АДМИНИСТРАЦИЯ КЫШТЫМСКОГО ГОРОДСКОГО ОКРУГА
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

«31» 10 2011 г. №2861 г. Кыштым

Об утверждении Положения об организации
и проведении работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
в Администрации Кыштымского городского округа

Во исполнение Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

ПОСТАНОВЛЯЮ:

1. Утвердить Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Кыштымского городского округа (прилагается).
2. Опубликовать настоящее постановление на официальном сайте Администрации Кыштымского городского округа в сети Интернет.
3. Организацию исполнения настоящего постановления возложить на ведущего специалиста по технической защите информации отдела мобилизационной работы Администрации Кыштымского городского округа Сычеву Н.А.
4. Контроль за исполнением настоящего постановления возложить на исполняющего обязанности начальника отдела мобилизационной работы Администрации Кыштымского городского округа Серышева Н.Л.

Глава Кыштымского городского округа Л.А. Шеболаева

10

Утверждено
постановлением Администрации
Кыштымского городского округа
от 31.10. 2011 г. № 2861

Положение
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Кыштымского городского округа

1. Общие положения

1. Данное Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации Кыштымского городского округа (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Положение определяет порядок работы муниципальных служащих и работников Администрации Кыштымского городского округа (далее-пользователь) в информационных системах персональных данных (далее - ИСПДн) в части обеспечения безопасности персональных данных (далее – ПДн) при их обработке, порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации, порядок контроля ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, правила антивирусной защиты, правила парольной защиты, правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, порядок охраны и допуска посторонних лиц в защищаемые помещения, порядок уничтожения носителей персональных данных, порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

2. Порядок работы пользователей в ИСПДн в части обеспечения безопасности ПДн при их обработке

3. Настоящий порядок определяет действия пользователей в ИСПДн в части обеспечения безопасности ПДн при их обработке.

4. Допуск пользователей к работе в ИСПДн осуществляется на основании распоряжения Администрации Кыштымского городского округа и в

соответствии со списком лиц, допущенных к работе в ИСПДн.

5. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

6. Пользователь несет ответственность за правильность включения и выключения ПЭВМ, входа в систему и все действия при работе в ИСПДн.

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

8. Запись информации, содержащей ПДн, может осуществляться пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

9. Каждый пользователь, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

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

2) знать и выполнять правила работы со средствами защиты информации, установленными на ПЭВМ (если такие имеются);

3) хранить в тайне свой пароль (пароли);

4) хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу); 5) выполнять требования Инструкции по организации антивирусной защиты в полном объеме.

6) известить администратора безопасности ИСПДн и ведущего специалиста по технической защите информации отдела мобилизационной работы Администрации Кыштымского городского округа (далее — ведущий специалист по технической защите информации) в следующих случаях:

при утере индивидуального устройства идентификации (ключа);

при подозрении компрометации личных ключей и паролей;

при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данной защищенной ПЭВМ;

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

при отклонениях в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (принтера и т.п.), а также перебоев в системе электроснабжения;

при некорректном функционировании установленных на ПЭВМ технических средств защиты;

при непредусмотренных отводах кабелей и подключенных устройств.

10. Пользователю ПЭВМ категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

2) 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 ПЭВМ;

3) осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

5) оставлять включенной без присмотра ПЭВМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

6) оставлять без личного присмотра на рабочем месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

7) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

8) размещать средства ИСПДн так, чтобы в них существовала возможность визуального считывания информации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации

11. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации.

12. К использованию для создания резервной копии в ИСПДн, допускаются только зарегистрированные носители конфиденциальной информации.

13. Постоянный пользователь обязан осуществлять периодическое резервное копирование конфиденциальной информации.

14. Перед резервным копированием пользователь обязан проверить электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель) на отсутствие вирусов.

15. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

16. Запрещается запись посторонней информации на электронные носители (ЖМД, ГМД, CD-ROM, USB накопитель и другие) резервной копии.

17. Порядок создания резервной копии:

вставить в ПЭВМ зарегистрированный электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель, другие) для резервного копирования;

выбрать необходимый каталог (файл) для создания резервного архива;

нажать по выбранному каталогу (файлу) правой кнопкой манипулятора и в появившемся меню выбрать пункт «Добавить в архив…»;

на вкладке «Общие» нажать на кнопку «Обзор» и в появившемся окне перейти на электронный носитель (ЖМД, ГМД, CD-ROM, USB накопитель), после чего нажать кнопку «Открыть»;

на вкладке «Общие» в поле «Имя архива» ввести имя архива следующего вида: «Имя каталога (файла) резервного копирования. Дата архивирования. Имя пользователя;

нажать кнопку «ОК».

18. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на пользователя.

19. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности ИСПДн.

20. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее - СЗИ) возлагается на ведущего специалиста по технической защите информации.

21. Администратор безопасности ИСПДн обязан:

знать состав основных и вспомогательных технических систем и средств, (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДН;

контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных ПЭВМ и других устройствах;

производить необходимые настройки подсистемы управления доступом установленных в ИСПДН СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

проводить инструктаж сотрудников - пользователей ПЭВМ по правилам работы с используемыми техническими средствами и системами защиты информации;

контролировать своевременное (не реже чем один раз в течение 180 дней) проведение смены паролей для доступа пользователей к ПЭВМ;

осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе на ПЭВМ;

вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;

проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок (далее - ПЭМИН), контролировать соблюдение требований по размещению и использованию ПЭВМ, указанных в техническом паспорте;

контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

сообщать ведущему специалисту по технической защите информации о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

22. Ведущий специалист по технической защите информации имеет право:

требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ОВТ;

требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4. Порядок контроля ИСПДн

23. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

24. Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в структурных подразделениях администрации муниципального района учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

выявление демаскирующих признаков объектов ИСПДн;

уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн организации;

разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

25. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах организации, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

26. В ходе контроля проверяются:

соответствие принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн);

своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

эффективность применения организационных и технических мероприятий по защите информации;

устранение ранее выявленных недостатков.

Кроме того, могут проводятся необходимые измерения и расчеты, приглашенными для этих целей специалистами органа по аттестации ИСПДн.

27. Основными видами технического контроля на объекте организации являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

28. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее — предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование.

Для проведения расследования назначается комиссия, которая должна установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению.

29. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты.

30. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год.

31. Обследование объектов информатизации проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требований по защите информации, установленным для аттестованных ИСПДн в «Аттестате соответствия», для неаттестованных ИСПДн — в руководящих документах по информационной безопасности.

32. В ходе обследования проверяется:

соответствие класса обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

соблюдение организационно-режимных требований защищаемых помещений;

сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

наличие электробытовой, радио и телевизионной аппаратуры и устройств иностранного и непромышленного изготовления, которые могут способствовать возникновению каналов утечки информации;

выполнение требований предписаний на эксплуатацию основных технических средств и систем по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;

соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в техническом паспорте;

выполнение требований по защите автоматизированных систем от несанкционированного доступа;

выполнение требований по антивирусной защите.

33. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы и т.д.;

вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;

проверить качество установки стеклопакетов оконных приемов;

провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры).

34. Периодический контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России в соответствии с действующим законодательством Российской Федерации. Доступ представителя указанного федерального органа исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, справки о допуске, а также предписания установленной формы на право проведения проверки.

5. Порядок проверки электронного журнала обращений к ИСПДн

35. Настоящая глава Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

36. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к конфиденциальной информации в ИСПДн.

37. Право проверки электронного журнала обращений имеют:

ведущий специалист по технической защите информации;

сотрудники отдела информационных технологий и телекоммуникаций;

администратор безопасности ИСПДн.

38. В ИСПДн, где установлены средства защиты информации (далее - СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

39. В ИСПДн, где защита от несанкционированного доступа (далее - НСД) реализована организационно-распорядительными мероприятиями, проверка электронного журнала обращений проводится внутренними средствами операционной системы по следующему пути C:\Documents and Settings\ *UserAccoun* \Recent, при этом рекомендуется в настройках данного каталога изменить настройки «Доступ» и «Безопасность» только в пользу Администратора ПЭВМ для разграничения прав доступа.

6. Правила антивирусной защиты

40. Правила антивирусной защиты определяются Инструкцией по организации антивирусной защиты на объектах информатизации Администрации Кыштымского городского округа, утвержденной правовым актом Администрации Кыштымского городского округа.

7. Правила парольной защиты

41. Правила регламентирующие организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями определяются Инструкцией пользователя автоматизированного рабочего места, на котором осуществляется обработка персональных данных, утвержденной правовым актом Администрации Кыштымского городского округа.

42. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ведущего специалиста по технической защите информации.

8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

43. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

44. Все изменения конфигураций технических и программных средств ПЭВМ должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИСПДн.

45. Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ПЭВМ предоставляется:

в отношении системных и прикладных программных средств — для аттестованных ИСПДн администратору безопасности по согласованию с органом по аттестации, для неаттестованных ИСПДн администратору безопасности по согласованию с ведущим специалистом по технической защите информации;

в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты для аттестованных ИСПДн - сотрудникам органа по аттестации ИСПДн.

46. Изменение конфигурации аппаратно-программных средств ПЭВМ другими лицам, кроме вышеперечисленных уполномоченных сотрудников и подразделений, запрещено.

47. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ПЭВМ инициируется заявкой ответственного за эксплуатацию ИСПДн.

48. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ПЭВМ подразделения:

установка (развертывание) на ПЭВМ программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

обновление (замена) на ПЭВМ программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

удаление с ПЭВМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной ПЭВМ).

Также в заявке указывается условное наименование ИСПДн.

49. Заявку рассматривает ведущий специалист по технической защите информации, обозначая тем самым производственную необходимость проведения указанных в заявке изменений.

После этого заявка передается в отдел информационных технологий и телекоммуникаций для непосредственного исполнения работ по внесению изменений в конфигурацию ПЭВМ, указанного в заявке ИСПДн.

50. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения аттестованных ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на ПЭВМ, (обновление) и удаление системных и прикладных программных средств производится уполномоченными специалистами органа по аттестации. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

51. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

52. Установка и обновление ПО (системного, тестового и т.п.) на ПЭВМ производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

53. Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

54. После установки (обновления) ПО, администратор безопасности либо ведущий специалист по технической защите информации должен произвести требуемые настройки средств управления доступом к компонентам ПЭВМ и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

55. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ»:

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

56. При возникновении ситуаций, требующих передачи ПЭВМ в ремонт, ответственный за ее эксплуатацию докладывает об этом ведущему специалисту по технической защите информации.

В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

Заявки должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств ПЭВМ» в отделе мобилизационной работы.

57. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью начальника отдела мобилизационной работы.

58. С целью соблюдения принципа персональной ответственности за свои действия каждому пользователю, допущенному к работе на ПЭВМ конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данной ПЭВМ.

59. Использование несколькими пользователями при работе на ПЭВМ одного и того же имени пользователя («группового имени») запрещено.

60. Процедура регистрации (создания учетной записи) пользователя и предоставления (изменения) ему права доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн.

9. Порядок контроля соблюдения условий использования средств защиты информации

61. Данная глава Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее — СЗИ).

62. Технические средства защиты информации являются важным компонентом ОБ ПДн.

63. Порядок работы с техническими СЗИ определен в соответствующих инструкциях, руководстве по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

64. Право проверки соблюдения условий использования средств защиты информации имеют:

начальник отдела информационных технологий и телекоммуникаций;

ведущий специалист по технической защите информации;

администратор безопасности.

65. Пользователю ИСПДн категорически запрещается:

обработка конфиденциальной информации с отключенными СЗИ;

менять настройки СЗИ, местоположение - для генератора шума.

66. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ («Страж», «Secret Net», других), установленные сотрудником органа по аттестации в ходе настройки системы ОБ ПДн.

10. Порядок охраны и допуска посторонних лиц в защищаемые помещения

67. Порядок охраны (сдачи под охрану) защищаемых помещений ИСПДн определяется Инструкцией о порядке приема (сдачи) под охрану режимных помещений в нерабочее время и в выходные праздничные дни, утвержденной главой Кыштымского городского округа.

68. В случае комиссионного вскрытия помещения при отсутствии ответственного сотрудника за помещение, ведущий специалист по технической защите информации и администратор безопасности организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации, о чём докладывается главе Кыштымского городского округа.

69. В соответствии с требованиями данного Положения при обработке конфиденциальной информации в ИСПДн исключить пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн определенные Техническим паспортом ограждающими конструкциями и межэтажными перекрытиями кабинета.

11. Порядок уничтожения носителей персональных данных

70. В случае достижения цели обработки персональных данных, носители персональных данных уничтожаются в срок, установленный федеральным законодательством.

71. Для уничтожения носителей персональных данных в Администрации Кыштымского городского округа создается комиссия по распоряжению Администрации Кыштымского городского округа. В состав комиссии по уничтожению носителей персональных данных входят администратор безопасности ИСПДн и руководитель подразделения Администрации, в котором функционирует ИСПДн.

72. Машиночитаемые носители, содержащие информацию с персональными данными и подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы компьютера с последующим «очищением корзины».

В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

73. В ходе процедуры уничтожения носителей необходимо присутствие членов комиссии, осуществляющей уничтожение персональных данных.

Комиссия составляет и подписывает соответствующий акт об уничтожении носителей в двух экземплярах. В течение трёх дней после составления акты об уничтожении направляются на утверждение Главе Кыштымского городского округа.

Факт уничтожения носителя персональных данных фиксируется в «Журнале регистрации носителей персональных данных», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные.

12. Порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления

74. Работа с ПДн должна приостанавливаться только при обнаружении нарушений первой и/или второй категорий.

75. Пользователь, обнаруживший нарушения при работе с ПДн обязан сообщить об этом своему непосредственному руководителю.

Ведущий специалист по технической защите информации, обязан:

установить категорию выявленного нарушения;

при установлении первой или второй категории нарушения инициировать проведение служебного расследования.

76. Распоряжением Администрации Кыштымского городского округа устанавливается прекращение доступа к ресурсам ИСПДн на время проведения служебного расследования.

77. Все пользователи, работающие с ПДн обязаны:

временно (на время проведения служебного расследования) приостановить свою деятельность по работе с ИСПДн;

содействовать проведению служебного расследования.

78. Работа с ПДн может возобновляться только после устранения всех выявленных нарушений, их последствий.

13. Заключительные положения

79. Требования настоящего Положения обязательны для всех работников и муниципальных служащих, обрабатывающих конфиденциальную информацию.

80. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

81. Нарушения, связанные с выполнением требований руководящих документов по информационной безопасности, применению средств защиты информации и разграничения доступа, использованию технического, информационного и программного обеспечения ИСПДн, по степени их опасности делятся на нарушения первой, второй и третьей категории.

82. К нарушениям первой категории относятся нарушения, повлекшие за собой разглашение (утечку) защищаемых сведений, утрату содержащих их машинных носителей информации и машинных документов, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

К нарушениям второй категории относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых сведений или утрате содержащих их машинных носителей информации и машинных документов, уничтожению (искажению) информационного и программного обеспечения, выведению из строя технических средств.

Остальные нарушения относятся к нарушениям третьей категории.

И. о. начальника отдела
мобилизационной работы Н.Л. Серышев