**Положение об Отделе информационной**

**безопасности организации ООО«МастерДрон»**

**Положение …**

**УТВЕРЖДАЮ**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** Борисенко А. А.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.

**1. Общие положения**

1.1. Отдел информационной безопасности (далее Отдел) представляет собой отдельное структурное подразделение организации. Он формируется, реструктуризируется и ликвидируется приказом руководства организации (директора либо другого уполномоченного лица).

1.2. Отдел находится в подчинении непосредственного начальника, которого назначает на данную должность руководитель организации. В его отсутствие управление осуществляет заместитель начальника либо другое уполномоченное лицо. Вышестоящим начальником Отдела является руководитель организации.

1.3. Работа отдела информационной безопасности выстраивается в соответствии с требованиями законодательства и иных нормативно-правовых актов, в том числе – уставной документации организации.

1.4. Обязанности работников отдела защиты информации, их полномочия и степень ответственности за сохранность информационных ресурсов организации определяются данным положением, уставной документацией организации, условиями трудового договора и должностными инструкциями.

1.5. Отдел взаимодействует с другими структурными подразделениями организации в пределах своей компетенции.

**2. Цели, задачи и функции Отдела**

2.1. Цель работы Отдела – обеспечить защиту информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения.

2.2. В задачи Отдела входит разработка и внедрение системы безопасности, а также контроль за ее работой и анализ эффективности используемых средств защиты информации.

2.3. В перечень функций отдела защиты информации входит:

* разработка комплексной системы безопасности, включающей использование разнообразных методов и способов защиты конфиденциальной информации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
* внедрение режима конфиденциальности и контроль за его соблюдением;
* взаимодействие с контрагентами, обеспечение конфиденциальности передачи данных и информации, сообщаемой партнерам в процессе открытых переговоров;
* разработка документов, предписывающих соблюдение режима конфиденциальности штатными сотрудниками организации и прикомандированными работниками;
* оценка эффективности внедренной системы защиты информационных ресурсов организации от намеренного и ненамеренного разглашения, утери, искажения, похищения;
* проведение аттестации сотрудников с последующим присвоением им необходимой степени допуска к чтению и использованию конфиденциальной информации;
* составление актов проверки техники, оборудования, помещений на предмет их соответствия требованиям безопасности;
* другие функции, выполнение которых поспособствует реализации целей и задач работы Отдела.

**3. Структура Отдела**

3.1. Сотрудников Отдела нанимают на работу в соответствии со штатным расписанием, установленным кадровой службой и согласованным с вышестоящим руководством организации. Штатное расписание разрабатывается в соответствии с целями и задачами структурного подразделения.

3.2. 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.

3.3. Обязанности работников Отдела защиты информации определяет непосредственный начальник Отдела.   
Права и обязанности

4.1. Отдел информационной безопасности уполномочен:

* контролировать работу всех сотрудников организации и следить за соблюдением режима конфиденциальности, введенного в организации;
* пользоваться информацией для служебного пользования, запрашивать ее у сотрудников других структурных подразделений организации;
* вступать во взаимодействие с органами исполнительной, законодательной и судебной власти для решения правовых вопросов, касающихся функций Отдела;
* принимать все необходимые меры для обеспечения защиты конфиденциальной информации;
* привлекать сторонних специалистов для разработки, внедрения и анализа эффективности системы защиты конфиденциальной информации;
* давать указания сотрудникам других структурных подразделений организации по вопросам, входящим в компетенцию Отдела;
* проводить внутренние служебные расследования при обнаружении фактов намеренного или ненамеренного разглашения, утери, искажения, похищения конфиденциальной информации;
* осуществлять другие действия, предусмотренные должностными инструкциями и направленные на реализацию целей и задач Отдела.

4.2. В права начальника Отдела защиты информации входит:

4.2.1. Обращаться к руководству:

* с требованиями оказания содействия в исполнении своих должностных обязанностей и прав;
* с представлениями о назначении, перемещении, увольнении работников отдела;
* с предложениями об их поощрении или наложении взысканий работников отдела;
* с предложениями по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией.

4.2.2. Знакомиться с проектами решений руководства предприятия, касающимися деятельности отдела.

4.2.3. Подписывать и визировать документы в пределах своей компетенции.

4.2.4. Осуществлять взаимодействие с руководителями всех структурных подразделений предприятия, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

4.3. В обязанности начальника Отдела информационной безопасности:

* распределять задачи между подчиненными в соответствии с их специализацией, контролировать скорость и качество их выполнения;
* участвовать в процессе подбора персонала;
* разрабатывать проекты по усовершенствованию системы защиты конфиденциальной информации;
* организовывать обучение сотрудников службы отдела защиты информации и работников других структурных подразделений организации;
* устанавливать порядок ремонтных работ, направленных на скорейшее восстановление работоспособности системы защиты информации при возникновении технических сбоев или аварий;
* координировать взаимодействие работников Отдел информационной безопасности с работниками других структурных подразделений организации.

4.4. Работники Отдела информационной безопасности:

* контролировать работу всех сотрудников организации и следить за соблюдением режима конфиденциальности;
* проводить профилактику намеренного или ненамеренного разглашения, утери, искажения, похищения конфиденциальной информации путем проведения инструктажа сотрудников организации;
* участвовать в разработке комплексной системы защиты конфиденциальной информации;
* периодически проверять журналы инструктажа и оборудование организации;
* проводить аттестацию всех сотрудников организации, проверять их знания в области существующих методов превентивной защиты конфиденциальной информации;
* выполнять другую работу, направленную на реализацию целей и задач Отдела информационной безопасности.

**5. Показатели эффективности работы Отдела информационной безопасности**

5.1. Количество выявленных и предотвращенных инцидентов.  
5.2. Уровень соответствия требованиям законодательства и стандартов ИБ.  
5.3. Количество проведенных обучающих мероприятий.  
5.4. Уровень защищенности ИТ-инфраструктуры по результатам аудитов.

**6. Взаимоотношения Отдела с другими структурными подразделениями организации**

Отдел защиты информации в пределах свой компетенции взаимодействует с:

6.1. Кадровой службой (для участия в собеседованиях с соискателями на должности, предусматривающими допуск к конфиденциальной информации, отражения в личных делах результатов аттестации и сведений о выявленных нарушениях режима конфиденциальности, изучения личных дел сотрудников организации).

6.2. Бухгалтерией (для предоставления информации о льготах и надбавках, предусмотренных для сотрудников с допуском к конфиденциальной информации, получения информации о расходовании фонда оплаты труда и других данных, необходимых в работе Отдела информационной безопасности).

6.3. Финансовой службой (для предоставления плановой документации, касающейся закупки необходимого оборудования).

6.4. Юридическим отделом (для своевременного изучения изменений законодательства, касающихся защиты информации, а также для применения законодательно обоснованных наказаний за нарушение режима конфиденциальности).

6.5. Другими структурными подразделениями (для координации их работы и обеспечения необходимого уровня защиты конфиденциальной информации).

6.6 Государственными регуляторами (ФСТЭК, ФСБ, Роскомнадзор).

6.7 Независимыми аудиторами.

**РАЗРАБОТАЛ**

Начальник ОИБ \_\_\_\_\_\_\_\_ …

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.

**СОГЛАСОВАНО**

Кадровая служба \_\_\_\_\_\_\_\_ …

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.

Юридический отдел \_\_\_\_\_\_\_\_ …

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г.