Приложение 1

к распоряжению

Администрации муниципального

района Исаклинский от 13.11.2019 г. № 33-р

ОБЯЗАННОСТИ

ответственного за обеспечение безопасности персональных данных в Администрации муниципального района Исаклинский

**1. Общие положения**

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности.

1.2. Администратор информационной безопасности назначается из числа сотрудников отдела информационных технологий Администрации муниципального района Исаклинский.

1.3. Администратор информационной безопасности подчиняется начальнику аппарата Администрации муниципального района Исаклинский, осуществляющему текущее руководство системой защиты информации.

1.4. Администратор информационной безопасности осуществляет контроль выполнения требований и предусмотренных Планом защиты автоматизированных систем (АС) организационных мероприятий по обеспечению безопасности информации при использовании персональных ЭВМ.

1.5. Методическое руководство работой администратора информационной безопасности осуществляется управлением информационной безопасности департамента информационных технологий и связи Самарской области.

**2. Обязанности администратора информационной безопасности**

2.1. Проводить инструктаж пользователей по правилам работы в АС в пределах компетенции этих пользователей;

2.2. Немедленно докладывать начальнику аппарата Администрации или лицу, исполняющему его обязанности, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности на объектах информатизации (ОИ);

2.3. Контролировать соблюдение пользователями АС установленных правил и параметров печати, регистрации и учета документов, а также регистрации и учета бумажных и машинных носителей информации;

2.4. Проводить совещательные мероприятия и инструктажи, направленные на:

- повышение уровня квалификации сотрудников в области информационной безопасности;

- разъяснение сотрудникам организации требований организационно-распорядительной документации и правил работы в ИСПДн;

- разъяснение порядка использования съёмных носителей информации.

Инструктажи должны проводиться периодически (не реже одного раза в полгода), а так же при возникновении нештатных ситуаций.

Запрещается допускать к работе с защищаемой информацией и средствами ЗИ сотрудников организации не прошедших инструктажа по правилам работы в ИСПДн;

2.5. Осуществлять контроль требований защиты информации при проведении технического обслуживания и ремонта аппаратных средств ИСПДн;

2.6. Вести «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств рабочих станций (РС) подразделения»;

2.7. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию РС подразделения;

2.8. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

2.9. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам ПЭВМ. При выявлении таковых сообщать о них начальнику аппарата Администрации.

**3. Права администратора информационной безопасности**

3.1. Требовать от сотрудников подразделений - пользователей АС соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в АС.

3.2. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС.

3.3. Обращаться к руководителям подразделений с требованием прекращения работы в АС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.4. Предлагать своему непосредственному руководителю проведение мероприятий по совершенствованию технологических мер защиты на своем участке работы.

**4. Ответственность администратора информационной безопасности**

4.1. На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в Администрации муниципального района Исаклинский.

4.2. Администратор информационной безопасности несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.