ДЕПАРТАМЕНТ ОБЩЕСТВЕННЫХ СВЯЗЕЙ
ТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА - ЮГРЫ

П Р И К А З

Об утверждении Инструкции о порядке работы пользователей формационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Департамента общественных связей Ханты-Мансийского автономного округа - Югры

» августа 2013 г. № 206

нты-Мансийск

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О сональных данных», постановлением Правительства Российской ерации от 17.11.2007 № 781 «Об утверждении положения об печении безопасности персональных данных при их обработке в ормационных системах персональных данных»

ПРИКАЗЫВАЮ:

1.Утвердить прилагаемую Инструкцию о порядке работы ьзователей информационных систем персональных данных в части спечения безопасности персональных данных при их обработке в ормационных системах персональных данных Департамента щественных связей Ханты-Мансийского автономного округа - Югры гласно приложению.

2.Организационному отделу довести настоящий приказ до сведения трудников Административного управления Департамента щественных связей Ханты-Мансийского автономного округа - Югры.

3.Контроль за исполнением приказа оставляю за собой.

ректор Департамента И.А. Верховский

Приложение к приказу
Департамента общественных связей Югры
от 20.08.13 № 206

Инструкция

порядке работы пользователей информационных систем персональных данных в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Департамента общественных связей Ханты-Мансийского автономного округа – Югры (далее – инструкция)

1.Настоящая инструкция определяет порядок действий пользователей формационных систем персональных данных (далее – ИСПДн) в части еспечения безопасности персональных данных при их обработке в СПДн.

2.Допуск пользователей для работы за автоматизированным рабочим стом (далее – АРМ) осуществляется на основании утверждаемого писка сотрудников, доступ которых к персональным данным, рабатываемым в информационных системах персональных данных, ходим для выполнения служебных обязанностей» Департамента ественных связей Ханты-Мансийского автономного округа – Югры.

3.Пользователь ИСПДн имеет право в отведенное ему время решать тавленные задачи в соответствии с полномочиями доступа к ресурсам ПДн. При этом для хранения информации, содержащей ПДн, решается использовать только машинные носители информации, енные в «Журнале учета машинных носителей информации, ользующихся в ИСПДн для обработки, хранения, транспортировки ормации».

4.Пользователь несет ответственность за правильность включения и лючения АРМ, входа в систему и все действия при работе в ИСПДн.

5.Вход пользователя в систему может осуществляться по выдаваемому электронному идентификатору или по персональному паролю.

6.Запись информации, содержащей персональные данные, может, ществляться пользователем ИСПДн на съемные машинные носители ормации, соответствующим образом учтенные в «Журнале учета инных носителей информации, использующихся в ИСПДн для аботки, хранения, транспортировки информации».

7.При работе со съемными машинными носителями информации ьзователь каждый раз перед началом работы обязан проверить их на утствие вирусов и иных вредоносных программ с использованием

ных антивирусных средств, установленных на АРМ. В случае ружения вирусов либо вредоносных программ пользователь ИСПДн ан немедленно прекратить их использование и действовать в ветствии с требованиями Инструкции по организации антивирусной ты.

Каждый сотрудник, участвующий в рамках своих служебных анностей в процессах обработки персональных данных в ИСПДн и ющий доступ к АРМ, программному обеспечению и данным ИСПДн, т персональную ответственность за свои действия и обязан:

.1.строго соблюдать установленные соответствующими трукциями правила обеспечения безопасности информации ИСПДн;

.2.знать и строго выполнять правила работы со средствами защиты рмации, установленными на АРМ;

.3.хранить в тайне свой пароль (пароли). Выполнять требования трукции по организации парольной защиты в полном объеме;

.4.хранить в установленном порядке свое индивидуальное устройство нтификации (ключ) и другие реквизиты в сейфе (металлическом фу);

.5.выполнять требования Инструкции по организации антивирусной ты в полном объеме;

.6.немедленно известить администратора безопасности информации в ПДн в случае утери индивидуального устройства идентификации оча) или при подозрении компрометации личных ключей и паролей, а же при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

9.Пользователю АРМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.);
- оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.