Приложение №8 к приказу №104 от «07» 02 2020 г.

# ИНСТРУКЦИЯ АДМИНИСТРАТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# 1. ВВЕДЕНИЕ

1.1. Настоящая инструкция определяет общие функции, права и обязанности администратора безопасности по вопросам обеспечения информационной безопасности при подготовке и обработки персональных данных на ПЭВМ, входящих в состав информационной системы персональных данных (ИСПДн).

1.2. Администратор безопасности информации назначается из числа сотрудников и обеспечивает правильное использование и функционирование установленных средств защиты информации (СЗИ) от несанкционированного доступа (НСД).

1.3. Настоящая Инструкция разработана на основании действующих нормативных документов по защите персональных данных.

# 2. ОСНОВНЫЕ ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Контроль за выполнением требований, действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на ПЭВМ.

2.2. Обеспечение управления учетными записями ИСПДН (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

2.3. Своевременное обеспечение корректировки разрешительной системы доступа:

2.4. - изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);

2.5. - изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

2.6. Корректировка разрешительной системы доступа осуществляется на основании служебной записки руководителя подразделения, в котором числится пользователь, на начальника отдела АСУ.

2.7. Контроль доступа пользователей к работе в ИСПДн (в соответствии с Перечнем должностей, допущенных к обработке персональных данных), выдача машинных носителей информации (для обработки на них персональных данных) и соблюдение пользователями требований нормативных и руководящих документов (в том числе путем просмотра системных журналов).

2.8. Контроль за вскрытием и ремонтом (модернизацией) ПЭВМ, недопущением доступа посторонних лиц к конфиденциальной информации во время вскрытия, ремонта, модернизации ПЭВМ.

## 3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

3.1. Требовать от сотрудников соблюдения установленной технологии обработки конфиденциальной информации и исполнения требований, действующих нормативных и руководящих документов по защите персональных данных, при проведении работ на ПЭВМ.

3.2. Участвовать в анализе ситуаций, касающихся функционирования СЗИ и расследованиях фактов (попыток) НСД.

3.3. Требовать от пользователей прекращения обработки информации в ИСПДн в случае:

- нарушения установленного порядка работ;
- нарушения работоспособности средств и систем защиты информации;
- получения информации о возможном проведении технической разведки в отношении ИСПДн.

## 4. ОБЯЗАННОСТИ АДМИНИСТРАТОР БЕЗОПАСНОСТИ

4.1. Обеспечивать правильное функционирование и поддерживать работоспособность средств СЗИ от НСД в пределах возложенных на него функций.

4.2. В случае отказа СЗИ от НСД принимать меры по их восстановлению.

4.3. Проводить инструктаж пользователей по правилам работы на ПЭВМ, с установленной СЗИ от НСД.

4.4. Немедленно докладывать начальнику отдела АСУ о фактах и попытках НСД к персональным данным, о неправомерных действиях пользователей и иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

4.5. Вносить изменения в документацию ИСПДн в соответствии с требованиями нормативных документов в части, касающейся СЗИ от НСД.

4.6. Проводить работы по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению.

4.7. Обеспечить обновление антивирусных баз не реже одного раза в неделю.

4.8. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать начальнику отдела АСУ.

4.9. Обеспечивать введение полномочий работников в разрешительную систему доступа, своевременную корректировку.

4.10. Регистрировать факты выдачи машинных носителей для обработки на них персональных данных в Журнале учета машинных носителей информации.

4.11. Требовать от пользователей прекращения обработки информации ИСПДн при появлении информации о возможном проведении технической разведки в отношении ИСПДн.

4.12. Контролировать действия пользователей по правильности затирания информации на машинных носителях информации.