ГЛАВНОЕ УПРАВЛЕНИЕ «ГОСУДАРСТВЕННАЯ ЖИЛИЩНАЯ ИНСПЕКЦИЯ» ТВЕРСКОЙ ОБЛАСТИ

г. Тверь

ПРИКАЗ

«14» 10 2013 № 58-ПР

Об утверждении Положения о работе с персональными данными в Главном управлении «Государственная жилищная инспекция» Тверской области

В целях обеспечения защиты информации в Главном управлении «Государственная жилищная инспекция» Тверской области, в соответствии с Федеральными законами от 27.07.2006 № 149 «Об информатизации, информационных технологиях и о защите информации», от 27.07.2006 № 152 «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Положение о работе с персональными данными в Главном управлении «Государственная жилищная инспекция» Тверской области (Приложение).
2. Настоящий приказ довести до сотрудников Главного управления «Государственная жилищная инспекция» Тверской области (по списку).
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Начальник
Главного управления **Т.С. Атаева**

Приложение
к приказу №58-ОД от «14» 10 2015 г.

Положение
о работе с персональными данными в Главном управлении «Государственная жилищная инспекция» Тверской области

Раздел I
Общие положения

1. Настоящее Положение устанавливает порядок обработки документов, содержащих сведения, отнесенные к персональным данным, с использованием средств автоматизации или без использования таких средств, а также исследования и оценки информационных систем персональных данных (далее – ИСПДн) и систем защиты персональных данных (далее – СЗПДн), на которых будет происходить обработка персональных данных в Главном управлении «Государственная жилищная инспекция» Тверской области (далее – Главное управление)

2. Обработка персональных данных физических лиц осуществляется должностными лицами Главного управления в соответствии с полномочиями, определенными их должностными регламентами.

3. Должностные лица Главного управления осуществляют обработку персональных данных следующих категорий субъектов персональных данных:

а) государственные гражданские служащие, служащие и работники Главного управления;

б) физические лица, обращающиеся в Главное управление с письменными предложениями, заявлениями или жалобами, а также устными обращениями;

в) руководители, уполномоченные представители юридических лиц, а также физические лица, состоящие в гражданско-правовых отношениях с Главным управлением;

г) иные физические лица, сведения о персональных данных которых имеются у Главного управления в связи реализацией им своих полномочий.

4. Категории субъектов персональных данных, чьи персональные данные обрабатываются в отделах Главного управления, определяются исходя из решаемых отделом Главного управления задач и полномочий, установленных соответствующими положениями об отделах Главного управления и должностными регламентами сотрудников отделов Главного управления.

5. Объем обрабатываемых персональных данных вышеуказанных категорий субъектов персональных данных определяется Главным управлением самостоятельно, исходя из решаемых задач и полномочий в соответствии с законодательством и нормативными правовыми актами, регулирующими его деятельность.

Раздел II
Принципы обработки персональных данных

6. Обработка персональных данных должна осуществляться на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Главного управления;

в) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки; персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

8. Субъект персональных данных является собственником своих персональных данных и самостоятельно решает вопрос передачи Главному управлению своих персональных данных.

9. Держателем персональных данных является Главное управление, которому субъект персональных данных добровольно передает во владение свои персональные данные. Главное управление выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

10. Право доступа к персональным данным субъекта персональных данных имеют:

начальник Главного управления;

заместитель начальника Главного управления;

должностные лица отдела организационно-правовой работы и бухгалтерского учета в полном составе;

начальник отдела инспектирования;

заместитель начальника отдела инспектирования;

начальник отдела контроля за энергосбережением.

11. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или в Главное управление за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

12. Получение, хранение, комбинирование, передача или любое другое использование персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъектам персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъектов персональных данных, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Раздел III
Обработка и хранение персональных данных

13. Условием обработки персональных данных субъекта персональных данных является его согласие, оформляемое согласно приложению 1 к настоящему Положению. Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных пунктом 14 настоящего Положения. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных при необходимости дается в письменной форме одним из его наследников, если такое согласие не было дано работником при его жизни.

14. Согласие субъекта персональных данных на обработку его персональных данных не требуется в следующих случаях:

а) если обработка персональных данных осуществляется на основании соответствующего федерального закона;

б) если обработка персональных данных осуществляется на основании исполнения трудового, гражданско-правового договора между субъектом персональных данных и Главным управлением;

в) если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

г) если обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение его согласия при данных обстоятельствах невозможно;

д) если обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

е) если осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

15. Не допускается получение и обработка персональных данных субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных пунктом 16 настоящего Положения.

16. Обработка указанных в пункте 15 настоящего Положения персональных данных допускается, в случаях если:

а) субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

б) персональные данные являются общедоступными;

в) персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов его или других лиц, и получение согласия субъекта персональных данных в данный момент невозможно;

г) в иных случаях, предусмотренных законодательством Российской Федерации.

17. Обработка персональных данных о судимости осуществляется в соответствии с федеральными законами.

18. Обработка персональных данных, перечисленных в пункте 15 настоящего Положения, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

19. Сведения, которые характеризуют физиологические особенности человека и на основе которых устанавливается его личность (биометрические персональные данные), обрабатываются только при наличии согласия субъекта персональных данных в письменной форме, за исключением случаев, предусмотренных пунктом 20 настоящего Положения.

20. Обработка биометрических персональных данных осуществляется без согласия субъекта персональных данных в случаях, предусмотренных законодательством Российской Федерации, в частности законодательством о государственной службе.

21. Документы, содержащие персональные данные субъекта персональных данных, составляют его личное дело. Личное дело хранится уполномоченным лицом на бумажных носителях, а помимо этого может храниться в виде электронных документов. Личное дело пополняется на протяжении всей трудовой деятельности субъекта персональных данных. Письменные доказательства получения Главным управлением согласия субъекта персональных данных на обработку его персональных данных хранятся в личном деле субъекта персональных данных.

22. При обработке персональных данных субъектов персональных данных Главное управление определяет способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

Раздел IV
Организация разрешительной системы доступа пользователей к обрабатываемой в информационных системах персональных данных информации

23. К требованиям при регистрации пользователей ИСПДн относятся:

а) получение сведений о персональных данных субъекта персональных данных из следующих документов:

паспорт или иной документ, удостоверяющий личность;

трудовая книжка;

страховое свидетельство государственного пенсионного страхования;

документы воинского учета;

документ об образовании, о квалификации или наличии специальных знаний;

анкета, заполняемая субъектом персональных данных при приеме на работу;

иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, в процессе работы, при обращении субъекта персональных данных к Главному управлению;

б) получение персональных данных лично от субъекта персональных данных. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от субъекта персональных данных документы, проверяет их полноту и правильность указываемых сведений. В случае невозможности получения персональных данных от субъекта персональных данных лично получение возможно от третьих лиц при условии уведомления субъекта персональных данных за 3 календарных дня и получения от него письменного согласия о передаче своих персональных данных третьим лицам;

в) Главное управление должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

24. Внутренний доступ к персональным данным субъекта персональных данных имеют сотрудники Главного управления, указанные в пункте 10 настоящего Положения, которым эти данные необходимы для выполнения должностных обязанностей на основании Регламента разграничения прав доступа (приложение 2 к настоящему Положению).

25. Пользователь персональных данных имеет доступ к своим персональным данным на основании разрешительной системы допуска на объект вычислительной техники.

Раздел V
Конфиденциальность персональных данных

26. Главным управлением и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных пунктом 27 настоящего Положения.

27. Обеспечение конфиденциальности персональных данных не требуется:

а) в случае обезличивания персональных данных;

б) в отношении общедоступных персональных данных.

Раздел VI
Общедоступные источники персональных данных

28. С целью информационного обеспечения деятельности могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и др.). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

29. Сведения о субъекте персональных данных исключаются в любое время из общедоступных источников персональных данных по его требованию, либо по решению Главного управления, либо суда или иных уполномоченных государственных органов.

Раздел VII
Права и обязанности сторон в области обеспечения безопасности персональных данных

30. Субъект персональных данных:

а) передает Главному управлению или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и иные сведения;

б) своевременно сообщает Главному управлению об изменении своих персональных данных;

в) получает полную информацию о своих персональных данных;

г) имеет свободный без взимания платы доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

д) имеет возможность получения относящихся к нему медицинских данных у выбранного им медицинского специалиста;

е) получает сведения о Главном управлении, о месте его нахождения, о наличии у Главного управления персональных данных, относящихся к соответствующему субъекту персональных данных;

ж) требует от Главного управления уточнения своих персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

з) получает информацию, касающуюся обработки его персональных данных, в том числе содержащую подтверждение факта обработки персональных данных Главным управлением, а также цель такой обработки; способы обработки персональных данных, применяемые Главным управлением; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для него может повлечь за собой обработка его персональных данных;

и) при отказе Главного управления исключить или исправить персональные данные субъекта персональных данных он имеет право заявить в письменной форме Главному управлению о своем несогласии с соответствующим обоснованием такого несогласия.

Сведения о наличии персональных данных предоставляются субъекту персональных данных в доступной форме, не содержащей персональные данные, относящиеся к другим субъектам персональных данных.

Доступ к своим персональным данным предоставляется субъекту персональных данных или его представителю Главным управлением при личном обращении либо при получении запроса.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

31. Право субъекта персональных данных на доступ к своим персональным данным ограничивается, в случае если:

а) обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

б) предоставление персональных данных нарушает конституционные права и свободы других лиц;

в) в иных случаях, предусмотренных законодательством Российской Федерации.

32. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных пунктом 33 настоящего Положения.

33. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, принимается на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия субъекта персональных данных в письменной форме или в случаях, предусмотренных федеральными законами.

34. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, разъясняет субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставляет возможность заявить возражение против такого решения, а также разъяснить порядок защиты своих прав и законных интересов. Главное управление рассматривает возражение субъекта персональных данных в течение 7 рабочих дней со дня его получения и уведомляет его о результатах рассмотрения такого возражения.

35. Если обязанность предоставления персональных данных субъектом персональных данных установлена федеральным законом, сотрудник, ответственный за документационное обеспечение кадровой деятельности, разъясняет субъекту персональных данных юридические последствия отказа предоставить свои персональные данные.

36. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, если персональные данные были предоставлены Главному управлению на основании федерального закона или если персональные данные являются общедоступными, Главное управление до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

а) цель обработки персональных данных и ее правовое основание;

б) предполагаемые пользователи персональных данных;

в) права субъекта персональных данных в области защиты персональных данных.

37. Главное управление безвозмездно предоставляет субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также вносит в них необходимые изменения, уничтожает или блокирует соответствующие персональные данные по предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Главное

управление обязано уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта персональных данных были переданы.

38. В случае выявления недостоверных персональных данных или неправомерных действий с ними Главное управление осуществляет блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности персональных данных Главное управление на основании соответствующих документов уточняет персональные данные и снимает их блокирование.

В случае выявления неправомерных действий с персональными данными Главное управление в срок, не превышающий 3 рабочих дней с даты такого выявления, устраняет допущенные нарушения.

В случае невозможности устранения допущенных нарушений Главное управление в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Главное управление уведомляет субъекта персональных данных.

39. В случае достижения цели обработки персональных данных Главное управление незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий 3 рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомляет об этом субъекта персональных данных.

40. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Главное управление прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий 3 рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон.

Раздел VII
Доступ к персональным данным и их передача

41. Внутренний доступ к персональным данным субъекта персональных данных имеют уполномоченные сотрудники отделов Главного управления, указанные в пункте 10 настоящего Положения, которым эти данные необходимы для выполнения должностных обязанностей.

Для хранения персональных данных используются специально оборудованные шкафы или сейфы, которые запираются на ключ.

42. После увольнения субъекта персональных данных документы, содержащие его персональные данные, хранятся в Главном управлении в течение сроков, установленных законодательством.

43. Внешний доступ со стороны третьих лиц к персональным данным субъекта персональных данных осуществляется только с письменного согласия субъекта персональных данных, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта персональных данных или других лиц, и иных случаев, установленных законодательством.

44. Главное управление обязано сообщать персональные данные субъекта персональных данных по надлежаще оформленным запросам суда, прокуратуры, правоохранительных органов.

45. При передаче персональных данных субъекта персональных данных внешнему потребителю Главное управление передает минимальный объем персональных данных и только в целях выполнения задач, соответствующих объективной причине сбора этих данных. Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

46. Доступ к персональным данным субъектов персональных данных, обрабатываемых Главным управлением, разрешается только специально уполномоченным лицам (внутреннему потребителю).

Внутренние потребители персональных данных в обязательном порядке под подпись знакомятся с настоящим Положением и подписывают обязательство о неразглашении информации, содержащей персональные данные (приложение 3 к настоящему Положению).

47. Регламентация доступа сотрудников Главного управления к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации. Для защиты персональных данных субъектов персональных данных Главное управление:

а) ограничивает и регламентирует состав сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

б) избирательно и обоснованно распределяет документы и информацию между сотрудниками;

в) рационально размещает рабочие места сотрудников, исключая бесконтрольное использование защищаемой информации;

г) обеспечивает ознакомление сотрудников с требованиями документов по защите персональных данных;

д) обеспечивает соответствие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

е) определяет и регламентирует состав сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

ж) организует порядок уничтожения информации;

з) своевременно выявляет нарушения требований разрешительной системы доступа сотрудниками структурных подразделений, допущенными к обработке персональных данных;

и) обеспечивает воспитательную и разъяснительную работу с сотрудниками по предупреждению утраты сведений при работе с конфиденциальными документами.

Раздел IX
Безопасность персональных данных

48. При обработке персональных данных необходимо принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

49. Использование и хранение биометрических персональных данных вне ИСПДн осуществляются только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

50. Организация работ по обеспечению безопасности персональных данных осуществляется в соответствии с установленной начальником Главного управления схемой организации работ по обеспечению безопасности персональных данных (приложение 4 к настоящему Положению).

Раздел X
Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

51. Каждый сотрудник Главного управления, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

52. Нарушение установленного законом порядка сбора, хранения, использования или распространения персональных данных влечет ответственность граждан и юридических лиц в соответствии с законодательством Российской Федерации.

Раздел XI
Порядок классификации информационных систем персональных данных

53. Классификация ИСПДн проводится на этапе их создания или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных.

54. Проведение классификации ИСПДн состоит из:

а) сбора и анализа исходных данных по ИСПДн;

б) присвоения ИСПДн соответствующего класса и его документального оформления.

55. При проведении классификации ИСПДн учитываются:

а) категория обрабатываемых в ИСПДн персональных данных - Хпд;

б) объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн) - Хнпд;

в) заданные Главным управлением характеристики безопасности персональных данных, обрабатываемых в ИСПДн;

г) структура ИСПДн;

д) наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена;

е) режим обработки персональных данных;

ж) режим разграничения прав доступа пользователей ИСПДн;

з) местонахождение технических средств ИСПДн.

56. Определяются следующие категории обрабатываемых в ИСПДн персональных данных (Хпд):

а) категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

б) категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

в) категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;

г) категория 4 - обезличенные и (или) общедоступные персональные данные.

57. Объем обрабатываемых персональных данных (Хнпд) может принимать следующие значения:

а) 1 - в ИСПДн одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах Тверской области;

б) 2 - в ИСПДн одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти (государственном органе) Тверской области, проживающих в пределах муниципального образования Тверской области;

в) 3 – в ИСПДн одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

58. Главное управление определяет ИСПДн как типовую информационную систему ИСПДн, в которой требуется обеспечение только конфиденциальности персональных данных, и как специальную

информационную систему ИСПДн, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

59. По результатам анализа исходных данных типовой ИСПДн присваивается один из следующих классов:

а) класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

б) класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

в) класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

г) класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

60. Класс типовой информационной системы ИСПДн определяется в соответствии с нижеприведенной таблицей.

Хпд \ Хнпд	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

61. В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем.

62. Результаты классификации ИСПДн оформляются соответствующим актом.

63. Класс ИСПДн пересматривается:

а) по решению лица, ответственного за обеспечение безопасности персональных данных, на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

б) по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Раздел XII
Порядок разработки, ввода в действие и эксплуатацию системы защиты персональных данных

64. Порядок предпроектного обследования ИСПДн включает:

а) определение перечня персональных данных обрабатываемых в ИСПДн;

б) определение перечня персональных данных, подлежащих защите от несанкционированного доступа (далее - НсД);

в) определение условий расположения ИСПДн относительно границ контролируемой зоны;

г) определение конфигурации и топологии ИСПДн в целом и ее отдельных компонентов; физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

д) определение технических средств и систем, предполагаемых к использованию в разрабатываемой ИСПДн, условия их расположения; общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

е) определение режимов обработки персональных данных в ИСПДн в целом и в отдельных компонентах;

ж) определение класса ИСПДн;

з) уточнение степени участия должностных лиц в обработке персональных данных, характер их взаимодействия между собой;

и) определение (уточнение) угроз безопасности персональным данным применительно к конкретным условиям функционирования ИСПДн.

65. По результатам предпроектного обследования на основе документа с учетом установленного класса ИСПДн задаются конкретные требования по обеспечению безопасности персональных данных, включаемые в техническое задание на разработку СЗПДн. Разработка технического задания на создание СЗПДн включает:

а) обоснование разработки СЗПДн;

б) исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

в) класс ИСПДн;

г) требования федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

д) перечень предполагаемых к использованию сертифицированных средств защиты информации;

е) обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;

ж) состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

66. Проектирование и реализация СЗПДн включает:

а) разработку задания и проекта проведения работ (в том числе строительных и строительно-монтажных) по созданию (реконструкции) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

б) выполнение работ в соответствии с проектной документацией;

в) закупку обоснованной совокупности используемых в ИСПДн серийно выпускаемых технических средств обработки, передачи и хранения информации;

г) разработку мероприятий по защите информации в соответствии с предъявляемыми требованиями;

д) закупку обоснованной совокупности используемых в ИСПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

е) проведение сертификации по требованиям безопасности информации технических, программных и программно-технических средств защиты информации, в случае когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

ж) разработку и реализацию разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

з) определение структурных подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, с их обучением по направлению обеспечения безопасности персональных данных;

и) разработку эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации;

к) выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности персональных данных.

67. Ввод в действие СЗПДн включает:

а) выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации;

б) опытную эксплуатацию средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

в) приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации;

г) организацию охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам

ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

д) оценку соответствия ИСПДн требованиям безопасности персональных данных.

Раздел XIII
Порядок контроля за обеспечением уровня безопасности персональных данных и оценки соответствия информационных систем персональных данных

68. Порядок обследования защищенности персональных данных включает:

а) выделение информационных ресурсов, содержащих в себе персональные данные, а также технические средства, позволяющие осуществлять обработку персональных данных, из всей совокупности обрабатываемой информации;

б) определение соответствия действующей системы обработки персональных данных требованиям, установленным федеральным законодательством;

в) классификация информационных систем персональных данных.

69. По итогам обследования Главное управление получает:

а) аналитический отчет о предпроектном обследовании и текущей защищенности персональных данных;

б) акт классификации ИСПДн.

70. Подготовка ИСПДн к проведению оценки соответствия ИСПДн требованиям безопасности персональных данных и созданию СЗПДн осуществляется путем:

а) анализа информационных ресурсов (определения перечня всех существующих ИСПДн; определения состава и структуры каждой ИСПДн; определения перечня и местонахождения персональных данных, подлежащих защите; категорирования персональных данных; определения режима обработки персональных в целом и отдельных компонентах);

б) анализа уязвимых звеньев и возможных угроз безопасности персональных данных (оценки возможности физического доступа к ИСПДн;

выявления возможных каналов утечки информации, в том числе технических; анализа возможностей программно-математического воздействия на ИСПДн; анализа возможностей электромагнитного воздействия на ИСПДн);

в) оценки ущерба от реализации угроз безопасности персональных данных (оценки непосредственного и опосредованного ущерба от реализации угроз безопасности персональных данных);

г) анализа имеющихся в распоряжении мер и средств защиты персональных данных (от физического доступа; от утечки по техническим каналам; от НсД; от программно-математического воздействия; от электромагнитных воздействий).

71. Обоснование требований по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, включает:

а) разработку модели угроз безопасности персональных данных;

б) разработку модели нарушителя безопасности персональных данных;

в) составление перечня и проведение оценки актуальных угроз безопасности персональных данных;

г) определение класса ИСПДн.

72. Проведение работ по организации обеспечения безопасности персональных данных при их обработке в ИСПДн включает:

а) разработку и согласование с уполномоченными службами требований к СЗПДн и формулирование задач по защите персональных данных (разработка перечня мероприятий по защите персональных данных в соответствии с выбранным классом ИСПДн);

б) выбор способов, мер и средств защиты персональных данных в соответствии с мероприятиями по защите;

в) разработку технического задания на СЗПДн;

г) разработку документов, регламентирующих вопросы организации обеспечения безопасности персональных данных и эксплуатации СЗПДн в ИСПДн;

д) развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

е) доработку СЗПДн по результатам опытной эксплуатации;

ж) проведение работ по аттестации ИСПДн по требованиям безопасности информации.

Приложение 1
к Положению о работе с
персональными данными
в Главном управлении
«Государственная жилищная
инспекция» Тверской области

СОГЛАСИЕ
на обработку персональных данных

г. _____ «___» _____ 20__г.

Я, _____,
(Ф.И.О)
_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)
_____,
(когда и кем)
проживающий (ая) по адресу:_____
_____,
настоящим даю свое согласие на обработку _____
_____
(наименование и адрес Главного управления)
моих персональных данных и подтверждаю, что, давая такое согласие, я действую осознанно и в своих интересах.
Согласие дается мною с целью _____
_____
(цель обработки персональных данных)
и распространяется на следующую информацию: _____
_____
_____;
(перечень персональных данных)

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с федеральным законодательством.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с «__» _____ 20___ г. по «__» _____ 20___ г.

_____
(Ф.И.О., подпись лица, давшего согласие)

Приложение 2
к Положению о работе с
персональными данными
в Главном управлении
«Государственная жилищная
инспекция» Тверской области

Утверждаю
Начальник Главного управления
«Государственная жилищная
инспекция» Тверской области

_____
«___» _____ 20__ г.

Регламент разграничения прав доступа

№ п/п	Ф.И.О. сотрудника	Структурное подразделение	Должность	Информационные системы персональных данных, к которым разрешен доступ

Ответственный за обеспечение безопасности
персональных данных _____
(фамилия и инициалы)

"____" _____ 20__ г.

Приложение 3
к Положению о работе с
персональными данными
в Главном управлении
«Государственная жилищная
инспекция» Тверской области

Обязательство
о неразглашении информации, содержащей персональные данные

Я,_____,
(Ф.И.О. сотрудника Главного управления)
исполняющий (ая) должностные обязанности по замещаемой должности
_____
_____,
(должность, наименование структурного подразделения Главного управления)
предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

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 об этом непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

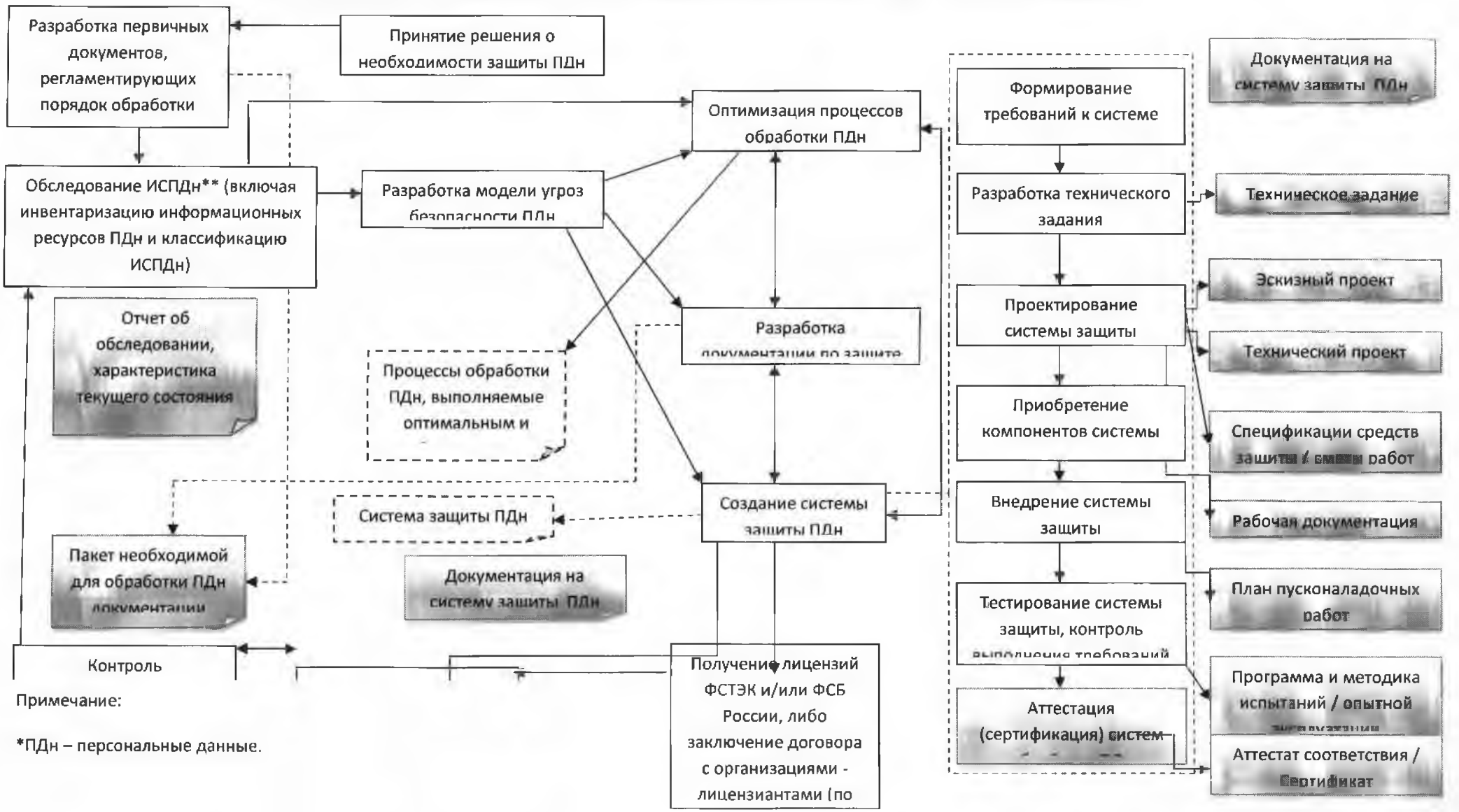
Я предупрежден (а) о том, что в случае нарушения данного обязательства могу быть привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(Ф.И.О.) (подпись)

«_____»_____ 20___ г.

Приложение 4
к Положению о работе с персональными данными
в Главном управлении «Государственная жилищная инспекция»
Тверской области

Схема организации работ по обеспечению безопасности персональных данных



Примечание:

*ПДн – персональные данные.