АДМИНИСТРАЦИЯ КАРАБАШСКОГО ГОРОДСКОГО ОКРУГА
ЧЕЛЯБИНСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 11.05.2012 № 146
г.Карабаш

Об утверждении Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационых системах персональных данных в администрации Карабашского городского округа

В целях совершенствования работы по обеспечению защиты персональных данных в администрации Карабашского городского округа в соответствии с Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17.11.2007г. №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»,
ПОСТАНОВЛЯЮ:

1. Утвердить Положение по организации и проведению работ по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Карабашского городского округа (прилагается).
2. Контроль за исполнением постановления возложить на начальника управления делами администрации Карабашского городского округа Кожевникова С.М.

Глава Карабашского
городского округа В.Ф. Ягодинец

Администрация Карабашского городского округа Челябинской области
ПРОТОКОЛЬНАЯ ЧАСТЬ

Утверждено
Постановлением администрации
Карабашского городского округа
от 21 мая 2010г. № 146

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Карабашского городского округа

I. Термины и понятия

1. Персональные данные (далее ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.2. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2. Обработка персональных данных-действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

3. Информационная система персональных данных (далее - ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

4. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

5. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

II. Общие положения

6. Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Карабашского городского округа (далее именуется - Положение) разработано на основании следующих документов:

Федерального закона Российской Федерации от 27 июля 200 № 152-ФЗ «О персональных данных»;

Постановления Правительства Российской Федерации от 17 ноября 2007г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

«Основных мероприятий по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённых 15 февраля 2008 г. заместителем директора ФСТЭК России.

7. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации Карабашского городского округа области, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

8. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

9. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-математических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

10. При обработке персональных данных в информационной системе должно быть обеспечено:

согласие субъекта персональных данных, составленного по форме (согласно приложению 1 к настоящему Положению) или сформированного в информационной системе персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных»;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к персональным данным;

недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

постоянный контроль за обеспечением уровня защищённости персональных данных.

11. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

1) определение информационных систем, содержащих персональные данные;

2) классификацию информационных систем персональных данных в соответствии с совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

3) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

4) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

5) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

6) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

7) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

8) учёт применяемых средств защиты информации; эксплуатационной и технической документации к ним, носителей персональных данных;

9) учёт лиц, допущенных к работе с персональными данными в информационной системе;

10) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

11) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных нарушений;

12) описание системы защиты персональных данных.

12. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

13. Ответственным за разработку и осуществление мероприятий по созданию системы защиты персональных данных при их обработке в информационных системах администрации Карабашского городского округа является управление делами администрации Карабашского городского округа.

14. Безопасность персональных данных при их обработке в информационных системах обеспечивают подразделения, эксплуатирующие информационные системы.

15. Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных обязанностей, допускаются к соответствующим персональным данным на основании списка, утверждённого Главой администрации Карабашского городского округа.

Изменения и дополнения в список вносятся на основании распоряжения Главы Карабашского городского округа.

16. Сотрудники, допущенные к обработке персональных данных, в обязательном порядке знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме (согласно приложения 2) к настоящему Положению.

17. Реализация требований Положения по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

III. Обязанности должностных лиц по обеспечению безопасности ПДн

18. В соответствии с распоряжением Главы Карабашского городского округа «О назначении ответственных лиц за обеспечение защиты персональных данных в администрации Карабашского городского округа» от 22 апреля 2010 г. № 116, а также в соответствии с настоящим постановлением:

ответственным за разработку и осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах администрации Карабашского городского округа назначен ведущий специалист по организации защиты персональных данных управления делами администрации Карабашского городского округа;

ответственным за выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных назначено управление делами администрации Карабашского городско округа;

ответственными за безопасную эксплуатацию информационных систем персональных данных назначаются руководители эксплуатационных отделов, управлений администрации Карабашского городского округа.

19. В целях обеспечения информационной безопасности персональных данных в администрации Карабашского городского округа ведущий специалист по организации персональных данных выполняет следующие основные задачи:

- проводит анализ и выявление возможных каналов утечки информации и воздействия на информационные ресурсы и процессы при автоматизированной обработке персональных данных;
- организует и проводит классификацию информационных систем персональных данных;
- внедряет организационно-технические меры защиты информации и организует работы по защите информационных систем персональных данных в соответствии с установленным классом системы;
- осуществляет контроль выполнения требований по защите персональных данных, а также функционирования средств защиты информации при эксплуатации информационных систем персональных данных;

- разрабатывает на основе руководящих и методических документов по технической защите информации внутренние организационно-распорядительные документы, определяющие порядок и мероприятия по защите персональных данных в информационных системах администрации Карабашского городского округа.

ответственный за выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - администратор) обязан выполнять следующие функции:

знать перечень установленных в подразделениях рабочих станций и перечень задач, решаемых с их использованием;

осуществлять учёт и периодический контроль за составом и полномочиями пользователей различных рабочих станций;

осуществлять оперативный контроль за работой пользователей защищённых рабочих станций, анализировать содержимое системных журналов всех рабочих станций и журналов систем мониторинга безопасности;

осуществлять управление режимами работы и административную поддержку функционирования применяемых на рабочих станциях специальных средств защиты от не санкционированного доступа и средств антивирусного контроля;

присутствовать при внесении изменений в конфигурацию аппаратно-программных средств защищённых рабочих станций и серверов, устанавливать и осуществлять настройку средств защиты рабочих станций и серверов;

периодически проверять состояние используемых систем защиты информации от несанкционированного доступа (далее - СЗИ НСД), осуществлять проверку правильности их настройки;

периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищённых рабочих станций и системы защиты персональных данных;

проводить работы по выявлению возможных каналов вмешательства в процесс функционирования информационных систем и осуществления НСД к информации и техническим средствам персональной электронно-вычислительной машины (далее - ПЭВМ);

докладывать руководителю аппарата администрации Карабашского городского округа об имевших место попытках несанкционированного доступа к информации и техническим средствам ПЭВМ;

по указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению средствами защиты от НСД, установленных на рабочих станциях информационных систем;

участвовать в расследовании причин совершения нарушений и возникновения серьезных ситуаций в результате НСД;

резервировать общесистемное и специальное программное обеспечение, программное обеспечение средств защиты информации и их настройки, базы персональных данных;

восстанавливать общесистемное и специальное программное обеспечение, программное обеспечение средств защиты информации и их настройки, базы персональных данных при сбоях;

вести журнал учёта машинных носителей персональных данных, журнал учёта средств защиты информации и журнал учёта лиц, допущенных к работе с персональными данными в администрации Карабашского городского округа;

проводить периодические проверки наличия, сохранности и соблюдения правил обращения с машинными носителями персональных данных (далее – ПДн);

проводить первичный инструктаж и периодические занятия с сотрудниками подразделений по правилам работы на ПЭВМ, оснащённых СЗИ НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации.

IV. Обязанности сотрудника, допущенного к обработке ПДн:

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

2) хранить в тайне свой пароль (пароли). В соответствии с разделом 5 «Правила парольной защиты» настоящего Положения с установленной периодичностью менять свой пароль (пароли);

3) выполнять требования части XI «Правила антивирусной защиты» настоящего Положения в части касающейся действий пользователей рабочих станций информационной системы;

4) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закреплённой за ним рабочей станции.

5) немедленно вызывать ответственного за безопасность информации в отделе, управлении и ставить в известность руководителя отдела, управления при обнаружении следующих нарушений:

нарушений целостности пломб (наклеек, печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищённой рабочей станции;

несанкционированных (произведённых с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств рабочей станции;

нарушений в работе средств защиты информации;

отклонений в работе системных или прикладных программных программ, затрудняющих эксплуатацию рабочей станции, выхода их строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтера и т.п.), а также перебоях в системе электроснабжения;

некорректного функционирования установленных на рабочей станции технических средств защиты;

непредусмотренных формуляром рабочей станции отводов кабелей и подключенных устройств.

V. Порядок предоставления информации органам государственной власти, физическим и юридическим лицам

20.В администрации Карабашского городского округа производится автоматизированная обработка персональных данных сотрудников в информационной системе «Автоматизированная система бухгалтерии администрации Карабашского городского округа»

21. В своей деятельности управление делами администрации Карабашского городского округа руководствуется следующими положениями:

информация, относящаяся к персональным данным сотрудника, может быть предоставлена государственным органам в порядке, установленном Федеральным законом от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»;

работодатель не вправе предоставлять персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных Федеральным законом от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации»;

в случае если лицо, обратившееся с запросом, не уполномочено Федеральным законом на получение персональных данных сотрудника или отсутствует письменное согласие сотрудника на предоставление его персональных сведений, работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных;

персональные данные сотрудника могут быть переданы представителем сотрудника в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

22. Отдел бухгалтерского учёта и отчётности администрации Карабашского городского округа обрабатывает и предоставляет персональные данные по установленному регламенту в Отделение Пенсионного Фонда Российской Федерации по Челябинской области и Управление Федеральной налоговой службы Российской Федерации по Челябинской области на электронных носителях информации без передачи по открытым каналам связи.

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

22. При обнаружении нарушений порядка предоставления персональных данных в соответствии с Федеральным законом от Федеральным законом от 2 марта 2007 г. № 25-ФЗ «О муниципальной службе в Российской Федерации» и частью V «Порядок предоставления информации органам государственной власти, физическим и юридическим лицам» настоящего положения уполномоченное лицо должно немедленно приостановить предоставление персональных данных.

24. Глава Карабашского городского округа назначает служебное расследование для выявления причин нарушения.

25. После устранения нарушений предоставление персональных данных возобновляется.

VII. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации и нарушения порядка предоставления ПДн, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям

26. При обнаружении инцидента информационной безопасности необходимо информировать о нём ответственных за организацию работ и обеспечение

безопасности персональных данных, ответственных за эксплуатацию информационной системы персональных данных.

Предположение о том, что произошел инцидент информационной безопасности, основывается на следующих признаках:

уведомление антивирусного средства о нарушении информационной безопасности;

сообщение пользователей об отклонениях в работе системных или прикладных программ;

сообщение пользователей о снижении производительности их рабочей станции;

системный администратор фиксирует наличие файлов с нечитаемыми названиями;

приложение фиксирует в журнале множественные неудачные попытки авторизации и другие подозрительные действия.

27. Администратором информационной безопасности осуществляется исходное протоколирование инцидента.

28. Проводится оценка риска и последствий инцидента, вследствие чего вырабатывается стратегия реагирования на инцидент.

29. Ответственные за реагирование на инцидент должны классифицировать и описать каждый инцидент, произошедший в организации, а также классифицировать и описать возможные инциденты, предположения о которых были сделаны на основе анализа рисков.

30. В случае неблагоприятных последствий или неправильной работы средств защиты информации необходимо немедленно остановить работы в информационных системах, на которые распространяются последствия инцидента, и принять меры по их устранению.

31. В случае возникновения нарушений на рабочей станции или сервере нельзя проводить расследование, используя эту же систему. Необходимо произвести полное дублирование информации с системы и проводить работы по разбирательству нарушения на отдельном компьютере.

32. Электронные журналы должны быть тщательно изучены и проанализированы.

33. События инцидента подлежат документированию.

Документирование необходимо для сбора и последующего обобщения свидетельств расследования. Документированию подлежат все факты и доказательства злонамеренного воздействия.

Рекомендуется ведение журнала расследования инцидента, форма которого разрабатывается командой реагирования. Ключевыми позициями данного журнала являются:

текущий статус расследования;

описание инцидента;

действия, производимые командой реагирования в процессе обработки инцидента;

перечень свидетельств, собранных в ходе обработки инцидента, с обязательным указанием источников.

34. В ходе расследования инцидента все свидетельства должны быть защищены от дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях информационной системы.

35. Устанавливается виновник инцидента.

36. После обработки инцидента результаты расследования должны быть документированы. Завершение расследования необходимо сопровождать совместным обсуждением его результатов со всеми привлечёнными и заинтересованными сторонами. Команда расследования инцидентов должна сделать соответствующие выводы об уязвимостях, классифицировать их и принять меры к недопущению в дальнейшем инцидентов подобного вида.

37. Администратором информационной безопасности составляется заключение по факту инцидента информационной безопасности, включающим в себя:

исходное протоколирование инцидента;

причины и следствия возникновения инцидента;

меры, предпринятые для ликвидации инцидента и его последствий;

предложения по внесению изменений в систему обеспечения безопасности информации.

VIII. Порядок взаимодействия со сторонними организациями, имеющими соответствующие лицензии на деятельность в области технической защиты информации

38. Администрация Карабашского городского округа может взаимодействовать со сторонними организациями, имеющими соответствующие лицензии на деятельность в области технической защиты информации. Каждая из таких организаций привлекается к работам по обеспечению безопасности ПДн в интересах администрации Карабашского городского округа в рамках договоров в соответствии с перечнем услуг, предоставляемых этой организацией, указанных в лицензии (к услугам относится также продажа средств защиты информации и поисковых приборов).

При выборе организации на проведение работ в области защиты ПДн на объектах защиты предпочтение отдается организациям:

имеющим лицензии по всему комплексу работ в области защиты ПДн, которые необходимо проводить на объектах защиты;

имеющим в качестве учредителей федеральные органы и государственные предприятия;

ранее выполнявшим работы для администрации Карабашского городского округа или других объектов в Челябинской области (на территории местного самоуправления) и положительно себя зарекомендовавшим.

Со сторонней организацией могут заключаться и договоры на выполнение защиты информационных систем персональных данных «под ключ». В этом случае указанная организация проводит все работы по защите персональных данных, получая все исходные данные и согласовывая проектные, технические и программные разработки с управлением делами администрации Карабашского городского округа, утверждая их у Главы Карабашского городского округа.

39. Запрещается привлекать для проведения работ по защите персональных данных на объектах администрации Карабашского городского округа иностранные организации, а также размещать на территории указанных объектов совместные с иностранными государствами предприятия.

IX. Порядок обучения администраторов средств (систем) защиты информации, в том числе средств антивирусной защиты, и первичного инструктажа пользователей

40. Администраторы средств (систем) защиты информации, в том числе средств антивирусной защиты (далее именуется - администраторы) должны быть ознакомлены с политикой безопасности, нормативными и руководящими документами, регламентирующими вопросы обеспечения безопасности информации в администрации Карабашского городского округа.

41. Администраторы должны ознакомиться с руководствами по применению конкретных средств (систем) защиты информации, средств антивирусной защиты.

42. Обучение администраторов производится на специализированных курсах в организациях по программам, согласованным с ФСТЭК России.

43. При отсутствии практических навыков работы с конкретными средствами (системами) защиты информации и средствами антивирусной защиты администраторы должны получить необходимые навыки путём внедрения СЗИ на тестовых системах.

44. Пользователи информационных систем проходят первичный инструктаж по организации своей работы с учётом обеспечения безопасности информации после получения допуска к работе с персональными данными. Инструктаж проводят сотрудники управления делами администрации Карабашского городского округа с отметкой в журнале учёта лиц, допущенных к работе с персональными данными в информационных системах администрации Карабашского городского округа.

X.Порядок организации ведения и периодической проверки электронного журнала обращений пользователей информационной системы к ПДн

45. Система защиты информации должна обеспечивать занесение в электронный журнал операций и событий в информационной системе, в том числе всех обращений пользователей информационной системы к персональным данным.

46. Журнал должен быть доступен только лицам, ответственным за обеспечение безопасности персональных данных.

47. Журнал не должен быть скомпрометирован, контрольные суммы журнала должны сохраняться в специальном электронном журнале и проверяться системой защиты информации при включении рабочих станций.

48. При ведении журнала необходимо обеспечивать:

корректность фиксации событий и генерации записей следящей программой;

неизменность при передаче записей от генерирующей программы к программе, ведущей журнал;

корректность обработки записей программой, ведущей журнал;

неизменность при хранении логов до момента изъятия;

корректность процедуры изъятия;

неизменность при хранении после изъятия до проверки.

49. Проверка электронных журналов должна проводиться администратором информационной безопасности регулярно, не реже 1 раза в неделю.

50. В случае обнаружения в электронном журнале записей о нарушениях администратор информационной безопасности обязан:

немедленно приостановить работы на объектах, где выявлены нарушения норм и требований по защите информации, и принять меры по устранению нарушений;

организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер защиты информации.

51. Средства защиты информации, предназначенные для обеспечения защиты безопасности ПДн при их обработке в ИСПДн, подлежат учёту в журнале учёта средств защиты информации, в котором отражается:

индексы и наименования средств защиты;

серийные (заводские) номера;

номера специальных защитных знаков;

номера и сроки действия сертификатов на средство защиты;

наименование организаций, установивших средства защиты;

место установки средств защиты информации.

Журнал в установленном порядке должен быть зарегистрирован в делопроизводстве.

52. Все магнитные, оптические и другие машинные носители ПДн подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учёт. Машинные носители информации, в том числе с резервными копиями ПДн, регистрируются в журнале учета машинных носителей ПДн, в котором отражается:

тип и ёмкость носителя;

учётный номер носителя;

место установки (использования) носителя;

дата установки носителя;

ответственное должностное лицо;

сведения о списании носителя и уничтожении информации.

Журнал в установленном порядке должен быть зарегистрирован в делопроизводстве.

53. Администратором информационной безопасности должна проводиться периодическая проверка наличия, сохранности и соблюдения правил обращения с машинными носителями ПДн, журнала учёта машинных носителей ПДн, журнала учёта средств защиты информации, не реже 1 раза в неделю.

XI. Правила парольной защиты

54. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационных систем и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора информационной безопасности администрации Карабашского городского округа.

55. Пароли должны генерироваться и распределяться централизованно или выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

1) длина пароля должна быть не менее 6 - 8 символов в зависимости от клас системы;

2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы ($, @, #, %, & и другие символы);

3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и другие сочетания);

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

5) личный пароль пользователь не имеет права сообщать никому.

56. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

57. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

58. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений.

59. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца.

60. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и другие изменения) должна проводиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

61. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие изменения) администратора информационной безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИС.

62. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

63. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, или в сейфах ответственного за информационную безопасность или руководителя отдела, управления.

64. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за эксплуатацию информационной системы персональных данных, периодический контроль возлагается на администратора информационной безопасности.

XII. Правила антивирусной защиты

65. В администрации Карабашского городского округа допускаются к использованию только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

66. Установка и настройка параметров средств антивирусного контроля на компьютерах осуществляется сотрудниками управления делами в соответствии с руководствами по применению конкретных антивирусных средств.

67. Ежедневно после включения компьютера (для серверов – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютера.

68. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, текстовые файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

69. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

70. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверенно на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

71. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с ответственным за обеспечение безопасности информации должен провести внеочередной антивирусный контроль компьютера. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

72. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за обеспечение информационной безопасности, владельца заражённых файлов, смежные отделы, использующие эти файлы в работе.

совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;

произвести лечение или уничтожение зараженных файлов.

73. Ежедневно в автоматическом режиме должно проводиться обновление антивирусных баз.

74. Сотрудниками ответственными за обеспечение информационной безопасности должны проводиться периодические проверки обновлений компонентов антивирусного средства не реже одного раза в месяц.

75. Администратор информационной безопасности должен своевременно оформлять заявки на приобретение антивирусных средств и продление лицензий.

XIII. Правила обновления общесистемного и прикладного программного обеспечения ИСПДн

76. Под обновлением понимается замена программного обеспечения(далее – ПО) устаревшей версии на новую версию этого же ПО. Поскольку ПО, установленное на ПЭВМ документально фиксируется при декларировании соответствия ИСПДн требованиям по безопасности информации, обновление ПО будет допустимо лишь в той мере и в том случае, если это подтверждено производственной необходимостью и имеет непосредственное отношение к технологическому процессу.

77. В процессе обновления ПО допускается ввод информации с CD и внешних магнитных носителей.

78. Установка и обновление ПО производится только с лицензионных дистрибутивных носителей.

79. Обновления должны подвергаться антивирусному контролю в соответствии с разделом XII «Правила антивирусной защиты» настоящего Положения.

80. Операция обновления производится администратором и фиксируется в журнале.

81. Установка нового автоматизированного рабочего места для пользователя информационной системы производится после выполнения требований к системе защиты персональных данных и настоящего Положения. По окончании работ производится оценка соответствия ИСПДн требованиям безопасности персональных данных и вносятся необходимые изменения и дополнения в техническую документацию.

82. Для обработки информации рекомендуется использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2542-96).

XIV. Порядок контроля за соблюдением условий использования средств защиты информации

83. Целями контроля за соблюдением условий использования средств защиты информации являются:

установление степени соответствия принятых мер требованиям законодательных и иных нормативных правовых актов, стандартов, норм, правил и инструкций по защите информации;

выявление технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на информацию, содержащую сведения о персональных данных;

выработка рекомендаций по закрытию этих каналов.

84. Контроль состояния информационной безопасности осуществляется сотрудниками управления делами администрации Карабашского городского округа.

85. Контроль за соблюдением условий использования средств защиты информации (далее - Контроль) осуществляется посредством проведения проверок (изучений, ознакомлений).

86. Перед проверкой проводится этап планирования проверки, включающий в себя выбор средств и методов проверки подсистем:

управления доступом;

регистрации и учета;

обеспечения целостности;

антивирусной защиты.

Проверка подсистем должна осуществляться в соответствии с Требованиями по обеспечению безопасности персональных данных при их обработке в конкретной информационной системе персональных данных.

При проверке могут быть использованы такие программные средства как:

программа анализа защищенности TCP/IP сетей «Ревизор сети»;

средство создания модели системы разграничения доступа «Ревизор 1 XP»;

программа контроля полномочий доступа к информационным ресурсам «Ревизор 2 XP»;

программа фиксации и контроля исходного состояния программного комплекса «Фикс».

87. Еженедельно администратором информационной безопасности должен проводиться анализ системных журналов всех рабочих станций и журналов систем мониторинга безопасности.

88. При Контроле необходимо проверять срок действия сертификатов используемых средств защиты информации.

89. Контроль должен проводиться регулярно, не реже 1 раза в месяц. Результаты Контроля докладываются руководителю управления делами и отдела, эксплуатирующего информационную систему.

90. Руководитель проверяемого объекта при обнаружении нарушений обязан:

немедленно приостановить работы на объектах, где выявлены нарушения норм и требований по защите информации, и принять меры по устранению нарушений;

организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер органом контроля, выявившим нарушение.

91. Ежегодная комплексная проверка состояния безопасности персональных данных при их обработке в информационных системах администрации Карабашского городского округа проводится комиссией в составе сотрудников управления делами с применением средств анализа защищённости ИСПДн. По окончанию проверки составляется справка, в которой отражаются результаты проверки, выводы и рекомендации по совершенствованию системы технической защиты информации. Содержание справки доводится до главы Карабашского

городского округа и начальника отдела, управления эксплуатирующе информационную систему.

Начальник управления делами
администрации Карабашского
городского округа Кожевников С.М.

Приложение 1
к Положению по организации
и проведению работ по обеспечению
безопасности персональных данных при их
обработке в информационных системах
персональных данных в администрации
Карабашского городского округа

СОГЛАСИЕ СУБЪЕКТА
на обработку персональных данных

№ _____ «___» _____ 2009г.

Я, _____,
(Фамилия, имя, отчество субъекта)

основной документ, удостоверяющий личность _____

_____
(номер, сведения о дате выдачи указанного документа и выдавшем его органе)

в дальнейшем «Субъект», даю согласие _____

_____,
(Наименование оператора персональных данных)

расположенным по адресу:_____

далее «Оператор», на обработку персональных данных на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий:

_____
(сбор, систематизацию, накопление, хранение, уточнение, использование, распространение)

_____
(обезличивание, блокирование, уничтожение персональных данных)

2. Оператор обязуется использовать данные Субъекта в целях _____

_____

_____

_____.

3. Типовой перечень персональных данных передаваемых Оператору на обработку:

_____
(дата рождения; место рождения; биографические сведения; сведения о местах обучения, сведения о местах работы; сведения о родителях; сведения о

_____
месте регистрации, проживания; контактная информация; паспортные данные)

_____

_____

_____

_____

4. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п.4 ст. 14 ФЗ №152 от 27.06.2006г.).

5. При поступлении Оператору письменного заявления Субъекта о прекращении действия Согласия, персональные данные уничтожаются установленным способом в:_____.
(указать срок уничтожения персональных данных)

6. Настоящее разрешение действует в течение: _____.
(указать срок хранения персональных данных субъекта)

Субъект _____ \ _____
(подпись) (Ф.И.О.)

Приложение 2
к Положению по организации
и проведению работ по обеспечению
безопасности персональных данных
при их обработке в информационных
системах персональных данных
в администрации Карабашского
городского округа

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____,

исполняющий (ая) должностные обязанности по замещаемой должности, в период служебных отношений с администрацией Карабашского городского округа и в течение двух лет после их окончания обязуюсь:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____ _____

Должность Подпись Ф.И.О.