Приложение
к приказу управления социальной защиты населения администрации Копейского городского округа Челябинской области от 15.06.2015 № 112

Политика
в области обеспечения безопасности персональных данных в управлении социальной защиты населения администрации Копейского городского округа Челябинской области

I. Общие положения

1. Политика в области обеспечения безопасности персональных данных в управлении социальной защиты населения администрации Копейского городского округа Челябинской области (далее - Политика, управление) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в управлении персональных данных, функции управления при обработке персональных данных, права субъектов персональных данных, а также реализуемые требования к защите персональных данных в управлении.

2. Политика разработана в соответствии со следующими нормативными правовыми актами в области обработки и обеспечения безопасности персональных данных:

1) Конституция Российской Федерации;

2) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3) Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

4) Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

5) Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

6) Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

7) иные нормативные правовые акты в области обработки и

обеспечения безопасности персональных данных, а также руководящие документы Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации.

3. В целях реализации положений Политики в управлении разрабатываются соответствующие локальные нормативные акты и иные документы, в том числе:

1) положение об обработке персональных данных в управлении;

2) перечень работников управления, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных (далее - ИСПДн), необходим для выполнения служебных (трудовых) обязанностей;

3) иные локальные нормативные акты и документы, регламентирующие вопросы обработки персональных данных.

4. В настоящей Политике используются следующие основные понятия:

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление ПДн - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение ПДн - действия, направленные на раскрытие

персональных данных неопределенному кругу лиц;

средства криптографической защиты информации - совокупность программных и технических средств, реализующих криптографические преобразования с исходной информацией и функцию выработки и проверки электронной цифровой подписи;

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители ПДн.

II. Принципы и цели обработки персональных данных

5. Управление, являясь оператором ПДн, осуществляет обработку ПДн работников управления и других субъектов ПДн.

Обработка ПДн в управлении осуществляется с учетом необходимости обеспечения защиты прав и свобод работников управления и других субъектов ПДн, в том числе защиты права не неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

1) обработка ПДн осуществляется на законной и справедливой основе;

2) обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей;

3) не допускается обработка ПДн, несовместимая с целями сбора ПДн;

4) не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

5) обработке подлежат только ПДн, которые отвечают целям их обработки;

6) содержание и объем обрабатываемых ПДн соответствует заявленным целям соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых ПДн по отношению к заявленным целям их обработки;

7) при обработке ПДн обеспечиваются точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Управлением принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных ПДн;

8) хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем того требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

9) обрабатываемые ПДн уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6. ПДн обрабатываются управлением в целях:

1) обеспечения соблюдения Конституции Российской Федерации законодательных и иных нормативных правовых актов Российской Федерации локальных и нормативных актов управления;

2) осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на управление, в том числе по предоставлению ПДн в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

3) регулирования трудовых отношений с работниками управления (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);

4) предоставления работникам управления и членам их семей дополнительных гарантий и компенсаций, в том числе негосударственного пенсионного обеспечения, добровольного медицинского страхования, медицинского обслуживания и других видов социального обеспечения;

5) защиты жизни, здоровья или иных жизненно важных интересов субъектов ПДн;

6) подготовки, заключения, исполнения и прекращения договоров с контрагентами;

7) обеспечения пропускного и внутриобъектового режимов на объектах управления;

8) формирования справочных материалов для внутреннего информационного обеспечения деятельности управления;

9) предоставления муниципальных услуг;

10) в иных законных целях.

III. Перечень субъектов ПДн

6. В управлении обрабатываются ПДн следующих категорий субъектов:

1) сотрудники управления;

2) сотрудники учреждений подведомственных управлению;

3) другие субъекты ПДн.

IV. Права субъектов ПДн

8. Субъекты ПДн имеют право на:

1) полную информацию об их ПДн, обрабатываемых в управлении;

2) доступ к своим ПДн, включая право на получение копии любой записи, содержащей их ПДн, за исключением случаев, предусмотренных федеральным законом, а также доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

3) уточнение своих ПДн, их блокирование или уничтожение в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели

обработки;

4) отзыв согласия на обработку ПДн;

5) принятие предусмотренных законом мер по защите своих прав;

6) обжалование действия или бездействия управления, осуществляемого с нарушением требований законодательства Российской Федерации в области обеспечения безопасности ПДн, в уполномоченный орган по защите прав субъектов ПДн или в суд;

7) осуществление иных прав, предусмотренных законодательством Российской Федерации.

V. Перечень ПДн, обрабатываемых в управлении и подлежащих защите

9. Перечень ПДн, обрабатываемых в управлении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами управления с учетом целей обработки ПДн, указанных в пункте 2 раздела I Политики.

10. Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в управлении не осуществляется.

11. В ИСПДн защите подлежит любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн), в том числе:

1) фамилия, имя, отчество;

2) год рождения;

3) месяц рождения;

4) дата рождения;

5) адрес;

6) образование;

7) профессия;

8) доходы;

9) фотография;

10) контактный номер;

11) сведения о документе, удостоверяющем личность;

12) реквизиты ИНН, СНИЛС, пенсионного удостоверения, расчетных счетов.

Фамилия, имя и отчество не являются информацией, позволяющей определить субъекта ПДн.

VI. Функции управления при осуществлении обработки ПДн

12. Управление при осуществлении обработки ПДн:

1) принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов управления в области обеспечения безопасности ПДн;

2) принимает правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

3) издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты ПДн в управлении;

4) публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

5) прекращает обработку и уничтожает ПДн в случаях, предусмотренных законодательством Российской Федерации в области ПДн;

6) совершает иные действия, предусмотренные законодательством Российской Федерации в области ПДн.

VII. Лица, ответственные за обеспечение безопасности ПДн

13. В управлении производится назначение следующих ответственных лиц:

1) ответственный за организацию работ по обеспечению безопасности ПДн, на которого приказом начальника управления возлагается:

- утверждение списка лиц, доступ которых к ПДн необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;
- принятие решения о распространении (передаче) ПДн;
- проведение разбирательств по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- приостановка предоставления ПДн пользователям информационной системы при обнаружении нарушений порядка предоставления ПДн;
- руководство работами по обеспечению безопасности ПДн при их обработке в ИСПДн;

2) ответственный пользователь криптосредств;

3) ответственный за выполнение работ по обеспечению безопасности ПДн, на которого приказом начальника управлениявозлагается:

- организация парольной защиты;
- организация учета средств защиты информации, эксплуатационной и технической документации к ним;

- администрирование средств и систем защиты ПДн в ИСПДн, включая средства антивирусной защиты (за исключением средств криптографической защиты информации);

- учет лиц, допущенных к работе с ПДн в ИСПДн;

- учет носителей ПДн, используемых в ИСПДн (как с использованием средств автоматизации, так и без их использования);

- периодическая (не реже одного раза в квартал) проверка электронного журнала обращений пользователей информационных систем к ПДн;

- инструктаж пользователей ИСПДн о порядке и правилах использования средств защиты информации, включая средства антивирусной защиты;

- контроль за соблюдением условий использования средств защиты информации (за исключением средств криптографической защиты информации).

VIII. Учет лиц, допущенных к работе с ПДн в ИСПДн

14. Лица, допущенные к работе с ПДн в ИСПДн управления, утверждаются приказом начальника управления.

15. Основанием для допуска сотрудника к ПДн, обрабатываемым в ИСПДн, является необходимость обработки ПДн в связи с выполнением должностных обязанностей, а также соответствующий приказ, утвержденный начальником управления.

16. Основанием для прекращения допуска сотрудника к ПДн, обрабатываемым в ИСПДн, может служить приказ об его увольнении (переводе на другую должность, не требующую работы с ПДн).

IX. Условия обработки ПДн в управлении

17. Обработка ПДн в управлении осуществляется с согласия субъекта ПДн на обработку его ПДн, если иное не предусмотрено законодательством Российской Федерации в области ПДн.

18. Управление без согласия субъекта ПДн не раскрывает третьим лицам и не распространяет ПДн, если иное не предусмотрено федеральным законом.

19. Управление вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели обработки, обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также требования к защите обрабатываемых ПДн в соответствии со статьей 19 Федерального закона «О персональных данных».

20. В целях внутреннего информационного обеспечения управление может создавать внутренние справочные материалы, в которые с письменного согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский

номер, электронной почты, иные ПДн, сообщаемые субъектом ПДн.

21. Доступ к ПДн, обрабатываемым управлением, разрешается только работникам управления, выполняющих служебные обязанности.

X. Перечень действий с ПДн и способы их обработки

22. Управлнение осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение ПДн.

23. Обработка ПДн управлением осуществляется следующими способами:

1) неавтоматизированная обработка ПДн;

2) автоматизированная обработка ПДн с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой.

XI. Порядок предоставления ПДн

24. Распространение ПДн - действия, направленные на передачу ПДн определенному кругу лиц.

25. ПДн могут быть распространены только на основании решения субъекта ПДн.

26. До передачи любых ПДн за пределы управления от каждого субъекта ПДн должно быть получено письменное согласие на распространение его ПДн, оформленное в соответствии с требованиями статьи 9 Федерального закона Российской Федерации № 152-ФЗ от 27 июля 2006 г. «О персональных данных», в каждом конкретном случае.

27. В случае смерти субъекта ПДн согласие на обработку его ПДн дают в письменной форме наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

28. Решение на предоставление ПДн принимается ответственным за организацию обработки ПДн.

29. ПДн, обрабатываемые в ИСПДн, могут быть предоставлены органам власти и органам местного самоуправления без согласия субъекта ПДн, если данные действия осуществляются в соответствии с федеральными законами Российской Федерации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. При этом решение на распространение ПДн должно содержать ссылку на соответствующую статью федерального закона Российской Федерации.

30. Трансграничная передача ПДн в управлении не осуществляется.

XII. Порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления и порядок разбирательств по фактам, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям

31. При обнаружении нарушений порядка предоставления ПДн предоставление ПДн пользователям информационной системы незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

32. Принятие решения на приостановку обработки ПДн принимается ответственным за организацию обработки ПДн.

33. Основаниями для приостановки обработки ПДн в ИСПДн и проведения разбирательства являются:

1) выявление недостоверных ПДн в ИСПДн;
2) предоставление ПДн в нарушение установленных правил;
3) допуск к ИСПДн лица, не имеющего на то разрешения;
4) утрата носителя ПДн;
5) нарушение правил хранения носителей ПДн;
6) нарушение правил эксплуатации средств защиты информации;
7) нарушение правил парольной защиты;
8) нарушение правил антивирусной защиты;
9) нарушение правил резервирования и восстановления общего и специального программного обеспечения, а также баз ПДн;
10) выявление в ИСПДн вредоносных программ (вирусов);
11) выявление в электронных журналах средств защиты информации несанкционированных действий пользователей, нарушающих безопасность ПДн или целостность (неизменность) программного обеспечения ИСПДн;
12) выявление несанкционированного внесения изменений в состав технических средств и (или) программного обеспечения ИСПДн.

34. Разбирательство проводится структурным подразделением или должностным лицом (работником), ответственным за обеспечение безопасности ПДн с обязательным привлечением руководителя структурного подразделения, осуществляющего эксплуатацию ИСПДн.

35. В ходе разбирательства составляется заключение, в котором отражается:

1) состав группы, проводившей разбирательство;
2) период времени, в который проводилось разбирательство;
3) основание для проведения разбирательства;
4) факты, выявленные в ходе разбирательства и имеющие значение в определении наличия нарушений конфиденциальности ПДн или нарушений правил использования средств защиты информации, а также иные факты, которые могут привести к нарушению конфиденциальности ПДн или к снижению уровня защищенности ПДн;
5) вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;

6) рекомендации по совершенствованию обеспечения безопасности исключающие в дальнейшем подобные нарушения.

36. Заключение представляется ответственному за организац обработки ПДн, который принимает решение на возобновление обработки Щ и принятие дополнительных мер защиты.

XIII. Организация резервирования и восстановления программного обеспечения, баз ПДн, ИСПДн

37. В ИСПДн резервированию подлежат:

1) базы ПДн;
2) специальное программное обеспечение;
3) средства защиты информации;
4) общее программное обеспечение;
5) средства вычислительной техники;
6) средства обеспечения функционирования информационных систем.

38. Резервные носители ПДн хранятся в подразделении, эксплуатирующем ИСПДн.

39. Резервные носители ПДн не могут быть переданы за пределы подразделения, эксплуатирующего ИСПДн.

40. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

41. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения машинных носителей дистрибутивов данных программ и машинных носителей обновлений к ним в подразделениях, отвечающих за их установку, настройку и сопровождение.

42. Машинные носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления). ;

43. В случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения осуществляется обязательное восстановление работоспособности ИСПДн.

XIV. Организация парольной защиты в ИСПДн

44. Защите паролем подлежит доступ к:

1) базовым системам ввода-вывода компьютеров;
2) настройкам сетевого оборудования;
3) настройкам операционных систем;
4) настройкам средств защиты информации (в том числе средств антивирусной защиты);

.

и

5) запуску специализированного программного обеспечения, предназначенного для обработки ПДн;

6) ресурсам АРМ и баз данных ИСПДн.

45. Базовые системы ввода-вывода, сетевое оборудование, операционные системы, средства защиты информации и файловые массивы (далее - объекты парольной защиты) должны быть настроены таким образом, чтобы:

1) исключить возможность просмотра ранее вводимых паролей;

2) блокировать доступ пользователей после пятикратной ошибки при вводе пароля и сигнализировать о наступлении данного события.

46. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на сотрудников отдела программно-технического обеспечения управления, и администраторов баз данных в территориальных отделах в соответствии с возложенными обязанностями.

47. Пользователь обязан запомнить личные пароли, никому их не передавать и не записывать их на местах, где их могут увидеть другие лица.

48. Информация о паролях пользователей является информацией ограниченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системы доступа.

49. Запрещается:

1) умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;

2) передача личного пароля сослуживцам или посторонним лицам;

3) запись личного пароля на бумагу и хранение его в потенциально доступном для ознакомления посторонними лицами и другими сотрудниками
месте

4) вход в систему с использованием чужих идентификаторов или паролей;

5) оставление без присмотра рабочего места при работе в ИСПДн.

50. 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.

51. Контроль за действиями пользователей системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора.

XV. Антивирусная защита в ИСПДн

52. К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антивирусные средства. Установка и настройка средств антивирусного контрой компьютерах осуществляется в соответствии с руководствами по примем, конкретных антивирусных средств.

53. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) ъ съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

54. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в 3 месяца.

55. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения, должна быть выполнена антивирусная проверка на всех компьютерах ИСПДн.

56. 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 должен провести внеочередной антивирусный контроль своего компьютера.

57. Ответственность за организацию антивирусного контроля возлагается на сотрудников отдела программно-технического обеспечения управления.

59. Ответственность за проведение мероприятий антивирусного контроля и выполнение требований по антивирусной защите возлагается на сотрудников отдела программно-технического обеспечения управления и всех сотрудников, являющихся пользователями ИСПДн.,

60. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований по антивирусной защите осуществляется ответственным за организацию работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

XV. Порядок взаимодействия по вопросам обеспечения безопасности ПДн

61. Взаимодействие по вопросам обеспечения безопасности ПДн может осуществляться :

1) управлением;

2) организациями, оказывающими услуги по обеспечению безопасности ПДн;

3) подчиненными организациями и обособленными структурными подразделениями.

62. Взаимодействие по вопросам обеспечения безопасности ПДн с управлением осуществляется в части методического обеспечения и

контроля, а также в целях определения единой стратегии и технической политики в области обеспечения безопасности ПДн. Методическое обеспечение в части методов и способов защиты информации в информационных системах осуществляется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

63. Взаимодействие с организациями, оказывающими услуги пс обеспечению безопасности ПДн, осуществляется на договорной основе. Такие организации в обязательном порядке должны иметь лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации, а в случае оказания ими услуг в области криптографической защиты информации - лицензии Федеральной службы безопасности Российской Федерации.

64. Существенным условием договора с организацией, оказывающей услуги по обеспечению безопасности ПДн, является требование соблюдения конфиденциальности сведений о степени защищенности ИСПДн (внедренных методах и способах защиты и их эффективности).

65. Взаимодействие с подчиненными организациями и обособленными структурными подразделениями осуществляется в части методического руководства и контроля за полнотой и эффективностью принятых мер обеспечения безопасности ПДн. Контрольные мероприятия в подчиненных организациях в обособленных структурных подразделениях осуществляются ответственным за организацию работ по обеспеченшо безопасности ПДн, ответственным пользователем криптосредств (в части использования средств криптографической защиты информации) и сотрудниками отдела программно-технического обеспечения управления, осуществляющими работы по обеспечению безопасности ПДн.

Заместитель начальника Е.В.Клем