**Приложение № 3**
**к Приказу от 05 февраля 2013 года № 19-П**
**«О проведении работ по защите персональных данных»**

# ИНСТРУКЦИЯ
## администратора по информационной безопасности в Отраслевом институте «Омскгазтехнология»

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 (далее по тексту-ИСПДн).

Администратор безопасности информации назначается из числа сотрудников Отраслевого института «Омскгазтехнология» (далее - институт) и обеспечивает за правильное использование и функционирование установленных средств защиты информации (далее по тексту - СЗИ) от несанкционированного доступа (далее по тексту - НСД).

Администратор безопасности информации имеет все права администратора СЗИ от НСД.

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

**1. Основные функции администратора по информационной безопасности.**

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

1.2. Работа с учетными записями пользователей ИСПДн (удаление, регистрация новых пользователей), их правильная настройка и разграничение прав доступа пользователей к защищаемым ресурсам ИСПДн согласно разрешительной системе доступа.

1.3. Своевременная корректировка разрешительной системы доступа:

- изменение списка постоянных пользователей ИСПДн (ввод или удаление пользователя из ИСПДн);
- изменение прав доступа к защищаемым программным ресурсам или портам ввода-вывода ИСПДн.

1.4. Корректировка разрешительной системы доступа осуществляется на основании служебной записки пользователя, согласованной с ответственным за эксплуатацию объекта и утвержденной директором института.

1.5. Контроль доступа пользователей к работе на ПЭВМ (в соответствии со списком допущенных сотрудников), выдача внешних носителей информации и соблюдения пользователями требований нормативных и руководящих документов.

1.6. Проведение в установленные сроки смены личных паролей пользователями ИСПДн для доступа к ПЭВМ.

1.7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе на ПЭВМ, в том числе и в части периодического контроля за печатью файлов пользователей на принтере и соблюдением

установленных правил и параметров регистрации и учета документов, бумажных и машинных носителей информации.

1.8. Сопровождение подсистемы обеспечения целостности информации на ПЭВМ:

- периодический контроль за отсутствием на жестком магнитном диске ПЭВМ остаточной информации по окончании работы пользователей;
- поддержание установленного порядка и правил антивирусной защиты информации, обрабатываемой на ПЭВМ;
- контроль за соблюдением пользователями инструкции по антивирусному контролю.

1.9. Контроль за наличием и целостностью пломб (печатей, специальных защитных знаков) на корпусе ПЭВМ и устройств.

1.10. Контроль за вскрытием и ремонтом (модернизацией) ПЭВМ, недопущением доступа посторонних лиц к конфиденциальной информации во время вскрытия, ремонта, модернизации ПЭВМ или устройств, последующим опечатыванием ПЭВМ (устройств), составлением соответствующих актов.

1.11. Контроль срока действия сертификатов соответствия ФСТЭК России на средства защиты от несанкционированного доступа, установленных на ИСПДн.

**2. Администратор безопасности имеет право:**

2.1. Требовать от сотрудников института соблюдения установленной технологии обработки конфиденциальной информации и исполнения настоящей Инструкции.

2.2. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и расследованиях фактов (попыток) несанкционированного доступа;

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

- нарушения установленного порядка работ;
- нарушения работоспособности средств и систем защиты информации или окончания срока действия сертификатов соответствия ФСБ России или ФСТЭК России;
- получения информации о возможном проведении технической разведки в отношении ИСПДн.

**3. Администратор безопасности обязан:**

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

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

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

3.4. Немедленно докладывать директору института или лицу, исполняющему его обязанности, о фактах и попытках несанкционированного доступа к персональным данным, о неправомерных действиях пользователей или иных лиц, приводящих к нарушению требований по защите информации, а также об иных нарушениях требований информационной безопасности ИСПДн.

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

3.6. Проводить работу по выявлению возможных каналов утечки конфиденциальной информации, вести их учёт и принимать меры к их устранению;
3.7. Осуществлять не реже одного раза в неделю обновление антивирусных баз на ПЭВМ в ИСПДн;
3.8. Контролировать целостность (неизменность, сохранность) программного обеспечения, разрешительной системы доступа, а при обнаружении фактов изменения проверяемых параметров немедленно докладывать по подчинённости;
3.9. Вводить полномочия работников в разрешительную систему доступа, обеспечивать их своевременную корректировку;
3.10. Регистрировать факты выдачи внешних носителей в журнале учета выдачи внешних носителей.
3.11. Требовать от пользователей прекращения обработки информации ИСПДн при появлении информации о возможном проведении технической разведки в отношении ИСПДн.
3.12. Заблокировать учетные записи пользователей на ПЭВМ в случае окончания срока действия сертификата соответствия ФСТЭК России, ФСБ России на любое СЗИ, из используемых в ИСПДн, до момента его продления. В случае не продления сертификата соответствия ФСТЭК России на СЗИ он обязан поставить в известность орган по аттестации, проводивший аттестацию ИСПДн, для принятия совместного решения.
3.13. Контролировать действия пользователей по правильности затирания информации на внешних накопителях информации.

РАЗРАБОТАЛ:
Руководитель группы
по работе с персоналом