Приложение № 2 к приказу
от «31» декабря 2015 г. № 63-0/09

Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Управлении социальной защиты населения администрации города Троицка

I. Общие положения

1. Положение об организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Управлении социальной защиты населения администрации города Троицка определяет основные мероприятия и порядок проведения работ по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) Управления социальной защиты населения администрации города Троицка (далее - Управление).

2. Обработка ПДн в Управлении осуществляется в информационных системах (далее – ИС) указанных в Перечне информационных систем персональных данных Управления (Приложением № 11 настоящего приказа).

3. Все работники Управления, участвующие в обработке ПДн в ИС, должны быть ознакомлены с настоящим Положением.

II. Порядок организации работ по обеспечению безопасности персональных данных

4. С целью организации работ по защите ПДн назначается должностное лицо, ответственное за обеспечение безопасности ПДн. Ответственным за выполнение работ по обеспечению безопасности ПДн при их обработке в ИС является администратор информационной безопасности (далее - администратор ИБ).

5. В обязанности администратора ИБ ПДн входит:

1) контроль и организация работ по обеспечению безопасности ПДн;

2) утверждение организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;

3) утверждение перечня структурных подразделений, работникам которых необходим доступ к ПДн для выполнения служебных обязанностей;

4) утверждение списка лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и системы защиты ПДн (далее - СЗПДн);

5) утверждение базовой конфигурации ИС и СЗПДн;

6) проведение разбирательств по фактам возникновения событий,

которые могут привести к снижению уровня защищенности ПДн.

6. Реализация требований по обеспечению безопасности ПДн осуществляется администраторами, разработчиками и пользователями информационных систем.

III. Требования по обеспечению безопасности персональных данных

7. Требования по обеспечению безопасности ПДн при их обработке в ИС формируются на основании установленного уровня защищенности ИСПДн и перечня актуальных угроз безопасности ПДн.

8. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются комплексом организационно-технических мер, средств и механизмов защиты информации, определенных в Техническом задании на создание СЗПДн.

9. Применение средства защиты информации разрешается после проверки корректности его функционирования и оформления заключения о готовности средства защиты информации к эксплуатации. Применяемые средства защиты информации, эксплуатационная и техническая документация к ним подлежат обязательному учету.

10. Требования по обеспечению безопасности ПДн при их обработке в ИСПДн реализуются в рамках следующих направлений:

1) организация системы допуска и учета лиц, допущенных к работе с ПДн;

2) организация системы защиты межсетевого взаимодействия;

3) организация режима безопасности помещений ИСПДн;

4) организация безопасного хранения и уничтожения носителей ПДн;

5) организация защиты от вредоносного кода;

6) организация парольной защиты;

7) организация учета инцидентов информационной безопасности и реагирования на них;

8) организация управления конфигурацией ИСПДн и СЗПДн;

9) организация системы криптографической защиты информации;

10) организация системы резервного копирования и восстановления;

11) организация управления СЗПДн;

12) организация контроля эффективности мер защиты ПДн;

13) организация системы обучения по вопросам обеспечения безопасности ПДн.

IV. Система допуска и учета лиц

12. Ответственным за организацию системы допуска к ПДн является администратор ИБ.

13. Сотрудники Управления допускаются к обработке ПДн в ИСПДн, использование которых необходимо для выполнения их функциональных обязанностей.

14. Обработка ПДн, не включенных в Перечень ПДн, не допускается.

15. Перечень ПДн определяется и пересматривается в установленном порядке не реже, чем один раз в три года.

16. Доступ сотрудников к ПДн, обрабатываемым в ИСПДн, определяется Перечнем должностных лиц, имеющих доступ к ПДн (Приложение №13 настоящего приказа).

17. Права доступа пользователей ИСПДн определяются в соответствии с Матрицами доступа, разрабатываемыми администратором ИБ для каждой ИСПДн.

18. Управление учетными записями пользователей и распределение прав доступа к информационным ресурсам ИСПДн, внешним носителям информации и периферийным устройствам осуществляется администратором ИСПДн, назначаемым приказом, по согласованию с администратором ИБ.

19. Общий порядок предоставления доступа, изменения и отмены доступа к информационным ресурсам ИСПДн устанавливается организационно-распорядительными документами Управления.

20. Администратор ИБ осуществляет оценку необходимости запрашиваемого уровня доступа к ПДн.

21. Администратор ИБ осуществляет учет лиц, допущенных к работе с ПДн в ИСПДн.

22. Администратор ИБ осуществляет контроль за своевременным блокированием доступа (изменением прав доступа) при увольнении пользователя ИСПДн (изменении должностных обязанностей).

23. В пределах контролируемой зоны запрещено подключение к информационной сети мобильных технических средств, портативных рабочих станций и внешних носителей информации.

24. Подключение к информационной сети указанных устройств допускается только при наличии согласования с администратором ИБ.

V. Система защиты межсетевого взаимодействия

25. Обеспечение защиты межсетевого взаимодействия реализуется по следующим направлениям:

1) выделение сетевых сегментов обработки ПДн в информационной сети;

2) межсетевое экранирование выделенных сегментов обработки ПДн;

3) разграничение доступа пользователей к ресурсам сетей связи общего пользования.

26. В информационной сети должны быть выделены:

1) сегменты серверов ИСПДн;

2) сегменты пользователей ИСПДн;

3) сегмент локальной вычислительной сети (далее - ЛВС);

4) сегмент СЗПДн.

27. Включение новых серверов и рабочих станций в сегменты ИСПДн

должно осуществляться только после выполнения требований по защите ПДн.

28. Доступ к сегментам ИСПДн из других сегментов информационной сети должен ограничиваться межсетевыми экранами.

29. Межсетевое экранирование сегментов ИСПДн должно обеспечивать:

1) фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

2) регистрацию входа (выхода), либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратного отключения межсетевого экрана);

3) восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

4) защиту беспроводных соединений, применяемых в ИСПДн.

30. Межсетевое экранирование должно обеспечивать отделение ЛВС и сети среды виртуализации от сетей связи общего пользования.

31. Серверы, доступные из сетей связи общего пользования, должны быть размещены в выделенном сегменте демилитаризованной зоны. Доступ к таким серверам из сетей связи общего пользования разрешается только по необходимым сетевым портам.

32. Используемые межсетевые экраны должны быть сертифицированы в соответствии с требованиями к средствам межсетевого экранирования, установленными Приказом ФСТЭК России №21 от 18.02.2013.

33. Управление сетевым оборудованием осуществляется системными администраторами.

34. Внесение изменений в правила межсетевого экранирования осуществляется системными администраторами по согласованию с администратором ИБ.

35. Доступ к сетевому оборудованию разрешен только с рабочих станций системных администраторов либо локально.

36. В случае производственной необходимости пользователям ИСПДн может предоставляться доступ:

1) к сети Интернет;

2) к сервисам внешней электронной почты.

37. Правила работы пользователей ИСПДн с ресурсами сети Интернет и электронной почты устанавливаются организационно-распорядительными документами Управления.

VI. Режим безопасности помещений информационных систем персональных данных

38. Обеспечение безопасности помещений ИСПДн направлено на исключение возможности несанкционированного доступа к техническим средствам ИСПДн, их хищения и нарушения работоспособности, хищения

носителей информации.

39. Приказом определяются границы контролируемой зоны, на территории которой исключено бесконтрольное пребывание посторонних лиц.

40. Режим безопасности помещений ИСПДн реализуется в соответствии с Положением об организации режима безопасности помещений ИСПДн.

41. Реализация режима безопасности помещений ИСПДн возлагается на сотрудников, работающих в данных помещениях.

VII. Безопасность носителей персональных данных

42. Безопасность информации, хранящейся на бумажных и отчуждаемых электронных носителях ПДн, обеспечивается путем организации системы учета и безопасного хранения носителей ПДн.

43. Ответственным за учет и соблюдение условий хранения электронных носителей ПДн является администратор ИБ.

44. Порядок учета, хранения и уничтожения носителей ПДн регламентируется Положением об учете, порядке хранения и уничтожения носителей ПДн.

45. При уничтожении носителя ПДн должны обеспечиваться и контролироваться гарантированное уничтожение (стирание) ПДн.

VIII. Защита от вредоносного кода

46. Средства защиты от вредоносного кода должны быть установлены на всех рабочих станциях и серверах.

47. Средства защиты от вредоносного кода должны обеспечивать:

1) автоматическое блокирование или удаление обнаруженного вредоносного программного обеспечения;

2) регулярную проверку программных модулей рабочих станций и серверов ИСПДн на предмет наличия в них вредоносного программного обеспечения по типовым шаблонам и с помощью эвристического анализа;

3) возможность отката операций удаления вредоносного программного обеспечения путем помещения файлов, содержащих вредоносное программного обеспечение, в карантин;

4) своевременное обновление антивирусных баз (сигнатур угроз) и программных модулей.

48. При выявлении фактов заражения вредоносным программным обеспечением ответственным за обеспечение безопасности ПДн проводится разбирательство с целью установления причин возникновения заражения.

49. Обязанности по устранению последствий заражения вредоносным программным обеспечением возлагаются на администратора ИБ.

IX. Парольная защита

50. Парольная защита применяется для исключения возможности получения несанкционированного доступа к элементам ИСПДн (рабочим станциям, серверам, активному сетевому оборудованию) в целях не допущения утечки, а также несанкционированной модификации или уничтожения ПДн.

51. Парольная защита применяется:

1) при доступе пользователей к операционным системам рабочих станций и серверов, прикладному программному обеспечению ИСПДн, средствам защиты информации;

2) при доступе системных администраторов к средствам управления сетевым и серверным оборудованием, операционным системам серверов и рабочих станций, специальному программному обеспечению ИСПДн, средствам защиты информации.

52. Требования парольной защиты определяются организационно-распорядительными документами.

53. При выявлении фактов нарушения требований парольной защиты ответственным за обеспечение безопасности ПДн проводится разбирательство.

X. Управление инцидентами информационной безопасности и реагирование на них

54. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности ПДн (далее - инцидентов), должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

55. Средства (системы) анализа защищенности должны обеспечивать, в том числе:

1) выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИСПДн;

2) контроль установки обновлений программного обеспечения рабочих станций и серверов ИСПДн.

56. Должен быть обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн.

57. Анализ инцидентов осуществляется:

1) администратором ИБ при просмотре журналов событий, формируемых средствами защиты информации;

2) администратором ИСПДн при просмотре журналов событий,

формируемых программным обеспечением ИСПДн и системами управления базами данных;

3) системными администраторами при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

58. Журналы аудита должны просматриваться ответственными работниками регулярно (не реже одного раза в неделю).

59. О фактах обнаружения инцидентов ответственные работники должны немедленно сообщать администратору ИБ.

60. Права доступа на модификацию и удаление журналов событий безопасности должны быть ограничены для всех пользователей ИСПДн.

XI. Система криптографической защиты информации

61. Система криптографической защиты информации (далее - СКЗИ) предназначена для криптографической защиты информации, передаваемой по каналам связи, расположенным вне контролируемой зоны Организации.

62. Криптографическая защита должна реализовываться алгоритмами, определяемыми ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 с применением программно-технических средств шифрования и/или специального программного обеспечения, сертифицированных в установленном порядке ФСБ России.

63. Эксплуатация СКЗИ должна осуществляться в соответствии с эксплуатационной и технической документации к ним.

64. Допуск сотрудников к работе с СКЗИ должен осуществляться в соответствии со списком лиц, допущенных к СКЗИ, утвержденным ответственным за обеспечение безопасности ПДн.

65. Допуск сотрудников к работе с СКЗИ должен осуществляться после проведения администратором ИБ обучения и ознакомления с требования по работе с СКЗИ.

66. Администратор ИБ должен вести учет используемых СКЗИ, технической и эксплуатационной документации к ним в Журнале учета СКЗИ.

67. Контроль выполнения требований по эксплуатации СКЗИ осуществляет администратор ИБ. При выявлении фактов нарушения требований по эксплуатации СКЗИ ответственным за обеспечение безопасности ПДн проводится разбирательство.

XII. Организация системы резервного копирования и восстановления

61. Для обеспечения возможности восстановления функционирования и работоспособности ИСПДн и средств защиты информации при возникновении аварийных ситуаций должна быть реализована система резервного копирования и восстановления.

62. Резервному копированию подлежит информация следующих

основных категорий:

1) ПДн, хранящиеся в виде отдельных файлов, каталогов или баз данных ИСПДн;

2) системные и конфигурационные файлы операционных систем и специального программного обеспечения серверов;

3) конфигурационные файлы сетевого оборудования;

4) системные и конфигурационные файлы средств защиты информации.

63. Ответственными за осуществление резервного копирования являются системные администраторы соответствующих информационных ресурсов.

64. Требования к периодичности и способам осуществления резервного копирования информационного ресурса определяются особенностями функционирования соответствующего информационного ресурса.

65. Администратор ИБ должен осуществлять регулярные проверки выполнения требований резервного копирования информационных ресурсов.

XIII. Управление конфигурацией информационных систем персональных данных и системы защиты персональных данных

66. Администратором ИБ и администратором ИСПДн должно обеспечиваться управление конфигурацией ИСПДн и СЗПДн.

67. В Управлении допускается использование ограниченного набора программного обеспечения (далее - ПО), формирующего базовую конфигурацию ИСПДн.

68. Состав базовой конфигурации ПО на рабочих станциях и серверах ИСПДн утверждается приказом. Установка на рабочих станциях и серверах ИСПДн ПО, не входящего в состав разрешенного ПО, не допускается.

69. Состав базовой конфигурации ПО СЗПДн устанавливается эксплуатационной документацией на СЗПДн.

70. При первоначальной настройке рабочих станций и серверов системными администраторами производится установка ПО на основании перечня разрешенного ПО.

71. Пересмотр базовой конфигурации осуществляется администратором ИБ при возникновении необходимости по согласованию с ответственным за обеспечение безопасности ПДн. Пересмотренная базовая конфигурация доводится до сведения всех сотрудников путем рассылки по электронной почте с обязательным запросом уведомления о прочтении письма.

72. Внесение изменений в конфигурацию ИСПДн осуществляется на основании заявки заинтересованного лица, согласованной с руководителем структурного подразделения.

73. При согласовании внесения изменений в конфигурацию ИСПДн администратору ИБ необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации и на работоспособность ИСПДн.

74. ПО, используемое в ИСПДн, должно регулярно обновляться. Получение обновлений должно осуществляться из официальных источников производителя ПО. Получение обновлений ПО сертифицированных средств защиты информации должно осуществляться из специализированных источников обновления производителей средств в соответствии с эксплуатационной документацией к ним.

75. Используемое ПО приобретается в соответствии с лицензионной политикой разработчика.

76. Установка обновлений ПО не считается внесением изменений в конфигурацию ИСПДн и СЗПДн и не требует заполнения заявки на внесение изменений.

XIV. Управление системой защиты информации информационной системы

77. СЗПДн должна обеспечивать управление:

1) заведением и удалением учетных записей пользователей, полномочиями пользователей и поддержанием правил разграничения доступа в ИСПДн;
2) резервным копированием и восстановлением работоспособности ИСПДн и СЗПД;
3) обновлением программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации;
4) регистрацией и анализом инцидентов ИБ.

78. Администрирование СЗПДн осуществляет администратор ИБ.

XV. Контроль принятых мер по обеспечению безопасности персональных данных

79. Ответственным за контроль выполнения принятых мер по обеспечению безопасности ПДн является ответственный за обеспечение безопасности ПДн.

80. Администратор ИБ осуществляет постоянный контроль выполнения требований по обеспечению безопасности ПДн в рамках выполнения своих обязанностей.

81. Мероприятия по контролю мер выполнения требований по обеспечению безопасности ПДн проводятся в соответствии с Планом внутренних проверок, утвержденным приказом.

82. Контроль эффективности мер защиты информации должен осуществляться в соответствии с Положением по организации контроля эффективности защиты информации.

XVI. Обучение по вопросам обеспечения безопасности

83. Администратор ИБ должен регулярно проходить обучение на

курсах повышения квалификации по вопросам защиты информации (не реже одного раза в три года).

84. Ознакомление сотрудников с правилами работы с ПДн осуществляется:

1) путем проведения руководителем структурного подразделения, в которое принят сотрудник, первичных инструктажей с вновь принятым сотрудником по соблюдению установленных правил работы с ПДн;

2) путем проведения обучения сотрудников (пользователей средств вычислительной техники) администратором ИБ правилам работы с используемыми средствами защиты информации и СКЗИ;

3) путем самостоятельного изучения сотрудником организационно-распорядительных документов, регламентирующих вопросы обеспечения безопасности ПДн.

85. Допуск сотрудников к ресурсам ИСПДн осуществляется только после прохождения первичного инструктажа и ознакомления с организационно-распорядительными документами по вопросам обеспечения безопасности ПДн.

86. При проведении первичного инструктажа нового пользователя ИСПДн должны быть разъяснены:

1) права и обязанности пользователя ИСПДн;

2) действия, которые запрещены при обработке ПДн;

3) возможные последствия и ответственность в случае нарушения правил работы с ПДн.

Заместитель начальника Управления,
начальник организационно-правового отдела _____ С. О. Григорян