АДМИНИСТРАЦИЯ ПРИАЗОВСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

РАСПОРЯЖЕНИЕ

21.01.2025 № 9

пгт Приазовское

Об утверждении Положения об отделе информационных технологий и информационной безопасности Администрации Приазовского муниципального округа

В соответствии с распоряжением №169 от 26.12.2024 «Об утверждении штатных расписаний» Администрации Приазовского муниципального округа, Положением об Администрации Приазовского муниципального округа, в связи со структурными и кадровыми изменениями, в целях повышения организации работы,

РАСПОРЯЖАЮСЬ:

1. Утвердить Положение об отделе по работе информационных технологий и информационной безопасности Администрации Приазовского муниципального округа (приложение).
2. Опубликовать настоящее распоряжение на официальном сайте Приазовского муниципального округа.
2. Контроль за исполнением настоящего распоряжения оставляю за собой.
3. Настоящее распоряжение вступает в силу со дня его подписания.

Глава
муниципального округа А.С. Диковченко

УТВЕРЖДЕНО
распоряжением Администрации
Приазовского муниципального
округа
«21» 01 2025 г.

Положение
об отделе информационных технологий и информационной безопасности

1 Общие положения

1.1 Отдел информационных технологий и информационной безопасности (далее - ОИТИБ) является самостоятельным структурным подразделением Администрации Приазовского муниципального округа (далее - Учреждения).

1.2 ОИТИБ подчиняется непосредственно начальнику управления по безопасности.

1.3 Структура и штат отдела утверждается Главой муниципального округа исходя из условий, особенностей и объема работы, возложенных на отдел.

1.4 ОИТИБ возглавляет начальник отдела. Назначение на должность начальника отдела и освобождение от занимаемой должности производится приказом Главы.

1.5 В период отсутствия начальника отдела (командировка, отпуск, больничный) его обязанности исполняет консультант согласно должностной инструкции.

1.6 ОИТИБ в своей деятельности руководствуется Конституцией Российской Федерации (РФ), Федеральными законами, Указами и распоряжениями Президента РФ, Постановлениями Правительства РФ, руководящими и методическими документами поинформационной безопасности Федеральной службы безопасности РФ (далее - ФСБ РФ), руководящими и методическими документами поинформационной 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 Учреждении, инструкциями по охране труда, пожарной безопасности, требованиями природоохранного законодательства РФ, правилами внутреннего трудового распорядка, распоряжениями по отделу, настоящим Положением и другими нормативными правовыми актами.

1.7 Всю полноту ответственности за качество и своевременность

выполнения возложенных настоящим Положением на отдел задач и функций несет начальник отдела.

1.8 Ответственность работников подразделения устанавливается должностными инструкциями.

1.9 Отдел реорганизуется или прекращает свою деятельность на основании распоряжения главы муниципального округа.

1.10 В перечень специалистов, которые могут быть сотрудниками Отдела, входят инженеры и техники по защите информации, программисты, системные администраторы, другие специалисты, отвечающие за выполнение отдельных функций по защите информации.

2 Основные задачи

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

2.1.1 Планирование мероприятий в сфере информационной безопасности.

2.1.2 Реализация мероприятий в сфере информационной безопасности.

2.1.3 Контроль мероприятий в сфере информационной безопасности.

2.1.4 Корректирующие действия в сфере информационной безопасности.

2.2 Взаимодействие в сфере информационной безопасности.

3 Основные функции

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

3.2 В части планирования мероприятий в сфере информационной безопасности:

3.1.1 Изучение, анализ, оценка состояния информационной безопасности.

3.1.2 Определение информационных и технических ресурсов, подлежащих защите.

3.1.3 Формулировка требований по защите информации при создании и развитии объектов информатизации.

3.1.4 Выявление угроз и уязвимостей информационной безопасности, каналов утечки информации, оценка риска и уровня сложности автоматизированных систем.

3.1.5 Планирование текущей деятельности отдела.

3.1.6 Планирование деятельности в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций.

3.2 В части реализации мероприятий в сфере информационной безопасности:

3.2.1 Пользоваться информацией для служебного пользования, запрашивать ее у сотрудников других структурных подразделений организации.

3.2.2 Вступать во взаимодействие с органами исполнительной, законодательной и судебной власти для решения правовых вопросов, касающихся функций службы.

3.2.3 Выполнение запланированных мероприятий.

3.2.4 Внедрение, модернизация или замена средств защиты информации и криптографических (шифровальных) средств.

3.2.5 Испытание и приемка в эксплуатацию объектов информатизации.

3.2.6 Разработка и внедрение нормативных и распорядительных документов.

3.2.7 Эксплуатация объектов информатизации.

3.2.8 Регистрация и хранение данных о событиях информационной безопасности.

3.2.9 Осуществление повседневной, периодической и дополнительной деятельности отдела.

3.3 В части контроля мероприятий в сфере информационной безопасности:

3.3.1 Контроль исполнительской дисциплины.

3.3.2 Контроль мер и средств защиты.

3.3.3 Контроль соблюдения установленных правил эксплуатации.

3.3.4 Расследование инцидентов.

3.3.5 Внутренний и внешний аудит.

3.4 В части корректирующих действий в сфере информационной безопасности:

3.4.1 Реагирование на попытки несанкционированных действий и нарушения правил функционирования системы защиты, действия в чрезвычайных ситуациях.

3.4.2 Выполнение восстановительных процедур после фактов нарушения информационной безопасности.

3.4.3 Разработка предложений по совершенствованию информационной безопасности и планов мероприятий.

3.4.4 Проведение мероприятий с сотрудниками филиала в сфере информационной безопасности.

3.4.5 Организация обучения сотрудников ОИТИБ.

3.5 В части взаимодействия в сфере информационной безопасности:

3.5.1 Координация деятельности обслуживающего персонала и администраторов автоматизированных систем в части обеспечения информационной безопасности.

3.5.2 Координация деятельности подразделений в целях защиты государственной, служебной и коммерческой тайны и персональных данных.

3.5.3 Взаимодействие с компаниями — поставщиками решений и услуг в сфере информационной безопасности.

3.5.4 Взаимодействие с регуляторами в сфере информационной безопасности.

4 Организационные взаимоотношения

4.1 ОИТИБ осуществляет взаимодействие со структурными

подразделениями Учреждения по вопросам, отнесенным к сфере деятельности отдела, а также взаимодействует:

4.2 Со всеми структурными подразделениями:

4.2.1 По вопросам применения перечней сведений, подлежащих защите или составляющих коммерческую тайну и конфиденциальную информацию;

4.2.2 По вопросам обеспечения установленного режима конфиденциальности при обсуждении или при обработке с использованием средств вычислительной техники информации, составляющей коммерческую тайну, а также персональные данные;

4.2.3 По вопросам соблюдения требований нормативных документов по информационной безопасности;

4.2.4 По вопросам аттестации и эксплуатации объектов информатизации;

4.2.5 По вопросам эксплуатации средств защиты информации и шифровальных (криптографических) средств;

4.2.6 По вопросам модернизации средств вычислительной техники, средств защиты информации и шифровальных (криптографических) средств;

4.2.7 По вопросам технологии обработки информации на объектах информатизации и в производственных технологических процессах;

4.2.8 По вопросам организации занятий и консультаций с сотрудниками подразделения по обеспечению информационной безопасности.

4.2.9 По вопросам оборудования помещений комплексом инженерно-технических средств охраны;

4.2.10 По вопросам соблюдения требований нормативных документов по безопасности;

4.2.11 По вопросам внутриобъектового и пропускного режима.

4.2.12 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.

4.3 С бухгалтерией:

4.3.1 По вопросам ввода основных средств;

4.3.2 По вопросам начисления заработной платы.

4.4 Со структурными подразделениями, осуществляемыми финансово-экономическую деятельность:

4.4.1 По вопросам дистанционного банковского обслуживания;

4.4.2 По вопросам планирования и освоения финансовых ресурсов, ввода основных средств.

4.5 Со структурными подразделениями по управлению персоналом:

4.5.1 По вопросам подбора кадров, обучения персонала предприятия, получения периодических изданий и специальной литературы, по работе с резервом и оформлению кадровой документации;

4.5.2 По вопросам движения и учёта личного состава;

4.5.3 По вопросам обработки и защиты персональных данных работников;

4.5.4 По правовым вопросам, связанным с подготовкой проектов приказов и других документов.

4.5.5 По вопросам разработки положения о структурном подразделении, должностных инструкций;

4.5.6 По вопросам организации оплаты труда;

4.5.7 По вопросам планирования отпусков, условий и режимов труда и отдыха.

4.6 Со структурными подразделениями, осуществляемыми договорно-юридическую деятельность - по правовым вопросам, связанным с подготовкой документов.

4.7 С отделом документооборота (ОД):

4.7.1 По вопросам обеспечения конфиденциального электронного документооборота (СКЭД);

4.7.2 По вопросам управления организационно-распорядительной документацией.

4.8 С руководством предприятия по вопросам, входящим в компетенцию ОИТИБ.

4.9 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.