Приложение 4

к Положению информационной

безопасности об организации

и обеспечении безопасности

персональных данных в администрации

Нефтекумского муниципального округа

Ставропольского края

ИНСТРУКЦИЯ

пользователя по обеспечению информационной безопасности

при работе с персональными данными, при их обработке в информационных системах персональных данных администрации Нефтекумского муниципального округа Ставропольского края

Список сокращений

|  |  |
| --- | --- |
| ИБ | Информационная безопасность |
| АРМ | Автоматизированное рабочее место |
| ИСПДн | Информационная система персональных данных |
| НСД | Несанкционированный доступ |
| ПЭВМ | Персональная электронная вычислительная машина |

1. Общие положения

1.1. Инструкция пользователя информационных систем (далее Инструкция) устанавливает обязанности, права и порядок работы пользователей в администрации Нефтекумского муниципального округа Ставропольского края (далее - Администрации).

Ознакомление с требованиями инструкции проводит администратор информационной безопасности персональных данных в Администрации.

2. Функции и обязанности пользователей

2.1. Каждый работник Администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем, несет персональную ответственность за свои действия и обязан:

1) знать и строго соблюдать требования законодательства Российской Федерации в области защиты ПДн, для ознакомления с действующими нормативно-правовыми документами обращаться к администратору информационной безопасности;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;

3) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

4) выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке.

5) хранить в тайне свой пароль (пароли);

6) исполнять требования "Порядка парольной защиты в информационных системах Администрации, "Инструкции по организации антивирусной защиты информационных систем Администрации, а также других документов регламентирующих вопросы работы в ИС;

7) немедленно ставить в известность администратора ИБ и начальника отдела в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей;

8) немедленно ставить в известность администратора ИСПДн при обнаружении;

9) при подозрении на совершение попыток несанкционированного доступа к ПЭВМ;

10) при обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

11) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

12) некорректного функционирования установленных технических средств защиты информации.

2.2. В случае если на ПЭВМ производится обработка защищаемой (конфиденциальной) информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в подразделении.

2.3. Работникам категорически запрещается:

использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

хранить и обрабатывать личную информацию на ПЭВМ и серверах ИСПДн;

использовать информационные ресурсы Internet, содержание которых нарушает действующее законодательство Российской Федерации;

использовать информационные ресурсы Internet для целей, не связанных с областью производственной деятельности пользователя;

использовать информационные ресурсы Internet в личных целях;

вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;

оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД;

оставлять без личного присмотра на рабочем месте или где бы то ни было свои реквизиты доступа;

оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие конфиденциальную информацию (сведения ограниченного распространения);

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты. Об обнаружении такого рода ошибок - ставить в известность Администратора ИБ и руководителя своего подразделения;

3. Порядок пересмотра инструкции

3.1. Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Администрации, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных Администрации с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Администрации.

Частичный пересмотр данного документа проводится ответственным за обеспечение безопасности персональных данных в Администрации с обязательным указанием оснований и внесенных изменений.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. Ответственные за контроль выполнения инструкции

4.1. Ответственными за постоянный контроль выполнения требований данной Инструкции в своих областях ответственности являются:

Администраторы ИБ.

Администраторы ИСПДн.

\_\_\_\_\_\_\_\_\_\_\_\_\_