИБ осуществляются по следующим критериям:

1) Ценность ИА по КЦД, методика категорирования по ценностям приведена в процедуре «Порядок оценки и обработки рисков информационной безопасности»:

2) Критичность уязвимостей, методика определения критичности ИА приведена в процедуре «Порядок оценки и обработки рисков информационной безопасности»;

3) Степень влияния угрозы, методика определения приведена в процедуре «Порядок оценки и обработки рисков информационной безопасности»;

4) Вероятность реализации угрозы, методика определения приведена в процедуре «Порядок оценки и обработки рисков информационной безопасности».

6.1.2.3 Идентификация и оценка возможности по обработке рисков.

Определение приемлемого уровня рисков ИБ и мер обработки рисков ИБ осуществляется в соответствии с процедурой процедуре «Порядок оценки и обработки рисков информационной безопасности».

6.1.2.4 Выбор целей и механизмов контроля для обработки рисков.

Из Приложения А стандарта ISO/IEC 27001:2022 выбираются цели контролей и контрольные меры, применяемые в СМИБ и соответствующие принятым решениям по обработке рисков ИБ и фиксируются в документе «Положение применимости». По каждой не выбранной для применения цели контроля и контрольной мере указывается причина ее исключения. Любые дополнительные цели контролей и контрольные меры, которые отсутствуют в Приложении А стандарта ISO/IEC 27001:2022, но применяются в СМИБ, также фиксируются в документе «Положение применимости».

После реализации контрольных мер по обработке РИБ проверяется их эффективность и определяются возможности по внесению улучшений. Все улучшения СМИБ реализуются в виде процесса, соответствующего модели ПРПД. Этот процесс осуществляется независимо от того, рассматривается один риск или много.

Оценка эффективности мер обработки рисков ИБ производится аналогично оценке эффективности защитных мер в соответствии с методикой, описанной в процедуре процедуре «Порядок оценки и обработки рисков информационной безопасности».

Любые изменения в Плане Обработки РИБ, влекущие изменения в СМИБ, должны быть санкционированы Руководством Компании.

6.1.3 Обработка рисков информационной безопасности

План Обработки РИБ отражает решения, принятые в фазе планирования, и определяет действия Руководства Компании, ответственность и приоритеты по управлению идентифицированными рисками ИБ.

Для обработки рисков в соответствии с Планом Обработки РИБ Обществом выделяются соответствующие финансирование и ресурсы.

Обработка рисков осуществляется в соответствии с процедуре «Порядок оценки и обработки рисков информационной безопасности»

6.2 Цели в области информационной безопасности и планирование их достижения

В Политике СМИБ определены цели применения контрольных мер СМИБ. Выбранные контрольные меры реализуются для достижения этих целей. Их реализация координируется Рабочей группой СМИБ.

7 Обеспечение

7.1 Ресурсы

Компания выделяет необходимые ресурсы для эффективного управления СМИБ, включая назначение Менеджера ИБ, наём дополнительных технических/обучающих кадров, внесение требований ИБ во все должностные инструкции, а также инвестиции в продукты и сервисы по защите информации, в соответствии с Планом обработки РИБ.

7.2 Компетентность

В Компании реализуются программы обучения и повышения осведомленности работников в соответствии с Планом Обработки РИБ.

7.3 Осведомленность

В Компании осуществляется работа по поддержанию соответствующего уровня осведомленности персонала.

В Компании разработан и утвержден план обучения сотрудников в области информационной безопасности, в соответствии с которым будет производиться регулярное повышение осведомленности сотрудников в части новых требований, правил и процедур обеспечения информационной безопасности.

7.4 Коммуникация

7.4.1 Внутренние коммуникации

7.4.1.1 Внутренние коммуникации между сотрудниками компании оговорены, описаны и установлены во внутренних регламентирующих и организационно-распорядительных документах компании.

7.4.1.2 Деятельность по внутренней коммуникации в компании включает также:

- проведение совещаний руководством разных уровней с целью доведения управленческих решений в отношении СМИБ до конкретных исполнителей;
- проведение заседаний рабочей группы по вопросам выполнения планов работ по СМИБ;
- привлечение персонала в работу по разработке и согласованию документации СМИБ, в том числе политик и целей СМИБ;
- информирование персонала (ознакомление и разъяснение положений политик и целей СМИБ, требований документации СМИБ, информации о делегируемых им полномочиях и ответственности);
- вводный инструктаж при приеме на работу;
- внутреннее обучение и инструктирование персонала;
- передачу информации от руководителя до исполнителей на рабочие места и обратно;
- консультирование персонала по всем изменениям, которые могут повлиять на информационную безопасность;
- привлечение работников к рассмотрению вопросов информационной безопасности, сбор предложений по улучшению показателей в данной области;
- размещение информации на корпоративном сайте и информационных стендах компании и ее филиалов;
- сбор информации о функционировании СМИБ, показателях результативности процессов СМИБ;
- коммуникации и консультации с внутренними заинтересованными сторонами на всех стадиях процесса управления рисками в СМИБ по вопросам, касающимся рисков непосредственно, их причин, последствий и мер, принятых с целью их обработки, механизмов отчетности для поддержания процессов контроля и владения данными рисками;
- проведение внутренних аудитов СМИБ;
- доведение результатов мониторинга СМИБ, ее аудита и анализа со стороны руководства до сотрудников и другое.

7.4.1.3 Внешние коммуникации компании - это коммуникации:

- с потребителями продукции и услуг;
- с вышестоящими организациями;
- государственными органами власти;
- с заинтересованными сторонами (организации, расположенные по соседству, общественные организации, потребители, подрядчики, поставщики, посетители зоны выполнения работ компании, аварийные службы и регулирующие уполномоченные органы) по вопросам, касающимся политик СМИБ и уровней результативности и эффективности в области СМИБ;
- с заинтересованными сторонами по отработке действий на случай возникновения нештатной ситуации;
- средства массовой информации, телевидение.

7.4.1.4 В компании разработана процедура, в рамках которой описаны цели и формы внутренних и внешних коммуникаций компании.

7.5 Документированная информация

7.5.1 Общие положения

7.5.1.1 Под информационными ресурсами компании понимаются отдельные документы и отдельные массивы документов в подразделениях, архивах и электронных базах данных информационных систем компании, используемые для управления деятельностью, организации и осуществления соответствующих видов деятельности.

7.5.1.2 В рамках карт процессов СМИБ компании определены потребности в информации, «поставщики» и «потребители» информации, требования к предоставляемой информации, установлены формы, место и сроки хранения информации, формы учета и отчетности, обеспечивающие сохранение выходных данных процессов создания продукции, эффективные внутренние коммуникации, а также, накопление данных для анализа результативности и эффективности деятельности.

7.5.1.3 Информационные ресурсы на электронных носителях управляются в рамках процесса компании «Управление информационными системами» при применении требований и рекомендаций международных стандартов серии ISO 27000, а также документированной процедурой «Управление документацией».

7.5.1.4 Обеспечение конфиденциальности отдельной информации обеспечивается в компании установлением соответствующих требований в рамках трудовых договоров, заключаемых с персоналом компании, договоров, заключаемых с потребителями и поставщиками товаров, работ и услуг.

8 Функционирование

8.1 Оперативное планирование и управление

8.1.1 В Компании осуществляется планирование, осуществление и управление процессами, необходимыми для обеспечения соответствия требованиям к системе информационной безопасности.

8.1.2 В Компании выполняются запланированные действия для достижения целей, определенных в Компании.

8.1.3 В Компании реализуются процедуры управления процессами и рабочие инструкции, требуемые Политикой ИБ.

8.2 Оценка рисков информационной безопасности

8.2.1 В Компании осуществляется оценка рисков информационной безопасности с учетом критериев, установленных в процедуре «Порядок оценки и обработки рисков информационной безопасности»

8.3 Обработка рисков информационной безопасности

8.3.1 В Компании планируется и реализуется обработка рисков информационный безопасности в соответствии с процедурой «Порядок оценки и обработки рисков информационной безопасности».

9 Оценка результатов деятельности

9.1 Мониторинг, измерение, анализ и оценка

9.1.1 В Компании реализуются процедуры и контрольные меры по обеспечению мониторинга в соответствии с целями контроля.

9.1.2 Компания стремится к постоянному улучшению своей деятельности для обеспечения информационной безопасности своей производственно-хозяйственной деятельности.

9.1.3 Постоянные улучшения в компании обеспечиваются через реализацию процедур мониторинга, измерения, анализа и улучшения СМИБ.

9.1.4 Критерии мониторинга, измерений и анализа в рамках СМИБ компании приводятся в «Положении о применимости» и в процедуре «Порядок оценки и обработки рисков ИБ».

9.2 Внутренний аудит

9.2.1 В компании внедрена процедура внутреннего аудита СМИБ с целью установления того, что СМИБ:

- соответствует запланированным мероприятиям, требованиям ISO/IEC 27001:2022 и другим требованиям к СМИБ, установленным самой компанией;
- результативна, и поддерживается в рабочем состоянии.

9.2.2 Также внутренний аудит СМИБ проводится с целью выявления потенциальных возможностей для улучшения процессов и СМИБ компании в целом.

9.2.3 Внутренние проверки (аудиты) СМИБ планируются ежегодно в начале года.

9.2.4 Критерии, область применения, частота и методы внутренних аудитов, требования к аудиторам, порядку проведения и оформления результатов проверок определены и изложены в документированной процедуре «Внутренний аудит».

9.3 Анализ менеджмента

9.3.1 Высшее руководство компании регулярно проводит анализ результатов работ по разработке, внедрению и функционированию целевых систем менеджмента СМИБ и СМИБ компании в целом. Порядок проведения анализа со стороны руководства в филиале/компании в целом изложен в документированной процедуре «Анализ и оценка системы менеджмента информационной безопасности со стороны высшего руководства».

9.3.2 Входные данные анализа функционирования СМИБ со стороны руководства.

9.3.2.1 К входным данным анализа функционирования СМИБ со стороны руководства филиала/компании относятся:

1) статус мероприятий, предусмотренных предыдущим анализом;
2) изменения в состоянии внешних и внутренних проблем, которые существенны для системы менеджмента информационной безопасности;
3) информацию о функционировании системы менеджмента информационной безопасности, включая тенденции в:
   - несоответствиях и корректирующих действиях;
   - результатах мониторинга и измерений;
   - результатах аудитов; и
   - достижении целей в области информационной безопасности;
4) обратную связь от заинтересованных сторон;
5) результаты оценки рисков и статус выполнения плана обработки рисков; и
6) возможности для постоянного улучшения.

9.3.2.2 Порядок предоставления входных данных для анализа со стороны руководства изложен в ДП-07.

9.3.3 Выходные данные анализа функционирования СМИБ со стороны руководства.

9.3.3.1 В результате анализа СМИБ со стороны руководства филиала/компании могут быть приняты следующие решения по улучшению СМИБ филиала/компании:

- необходимые изменения в политиках СМИБ;
- необходимые изменения в целях, задачах, планах, программах и в других элементах СМИБ в соответствии с обязательствами компании по непрерывному улучшению СМИБ;
- необходимые ресурсы, необходимые для реализации политик, целей, задач, планов и программ.

10 Улучшение.

10.1 Несоответствия и корректирующие действия

10.1.1 В СМИБ компании регламентированы действия, в случае выявления несоответствий: фактических значений контрольных показателей процессов - нормативным значениям, действий - процедурам, основанные на выполнении процедуры корректирующих действий в отношении причин этих несоответствий в соответствии с требованиями документированной процедуры «Корректирующие действия».

10.2 Непрерывное улучшение

В компании результативность СМИБ улучшается посредством использования политик и целей СМИБ, результатов аудитов, анализа данных, корректирующих и предупреждающих действий, анализа данных и анализа со стороны руководства.

Приложения

Приложение 1

Лист регистрации изменений

Номер изменения	Номера страниц	Всего листов в документе	Номера разделов, к которым относятся изменения	Описание изменений	Отметка о внесении изменений		
					Ф.И.О.	Подпись	Дата

Лист ознакомления

№ п / п	**Ф. И О**	**Должность**	**Дата**	**Подпись**