|  |
| --- |
| УТВЕРЖДАЮ |
| Директор муниципалитета населенного пункта «---» |
| Начальников К.К. |
| « » 2025 г. |

**Положение**

**об отделе информационной безопасности**

1. **Общие положения**
   1. Отдел информационной безопасности (далее – ОИБ) является самостоятельным структурным подразделением муниципалитета населенного пункта «---»
   2. ОИБ подчиняется непосредственно главе отдела информационной безопасности.
   3. Подчиненность отдела приведена в виде схемы:

|  |
| --- |
| Директор муниципалитета |
|  |
| Глава отдела информационной безопасности |
|  |
| Специалисты по безопасности других отделов муниципалитета |

* 1. Структура и штат отдела утверждается приказом директора муниципалитета по представлению главы ОИБ исходя из условий, особенностей и объема работы, возложенных на отдел.
  2. ОИБ возглавляет глава отдела. Назначение на должность главы отдела и освобождение от занимаемой должности производится

приказом директора по представлению начальника управления по безопасности.

* 1. В период отсутствия начальника отдела (командировка, отпуск, больничный) его обязанности исполняет иное лицо, если принято решение о назначении исполняющего обязанности. Решение о назначении исполняющего обязанности утверждается приказом директора муниципалитета по представлению главы ОИБ. Вышеуказанное лицо приобретает соответствующие права, обязанности и несет ответственность за их ненадлежащее исполнение.
  2. ОИБ в своей деятельности руководствуется Конституцией Российской Федерации (РФ), Федеральными законами, Указами и распоряжениями Президента РФ, Постановлениями Правительства РФ, руководящими и методическими документами по информационной безопасности Федеральной службы безопасности РФ (далее – ФСБ РФ), руководящими и методическими документами по информационной безопасности Федеральной службы по техническому и экспортному контролю РФ (далее – ФСТЭК РФ), предписаниями на эксплуатацию основных и вспомогательных технических средств и систем, Уставом, приказами, регламентами и инструкциями принятыми в Компании, инструкциями по охране труда, пожарной безопасности, требованиями природоохранного законодательства РФ, правилами внутреннего трудового распорядка, распоряжениями по отделу, настоящим Положением и другими нормативными правовыми актами.
  3. Всю полноту ответственности за качество и своевременность выполнения возложенных настоящим Положением на отдел задач и функций несет начальник отдела.
  4. Ответственность работников подразделения устанавливается должностными инструкциями.
  5. Отдел реорганизуется или прекращает свою деятельность на основании приказа директора.

1. **Основные задачи**

Основными задачами ОИБ являются защита коммерческой тайны и конфиденциальной информации, персональных данных, обеспечение информационной безопасности. Основные задачи ОИБ подразделяются на следующие:

* 1. Планирование мероприятий в сфере информационной безопасности.
  2. Реализация мероприятий в сфере информационной безопасности.
  3. Контроль мероприятий в сфере информационной безопасности.
  4. Обеспечение конфиденциальности, целостности и доступности информации.
  5. Защита персональных данных граждан и служебной информации.
  6. Предотвращение утечек информации и несанкционированного доступа.
  7. Соблюдение требований законодательства РФ в области информационной безопасности.
  8. Защита критической информационной инфраструктуры, включая АСУГТ и ЭПГ.

1. **Основные функции**

ОИБ в соответствии с возложенными на него основными задачами выполняет следующие функции:

* 1. В части планирования мероприятий в сфере информационной безопасности:
     1. Изучение, анализ, оценка состояния информационной безопасности.
     2. Определение информационных и технических ресурсов, подлежащих защите.
     3. Формулировка требований по защите информации при создании и развитии объектов информатизации.
     4. Выявление угроз и уязвимостей информационной безопасности, каналов утечки информации, оценка риска и уровня сложности автоматизированных систем.
     5. Планирование текущей деятельности отдела.
     6. Планирование деятельности в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций.
  2. В части реализации мероприятий в сфере информационной безопасности:
     1. Выполнение запланированных мероприятий.
     2. Внедрение, модернизация или замена средств защиты информации и криптографических (шифровальных) средств.
     3. Испытание и приемка в эксплуатацию объектов информатизации.
     4. Разработка и внедрение нормативных и распорядительных документов.
     5. Эксплуатация объектов информатизации.
     6. Регистрация и хранение данных о событиях информационной безопасности.
     7. Осуществление повседневной, периодической и дополнительной деятельности отдела.
  3. В части контроля мероприятий в сфере информационной безопасности:
     1. Контроль исполнительской дисциплины.
     2. Контроль мер и средств защиты.
     3. Контроль соблюдения установленных правил эксплуатации.
     4. Расследование инцидентов.
     5. Внутренний и внешний аудит.
  4. В части корректирующих действий в сфере информационной безопасности:
     1. Реагирование на попытки несанкционированных действий и нарушения правил функционирования системы защиты, действия в чрезвычайных ситуациях.
     2. Выполнение восстановительных процедур после фактов нарушения информационной безопасности.
     3. Разработка предложений по совершенствованию информационной безопасности и планов мероприятий.
     4. Проведение мероприятий с сотрудниками филиала в сфере информационной безопасности.
     5. Организация обучения сотрудников ОИБ.
  5. В части взаимодействия в сфере информационной безопасности:
     1. Координация деятельности обслуживающего персонала и администраторов автоматизированных систем в части обеспечения информационной безопасности.
     2. Координация деятельности подразделений в целях защиты государственной, служебной и коммерческой тайны и персональных данных.
     3. Взаимодействие с компаниями — поставщиками решений и услуг в сфере информационной безопасности.
     4. Взаимодействие с регуляторами в сфере информационной безопасности.

1. **Организационные взаимоотношения**

ОИБ осуществляет взаимодействие со структурными подразделениями Компании по вопросам, отнесенным к сфере деятельности отдела, а также взаимодействует:

* 1. Со всеми структурными подразделениями:
* по вопросам применения перечней сведений, подлежащих защите или составляющих коммерческую тайну и конфиденциальную информацию;
* по вопросам обеспечения установленного режима конфиденциальности при обсуждении или при обработке с использованием средств вычислительной техники информации, составляющей коммерческую тайну, а также персональные данные;
* по вопросам соблюдения требований нормативных документов по информационной безопасности;
* по вопросам аттестации и эксплуатации объектов информатизации;
* по вопросам эксплуатации средств защиты информации и шифровальных (криптографических) средств;
* по вопросам модернизации средств вычислительной техники, средств защиты информации и шифровальных (криптографических) средств;
* по вопросам технологии обработки информации на объектах информатизации и в производственных технологических процессах;
* по вопросам организации занятий и консультаций с сотрудниками подразделения по обеспечению информационной безопасности.
* по вопросам оборудования помещений комплексом инженерно- технических средств охраны;
* по вопросам соблюдения требований нормативных документов по безопасности;
* по вопросам внутриобъектового и пропускного режима.
  1. С отделом информационных технологий (далее – ОИТ):
* по вопросам обеспечения информационной безопасности, использования средств вычислительной техники и технической поддержки средств связи и программного обеспечения при проектировании, создании и эксплуатации автоматизированных систем и информационных ресурсов.
  1. С бухгалтерией:
* по вопросам ввода основных средств;
* по вопросам начисления заработной платы.
  1. Со структурными подразделениями, осуществляемыми финансово- экономическую деятельность:
* по вопросам дистанционного банковского обслуживания;
* по вопросам планирования и освоения финансовых ресурсов, ввода основных средств.
  1. Со структурными подразделениями, отвечающими за метрологию, стандартизацию и менеджмент:
* по вопросам внедрения и функционирования СМК.
  1. Со структурными подразделениями по управлению персоналом:
* по вопросам подбора кадров, обучения персонала предприятия, получения периодических изданий и специальной литературы, по работе с резервом и оформлению кадровой документации;
* по вопросам движения и учёта личного состава;
* по вопросам обработки и защиты персональных данных работников;
* по правовым вопросам, связанным с подготовкой проектов приказов и других документов.
* по вопросам разработки положения о структурном подразделении, должностных инструкций;
* по вопросам организации оплаты труда;
* по вопросам планирования отпусков, условий и режимов труда и отдыха.
  1. Со структурными подразделениями, осуществляемыми договорно- юридическую деятельность:
* по правовым вопросам, связанным с подготовкой документов.
  1. С отделом документооборота (ОД):
* по вопросам обеспечения конфиденциального электронного документооборота (СКЭД);
* по вопросам управления организационно-распорядительной документацией.
  1. Со структурными подразделениями, отвечающими за промышленную безопасность, охрану труда и экологию:
* по вопросам обеспечения охраны труда и экологии;
* по вопросам функционирования СЭМ и СМПБиЗ в подразделении.
  1. С руководством предприятия по вопросам, входящим в компетенцию

ОИБ.

* 1. С соответствующими подразделениями ФСБ РФ и ФСТЭК РФ,

правоохранительными и другими ведомствами, специализированными организациями и коммерческими структурами в части разработки, согласования и проведения мероприятий по обеспечению защиты информации и оценке состояния защищенности объектов информатизации.

* 1. Согласованное взаимодействие подразделений филиала для выполнения дополнительных функций, нерегламентированных настоящим Положением, определяются отдельными документами (приказами директора филиала) на период проведения соответствующих работ или действий.

1. **Права и обязанности руководителя отдела информационной безопасности**

Права руководителя отдела информационной безопасности:

* 1. Принимать решения в рамках своей компетенции, направленные на обеспечение информационной безопасности организации.
  2. Требовать от сотрудников организации соблюдения установленных правил и норм информационной безопасности.
  3. Взаимодействовать с другими подразделениями организации для выполнения задач, связанных с информационной безопасностью.
  4. Запрашивать и получать необходимую информацию и документы от структурных подразделений организации для выполнения своих функций.
  5. Участвовать в разработке и внедрении нормативных документов, регламентирующих вопросы информационной безопасности.
  6. Представлять организацию во взаимодействии с внешними организациями (ФСБ РФ, ФСТЭК РФ, правоохранительными органами и коммерческими структурами) по вопросам информационной безопасности.
  7. Вносить предложения по совершенствованию системы информационной безопасности организации.

Обязанности руководителя отдела информационной безопасности:

* 1. Обеспечивать выполнение задач и функций, возложенных на отдел информационной безопасности.
  2. Контролировать соблюдение требований законодательства РФ, нормативных актов и внутренних документов организации в области информационной безопасности.
  3. Организовывать и проводить мероприятия по предотвращению утечек информации и несанкционированного доступа к данным.
  4. Обеспечивать своевременное реагирование на инциденты информационной безопасности и проведение расследований.
  5. Организовывать обучение сотрудников организации по вопросам информационной безопасности.
  6. Контролировать выполнение планов мероприятий по информационной безопасности и предоставлять отчеты руководству организации.
  7. Обеспечивать защиту персональных данных, коммерческой тайны и конфиденциальной информации.

1. **Показатели эффективности службы информационной безопасности**

Показатели эффективности отдела информационной безопасности**:**

* 1. Количество успешно предотвращенных инцидентов информационной безопасности за отчетный период.
  2. Уровень соблюдения требований законодательства РФ и внутренних нормативных актов в области информационной безопасности.
  3. Результаты внутренних и внешних аудитов информационной безопасности, включая оценку уровня защищенности информационных систем.
  4. Время реагирования на инциденты информационной безопасности (среднее время обнаружения и устранения угроз).
  5. Уровень защищенности критической информационной инфраструктуры организации (АСУГТ, ЭПГ и др.).
  6. Количество проведенных обучающих мероприятий для сотрудников организации по вопросам информационной безопасности.
  7. Уровень удовлетворенности руководства организации работой отдела информационной безопасности (на основе регулярных опросов и отчетов).

Методы оценки эффективности**:**

* 1. Регулярный мониторинг и анализ инцидентов информационной безопасности.
  2. Проведение внутренних аудитов и проверок на соответствие требованиям нормативных документов.
  3. Анализ отчетов о выполнении планов мероприятий по информационной безопасности.
  4. Оценка уровня защищенности информационных систем с привлечением внешних экспертов (при необходимости).
  5. Проведение тестирования на проникновение (пентестов) для оценки уязвимостей информационных систем.

Отчетность:

* 1. Руководитель отдела информационной безопасности предоставляет ежеквартальные отчеты о выполнении задач и показателях эффективности директору муниципалитета.
  2. В случае выявления критических уязвимостей или инцидентов, руководитель отдела обязан немедленно информировать руководство и предоставить план действий по устранению угроз.

|  |  |
| --- | --- |
| Разработчик |  |
| Начальник отдела | Другонач В.И. |