**УТВЕРЖДЕНА**

**приказом директора**

**ТОО "Центр информационных отраслевых решений ИНТЕГРО"**

**от «\_\_\_» \_\_\_\_\_\_\_\_ 2022 г.**

**№ \_\_**

**Политика**

**Информационной Безопасности**

**ТОО "Центр информационных отраслевых решений ИНТЕГРО"**

г. Петропавловск

Содержание

Назначение документа………………………………………………………………3

Нормативные ссылки……………………………………………………………..…4

Цели и задачи обеспечения ИБ……………………………………………………..4

Основные принципы обеспечения ИБ…………………………………………..….5

Область распространения…………………………………………………….……..8

Распределение обязанностей по обеспечению ИБ………………………….……..8

Координация ИБ……………………………………………………………….…….9

Обучение и осведомленность в вопросах ИБ………………………………..…….9

Управление инцидентами……………………………………………………….…10

Управление непрерывностью бизнеса…………………………………………….10

Анализ и оценка рисков……………………………………………………………12

Пересмотр политики ИБ…………………………………………………………...12

Инвентаризация, идентификация, классификация и маркировка активов организации…………………………………………………………………………13

Процедура аудита информационной безопасности……………………………...14

Соблюдение конфиденциальности и защиты информации от неконтролируемого использования и модификации…………………………….14

Ответственность и контроль эффективности

политики информационной безопасности………..………………………………12

# Назначение документа

1. Политика информационной безопасности (далее - Политика) предназначена для определения целей и требований обеспечения информационной безопасности ТОО «Центр информационных отраслевых решений ИНТЕГРО».
2. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается предоставлением доступа к информационным ресурсам только авторизованным пользователям, целостность – обеспечивается в случае внесения изменений в данные авторизованными пользователями, доступность – в обеспечении возможности доступа к информационным ресурсам авторизованным пользователям в нужное для них время.
3. В Политике используются следующие основные термины и определения:

Товарищество – товарищество с ограниченной ответственностью «Центр информационных отраслевых решений ИНТЕГРО».

**Информационная безопасность** (далее - ИБ) – комплекс правовых, технических и организационных мероприятий, направленных на обеспечение защиты информационных ресурсов от несанкционированного доступа, преднамеренного или случайного искажения и разрушения, физического разрушения, в том числе в результате воздействий техногенного и природного характера. А также состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

**Отдел информационных технологий, внедрения и сопровождения систем** (далее – ОИТ) – структурное подразделение Товарищества, осуществляющее внедрение и сопровождение информационных ресурсов и информационных систем;

Информационная система (далее – ИС) – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

Электронные информационные ресурсы (далее - ЭИР) - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

**Администратор ИС** – работник, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования ИС Товарищества;

Пользователь **ИС** – субъект информатизации, использующий объекты информатизации для выполнения конкретной функции и (или) задачи;

**База данных** – совокупность связанных данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования, независимая от прикладных программ. База данных является информационной моделью предметной области;

**Конфиденциальность информации** – обеспечение предоставления информации только определенной категории авторизированных лиц;

**Целостность информации** – состояние информации (информационных ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только авторизованными пользователями;

**Доступность** – обеспечение возможности доступа авторизованным пользователям к информационным ресурсам автоматизированной информационной системы в нужное время.

# Нормативные ссылки

1. Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами и документами:

Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;

Постановление Правительства Республики Казахстан от 23 мая 2016 №298 «Об утверждении Правил проведения аттестации информационной системы, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа на соответствие требованиям информационной безопасности»;

Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности;

Методика проведения аттестационного обследования информационной системы, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа на соответствие требованиям информационной безопасности, утвержденная приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 54/НҚ.

СТ РК ИСО/МЭК 27002 «Методы обеспечения защиты. Свод правил по управлению защитой информации».

СТ РК ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

СТ РК ГОСТ Р 50739 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

# Цели и задачи обеспечения ИБ

1. Целью обеспечения информационной безопасности является предотвращение и минимизация ущербов от реализации угроз информационной безопасности, обеспечение более высокой привлекательности со стороны потенциальных клиентов, требующих особое отношение к информационной безопасности активов, а также повышение общего уровня конфиденциальности, целостности и доступности информации Товарищества.
2. Задачами обеспечения ИБ являются:

обеспечение непрерывности деятельности Товарищества, организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов посредством комбинации предупреждающих и восстанавливающих мер и мероприятий;

определение рисков для активов организации;

управление рисками в целях недопущения или снижения вероятности возникновения внештатных ситуаций;

защита от вмешательства посторонних лиц в процесс функционирования Товарищества;

разграничение прав доступа к информации аппаратными;

выявление и недопущение нарушений, а также условий для их реализации;

создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

защита информации от несанкционированной модификации искажения;

создание механизма оперативного мониторинга и реагирования на нарушения.

# Основные принципы обеспечения ИБ

1. Основными принципами построения и функционирования системы ИБ является принципы:

* законности – соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;
* системности – подход к вопросам ИБ должен быть логическим и последовательным: в первую очередь оценка риска ИБ исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику деятельности работников;
* эффективности – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению ИБ должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;
* целесообразности – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;
* непрерывности – принцип функционирования системы ИБ, учитывающий, что злоумышленники в любой момент времени ищут возможность обхода защитных мер, прибегая для этого к легальным и нелегальным методам;
* взаимодействии и координации – осуществление мер обеспечения ИБ на основе четкой взаимосвязи подразделений службы безопасности, информационных технологий и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания ИС, координации их усилий для достижения поставленных целей, а также взаимодействия с уполномоченными государственными органами. Эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными специалистами;
* совершенствовании – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;
* приоритетности – категорирование (ранжирование) всех информационных ресурсов КГУ по степени важности и оценка реальных, а также потенциальных угроз ИБ;
* информированности и персональной ответственности – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационные сервисы индивидуально идентифицирует пользователей и инициируемые ими процессы;
* соответствие стандартам – система ИБ должна международным стандартам в данной области;
* обязательность контроля – контроль за деятельностью пользователей, а также мониторинг работы ИС должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

1. Защита ИС и ЭИР Товарищества достигается посредством обеспечения и постоянного поддержания следующих свойств:

доступности обрабатываемой информации;

обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники (далее - СВТ) и передаваемой по каналам связи;

целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой и передаваемой по каналам связи.

1. Для обеспечения указанных свойств Товарищество должно обеспечивать эффективное решение следующих задач:

защиту от вмешательства в процесс функционирования посторонних лиц (возможность использования ИС Товарищества и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи;

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа: к информации, средствам вычислительной техники, аппаратным, программным

регистрацию действий пользователей при использовании защищаемых ресурсов в системных журналах н периодический контроль корректности действий пользователей ИС Товарищества путем анализа содержимого этих журналов ответственными работниками;

контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

защиту от несанкционированной модификации и контроль целостности ИС и ЭИР Товарищества, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

защиту конфиденциальной информации, информации с ограниченным доступом, персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

защиту конфиденциальной информации, персональных данных, информации с ограниченным доступом, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам Товарищества, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

# Область распространения

1. Действие настоящей Политики распространяется на все активы, определённые в документе Область применения политики информационной безопасности ТОО "Центр информационных отраслевых решений ИНТЕГРО" и учитывается в договорных отношениях с поставщиками услуг.
2. В целях обеспечения выполнения содержащихся в Политике нормативных правил необходимо обеспечить её соблюдение третьими сторонами. Поэтому, в соответствующих случаях все договоры субподряда должны содержать требование о соблюдении требований Политики и обеспечения ИБ. Вся деятельность, подразумевающая контакт субподрядчика с данными, содержащимися в ИС и ЭИР Товарищества, должна осуществляться в соответствии с изложенными здесь нормативными требованиями. Данное требование распространяется на всех работников субподрядчика. Выполнение данного требования является обязанностью структурного подразделения Товарищества, занимающегося подготовкой договоров.

# Распределение обязанностей по обеспечению ИБ

1. Руководство Товарищества совместно с ОИТ и Ответственным за ИБ обязано активно реализовывать комплекс мероприятий по поддержанию ИС и ЭИР Товарищества посредством дачи ясных указаний, демонстрированных обязательств, четких постановок задач и осведомленности работников об обязанностях по обеспечению ИБ:

Ответственный за ИБ обеспечивает формирование и контроль выполнения всех пунктов данной политики;

Ответственный за ИБ должен пересматривать эффективность реализации политики ИБ не менее одного раза в два года;

Ответственный за ИБ должен обеспечить четкое управление и зримую поддержку инициатив в области поддержки Системы управления информационной безопасностью;

Руководство должно обеспечивать координацию мер контроля за ИБ в Товариществе;

Руководство должно предоставлять ресурсы для обеспечения ИБ;

Руководство должно утверждать распределение специфических ролей и обязанностей по ИБ;

Ответственный за ИБ совместно с ОИТ должен инициировать планы и программы по поддержанию осведомленности об ИБ.

1. Администраторы ИС Товарищества обязаны действовать в строгом соответствии с зонами их ответственности, согласно Руководству администратора ИС Товарищества.
2. Пользователи ИС Товарищества обязаны действовать в строгом соответствии с зонами их ответственности, согласно своим должностным обязанностям, учетных ролей в ИС и Руководству пользователя ИС Товарищества.
3. Ответственный за ИБ отвечает за руководство разработкой, анализом Политики ИБ Товарищества.

# Координация ИБ

1. Действия по обеспечению ИБ должны координироваться руководством Товарищества в соответствии с их компетенцией и должностным положением.
2. Координация ИБ должна включать взаимосвязь и сотрудничество, пользователей, администраторов, разработчиков прикладного программного обеспечения и квалифицированных специалистов в таких областях, как кадровые ресурсы, информационные технологии и управление рисками. Эта деятельность должна:

Обеспечивать соответствие выполнения мероприятий по обеспечению ИБ;

Определять мероприятия по обеспечению ИБ в случае её несоответствия политике ИБ;

Утверждать методологии и процессы обеспечения ИБ, например, оценку рисков, классификацию информации;

Идентифицировать все изменения угроз ИБ и степень уязвимости информации и средств обработки информации к угрозам ИБ;

Оценивать адекватность принимаемых решений и координировать реализацию мер контроля ИБ;

Обеспечивает контроль издания и доведения до сведения утвержденных документов по ИБ и ИС разрабатываемых и используемых в организации;

Повышать профессиональный уровень пользователей за счет обучения, подготовке по ИБ и осведомленности о ней;

Оценивать информацию, полученную от мониторинга и просмотра инцидентов по ИБ и рекомендовать соответствующие мероприятия в ответ на идентифицированные инциденты ИБ.

# Обучение и осведомленность в вопросах ИБ

1. Требования к обучению и осведомленности в вопросах ИБ:

Пользователи, сотрудники ОИТ и администраторы ИС Товарищества, должны быть ознакомлены с политикой ИБ;

Ответственный за ИБ Товарищества должен проводить первичный инструктаж по ИБ;

Сотрудники ОИТ и Администратор ИС Товарищества, обеспечивающие функционирование ИС Товарищества должны проходить регулярный инструктаж по соблюдению требований ИБ;

В целях обеспечения ИБ необходимо согласовать и определить в соглашении с третьей стороной мероприятия по управлению ИБ Товарищества;

Ответственный за ИБ по мере необходимости проходит курсы по повышению квалификации по информационной безопасности, но не менее одного раза в три года;

В целях обеспечения гарантированного уведомления ответственным за ИБ, всех заинтересованных сторон об инциденте и уязвимости ИБ по отношению к ИС Товарищества должны быть реализованы формальные процедуры по уведомлению об инциденте и проявлении угроз. Для трансляции уведомлений должен быть избран способ, гарантированно позволяющий своевременно принять корректирующие меры по сохранению ИБ;

Ответственный за ИБ Товарищества должен знать процедуры уведомления, а также располагать сведениями о различных типах событий или слабых местах, которые могут влиять на безопасность ресурсов, о наступлении которых или предпосылках к таковым необходимо отправить уведомление;

Сотрудники ОИТ и Администраторы ИС Товарищества обязаны как можно быстрее сообщать о любых нарушениях в сфере ИБ ответственному лицу по ИБ;

Лица, ответственные за ИБ, должны проводить первичные инструктажи, регулярные обучения в сфере ИБ и действий при чрезвычайных ситуациях для всех работников Товарищества;

Ответственные лица по ИБ должны вести мониторинг посещения серверного помещения за сотрудниками ОИТ.

# Управление инцидентами

1. В случае обнаружения нарушения информационной безопасности следует незамедлительно доложить ответственному по ИБ.
2. Все сотрудники, подрядчики и пользователи, пользующиеся ИС и ЭИР Товарищества обязаны незамедлительно доложить ответственному по ИБ и по возможности обеспечить минимизацию ущерба.
3. В случае возникновения инцидента ИБ или другой нештатной ситуации необходимо руководствоваться «Инструкцией о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях».

# Управление непрерывностью бизнеса

1. Необходимо внедрить процесс управления непрерывностью бизнеса с целью минимизации влияния на деятельность Товарищества и восстановления после потери информационных активов (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования, и преднамеренных действий) до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью. Этот процесс должен идентифицировать важные бизнес-процессы и интегрировать требования непрерывности бизнеса управления информационной безопасностью с другими требованиями непрерывности касательно таких аспектов, как операции, кадровое обеспечение, материалы, транспорт и оборудование.
2. Последствия бедствий, нарушений безопасности, отказов в обслуживании и доступность сервисов должны быть предметом анализа степени влияния на бизнес. Необходимо разрабатывать и внедрять планы обеспечения непрерывности бизнеса с целью возобновления важных операций в течение требуемого времени при их нарушении. Информационная безопасность должна быть составной частью общего процесса непрерывности бизнеса, и других процессов управления в организации.
3. Необходимо, чтобы обеспечение управления непрерывностью бизнеса включало мероприятия по управлению информационной безопасностью для идентификации и уменьшения рисков, в дополнение к общему процессу оценки степени риска, ограничения последствий разрушительных инцидентов, и обеспечения доступности информации, требуемой для процессов бизнеса.
4. Необходимо разработать и поддерживать управляемый процесс непрерывности бизнеса для всей организации, который соответствует требованиям информационной безопасности, необходимым для обеспечения непрерывности бизнеса.
5. В процессе должны быть собраны вместе следующие ключевые элементы управления непрерывности бизнеса:

Понимание рисков, с которыми сталкивается организация, с точки зрения вероятности возникновения и последствий, включая идентификацию и определение приоритетов критических бизнес-процессов;

Определение всех активов, задействованных в критических бизнес-процессах;

Понимание возможных последствий нарушения бизнес-процессов, вызванных инцидентами нарушения информационной безопасности, в случае незначительных или существенных инцидентов, потенциально угрожающих жизнедеятельности организации, а также выбора средств и способов обработки информации, соответствующих к целям бизнеса;

Организация оптимального страхования результатов обработки информации, которое может быть частью общего процесса непрерывности бизнеса, а также частью управления операционным риском;

Определение и рассмотрение вопроса реализации дополнительных превентивных и подавляющих средств контроля;

Идентификация достаточных финансовых, организационных, технических ресурсов и ресурсов окружающей среды для соответствия идентифицированным требованиям информационной безопасности;

Обеспечение безопасности персонала и защиты средств обработки информации и собственности организации;

Формулирование и документирование планов обеспечения непрерывности бизнеса, удовлетворяющих требования информационной безопасности в соответствии с согласованной стратегией;

Регулярное тестирование и обновление планов развития информационных технологий и существующих процессов;

Обеспечение органичного включения в процессы и структуру организации планов управления непрерывностью бизнеса.

# Анализ и оценка рисков

1. Требования к анализу и оценке рисков:

Политика ИБ Товарищества первоначально должна основываться на данных, полученных в результате анализа и оценки рисков ИБ;

С целью совершенствования политики информационной безопасности Товарищества, должен проводиться ежегодный анализ и оценка рисков информационной безопасности для ИС и ЭИР Товарищества;

Анализ и оценка рисков должна проводиться в соответствии со стандартами, действующими на территории Республики Казахстан;

При оценке рисков должно учитываться влияние реализации угроз ИБ на финансовое состояние. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

# Пересмотр политики ИБ

1. Товарищество является владельцем Политики ИБ. Руководство общества утверждает административную ответственность за развитие, пересмотр и оценку политики ИБ. Пересмотр должен включать возможности оценки для улучшения политики ИБ и подход к управлению ИБ в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.
2. При пересмотре политики ИБ необходимо учитывать результаты пересмотров управления ИБ. Должны быть определены график и продолжительности пересмотра.
3. Входные данные для пересмотра управления должны включать информацию по:

Обратной связи от заинтересованных сторон;

Результатам независимых пересмотров;

Статусу превентивных и корректирующих действий;

Результатам предыдущих пересмотров;

Характеристикам процесса и соответствию политики безопасности информации;

Изменениям, которые могут повлиять на подход организации к управлению ИБ, включая изменения в законодательстве, организационной среде, деловой ситуации, наличии ресурсов, договорных, регулятивных или юридических условиях, или в технической среде;

Тенденции, связанные с угрозами и уязвимостями;

Сообщенным инцидентам с информационной безопасностью;

Рекомендациям, представленным соответствующими учреждениями.

1. Выходные данные из пересмотра управления должны включать любые решения и действия, связанные с:

Усовершенствованием подхода организации к управлению информационной безопасностью и его процессами;

Усовершенствованием целей и мер контроля;

Улучшением распределения ресурсов и/или обязанностей.

1. Пересмотр управления ИБ необходимо регистрировать.
2. Политика ИБ Товарищества должна пересматриваться в случае появления существенных изменений в целях обеспечения конфиденциальности, целостности, доступности, адекватности и эффективности.
3. Политика ИБ Товарищества должна пересматриваться не реже одного раза в два года.
4. Пересмотренная политика должна утверждаться руководством.
5. Политика должна пересматриваться в случае обнаружения недочетов или неэффективности исполнения.

# Инвентаризация, идентификация, классификация и маркировка активов организации

1. В целях эффективного управления в кризисных ситуациях, разграничения ответственности, обеспечения эффективного анализа рисков и угроз информационной безопасности производится маркировка объектов
2. Все объекты, связанные со средствами обработки информации организации должны идентифицированы, промаркированы и учтены на балансе организации при инвентаризации или иным образом учтены как взаимодействующие с информацией.
3. Маркировка объектов производится согласно документу “Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации”.
4. Процедуры учёта ПО и Техники, передачи и их утилизации описаны в документе “Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения”

# Процедура аудита информационной безопасности

1. В целях контроля качества политики информационной безопасности, оценки рисков ИБ, а также оценки навыков сотрудников в сфере ИБ производится регулярный аудит информационной безопасности.
2. Правила проведения аудита информационной безопасности утверждены в документе “Правила проведения внутреннего аудита информационной безопасности”.
3. Документ, регламентирующий правила проведения аудита должен оцениваться в рамках отдельного аудита документации после первичного аудита.

# Соблюдение конфиденциальности и защиты информации от неконтролируемого использования и модификации

1. В целях защиты информации в организации утверждены правила использования криптографических средств.
2. Для обеспечения работы со информацией только авторизованных пользователей, а так же в целях контроля рисков, связанных с неконтролируемым использованием активов в организации утверждаются правила разграничения прав доступа к ИС, правила организации процедуры организации аутентификации и правила использования электронной почты, регламентирующие инструкции по использованию ПО, связанного с информацией и средствами обработки информации.
3. Для организации защиты информации на электронных носителях в организации утверждаются правила использования съемных носителей информации, инструкции по организации антивирусной защиты, правила по обеспечению физического доступа

# Ответственность и контроль эффективности политики информационной безопасности

1. Для обеспечения необходимого уровня информационной безопасности необходимо производить постоянный контроль эффективности.
2. Руководство несет ответственность за выполнение всех пунктов данной политики.
3. Ответственность за контроль эффективности несут должностные лица ответственные за информационную безопасность.
4. Планирование и контроль состояния информационной безопасности в Товариществе несет Ответственный за ИБ.
5. В случае нарушения требований настоящей Политики ИБ все субъекты Товарищества привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

ЛИСТ ОЗНАКОМЛЕНИЯ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Фамилия, имя, отчество | Должность | Подпись | Дата |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

ЛИСТ ОЗНАКОМЛЕНИЯ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Фамилия, имя, отчество | Должность | Подпись | Дата |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

ЛИСТ ОЗНАКОМЛЕНИЯ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Фамилия, имя, отчество | Должность | Подпись | Дата |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |