Приложение
к приказу комитета по делам
молодежи Тверской области
от 28.04.2011 № 86
(в редакции приказа Комитета по
делам молодежи Тверской области
от 14.10.2013 № 184)

# Положение
# о работе с персональными данными в Комитете по делам молодежи 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 Комитете по делам молодежи Тверской области (далее – оператор).

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

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

а) государственные гражданские служащие, служащие и работники оператора;

б) физические лица, обращающиеся к оператору 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 оператором;

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

4. Категории субъектов персональных данных, чьи персональные данные обрабатываются в структурных подразделениях оператора, определяются исходя из решаемых структурным подразделением оператора задач и полномочий, установленных соответствующими положениями о структурных подразделениях оператора и должностными регламентами сотрудников структурных подразделений оператора.

5. Объем обрабатываемых персональных данных вышеуказанных категорий субъектов персональных данных определяется оператором

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 осуществляется 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 оператора;

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 оператору своих персональных данных.

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

10. Право доступа к персональным данным субъекта персональных данных имеют лица, уполномоченные оператором.

11. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или оператору 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 оператором;

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 оператором согласия субъекта персональных данных на обработку его персональных данных хранятся в личном деле субъекта персональных данных.

22. При обработке персональных данных субъектов персональных данных оператор 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 оператору;

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) оператор должен 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 структурных подразделений оператора, 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 «Автоматизированное рабочее место на базе автономной персональной электронной вычислительной машины (инв. №_____)_____» (приложение 3 к настоящему Положению).

(наименование оператора)

## Раздел V
## Конфиденциальность персональных данных

26. Оператором 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 оператора, 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 оператору 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 оператору 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 об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных;

ж) требует от оператора 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 оператором, а также цель такой обработки; способы обработки персональных данных, применяемые оператором; 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 оператора исключить или исправить персональные данные субъекта персональных данных он имеет право заявить в письменной форме оператору 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 оператором 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 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. Оператор 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. Оператор 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, оператор 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 оператору на основании федерального закона или если персональные данные являются общедоступными, оператор до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:

а) наименование и адрес оператора или его представителя;

б) цель обработки персональных данных и ее правовое основание;

в) предполагаемые пользователи персональных данных;

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

37. Оператор 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 оператор обязан 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 оператор 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 оператор на основании соответствующих документов уточняет персональные данные и снимает их блокирование.

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

В случае невозможности устранения допущенных нарушений оператор 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 оператор уведомляет субъекта персональных данных.

39. В случае достижения цели обработки персональных данных оператор 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 оператор 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. Об уничтожении персональных данных оператор уведомляет субъекта персональных данных.

## Раздел VIII
## Доступ к персональным данным и их передача

41. Внутренний доступ к персональным данным субъекта персональных данных имеют уполномоченные сотрудники структурных подразделений оператора, 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 у оператора 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. Оператор обязан сообщать персональные данные субъекта персональных данных по надлежаще оформленным запросам суда, прокуратуры, правоохранительных органов.

45. При передаче персональных данных субъекта персональных данных внешнему потребителю оператор 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 оператором, 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 4 к настоящему Положению).

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

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. Оператор при обработке персональных данных обязан 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 председателем оператора схемой организации работ по обеспечению безопасности персональных данных (приложение 5 к настоящему Положению).

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

51. Каждый сотрудник оператора, 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 оператором 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. Оператор 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 оператора.

63. Класс ИСПДн пересматривается:

а) по решению оператора 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 оператор 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 комитете по делам молодежи 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 оператора)
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 комитете по делам молодежи Тверской области

Утверждаю
_____
(должность, фамилия и инициалы)
«___» _____ 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
комитете по делам молодежи
Тверской области

Утверждаю
_____
(должность, фамилия и инициалы)
«___» _____ 20__ г.

Разрешительная система допуска
на объект вычислительной техники
«Автоматизированное рабочее место
на базе автономной персональной электронной вычислительной машины
(инв. №___)

»

(наименование оператора)

1. Перечень лиц, имеющих самостоятельный доступ к штатным средствам объекта вычислительной техники (субъектов доступа):

| Ф.И.О. | Уровень полномочий (Администратор/ Пользователь) | Имя в системе | Вид выполняемых функций |
|---|---|---|---|
| | | | |

2. Перечень защищаемых информационных ресурсов объекта вычислительной техники (объектов доступа):

| Место хранения защищаемого ресурса | Категория защищаемого ресурса | Содержание ресурса |
|---|---|---|
| | | |

3. Матрица разграничения доступа к защищаемым ресурсам автоматизированной системы (месту хранения и используемым техническим средствам):

| Тип ресурса (информационный/ аппаратный) | Название ресурса | Имя пользователя и полномочия* | |
|---|---|---|---|
| | | Администратор | Пользователи |
| | | | |

Примечание*
«+» – полные права на доступ;
«-» – отсутствуют права на доступ;
«Ч» – читать файлы (массивы информации);

«З» – записывать: добавлять (создавать) файлы (массивы информации), вносить изменения, удалять файлы (массивы информации), сохранять (записывать) на учтенные магнитные носители, распечатывать на принтере файлы (массивы информации).

Ответственный за обеспечение безопасности
персональных данных _____

( фамилия и инициалы)

“____” _____ 20__ г.

Приложение 4
к Положению о работе с персональными данными в комитете по делам молодежи Тверской области

Обязательство
о неразглашении информации, содержащей персональные данные

Я,_____,
(Ф.И.О. сотрудника оператора)
исполняющий (ая) должностные обязанности по замещаемой должности
_____
_____,
(должность, наименование структурного подразделения оператора)
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.

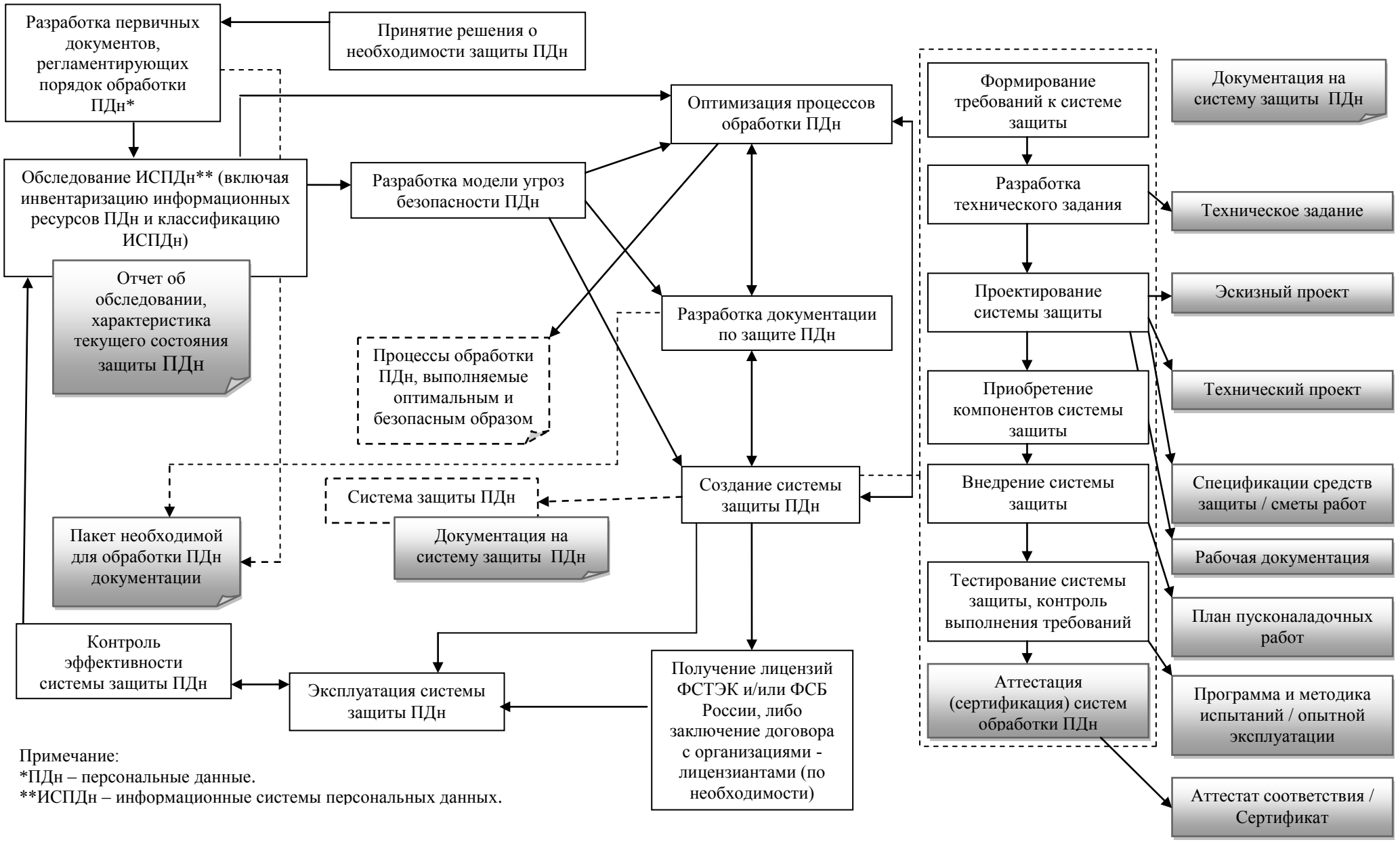
Я предупрежден (а) о том, что в случае нарушения данного обязательства могу быть привлечен (а) к ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(Ф.И.О.) (подпись)

«_____»_____ 20___г.

Приложение 5
к Положению о работе с персональными данными
в комитете по делам молодежи Тверской области

# Схема организации работ по обеспечению безопасности персональных данных




Примечание:
*ПДн – персональные данные.
**ИСПДн – информационные системы персональных данных.

Приложение 6
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Правила обработки персональных данных**
**в Комитете по делам молодежи Тверской области**

Раздел I
Общие положения

1. Настоящие Правила обработки персональных данных (далее — Правила) в Комитете по делам молодежи Тверской области разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. В состав персональных данных, обрабатываемых в Комитете по делам молодежи Тверской области, входят_____
_____
_____.
(перечень персональных данных, обрабатываемых в Комитете по делам молодежи Тверской области)

Раздел II
Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных

3. Источником информации о нарушениях законодательства Российской Федерации в сфере персональных данных могут служить:

сообщения работников, или пользователей информационных систем персональных данных (далее – ИСПДн) Комитета по делам молодежи Тверской области;

сообщения субъектов персональных данных;

уведомления/сообщения органов, осуществляющих контроль или надзор за деятельностью Комитета по делам молодежи Тверской области;

данных, полученных на основании анализа электронных журналов безопасности ИСПДн.

4. При получении сообщения о нарушениях законодательства Российской Федерации в сфере персональных данных по электронной почте или по телефонному звонку необходимо убедиться в достоверности полученной информации (например, путем совершения «обратного» звонка по указанным в сообщении телефонам, проверки данных указанных в подписи сообщения или названных при звонке).

5. Сотрудник, получивший информацию о нарушениях законодательства Российской Федерации в сфере персональных данных, сообщает об этом должностному лицу Комитета по делам молодежи Тверской области, ответственному за организацию обработки персональных данных, и руководителю структурного подразделения Комитета по делам молодежи Тверской области.

6. Должностное лицо, ответственное за организацию обработки персональных данных, в письменной форме сообщает о факте нарушения председателю Комитета по делам молодежи Тверской области.

7. Приказом председателя Комитета по делам молодежи Тверской области для разбора факта нарушения законодательства Российской Федерации в сфере персональных данных создается комиссия, в состав которой могут входить:

должностное лицо, ответственное за организацию обработки персональных данных;

руководитель структурного подразделения Комитета по делам молодежи Тверской области, в котором зафиксирован факт нарушения законодательства Российской Федерации в сфере персональных данных;

председатель (заместитель председателя) Комитета по делам молодежи Тверской области;

субъект персональных данных, права которого в сфере персональных данных нарушены.

8. Комиссия собирает и анализирует все данные об обстоятельствах нарушения законодательства Российской Федерации в сфере персональных данных (электронные письма, логи информационных систем, показания сотрудников и др.), устанавливает, имела ли место утечка сведений и обстоятельства ей сопутствующие, определяет перечень лиц, виновных в нарушении предписанных федеральным законодательством и законодательством Тверской области мероприятий по защите персональных данных, устанавливает причины и условия, способствовавшие нарушению.

9. По итогам работы комиссии председателю Комитета по делам молодежи Тверской области предоставляется отчет, в котором указываются причина нарушения законодательства Российской Федерации в сфере персональных данных, последствия данного факта, лица, виновные в возникновении нарушения законодательства Российской Федерации в сфере персональных данных, предложения о наказании виновных лиц и мерах по недопущению подобных инцидентов в будущем.

## Раздел III
## Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения

10. Процедуры, определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения сводятся в соответствующую таблицу.

| № п/п | Цели обработки персональных данных | Содержание обрабатываемых персональных данных | Категории субъектов персональных данных | Сроки обработки/ хранения персональных данных |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |

## Раздел IV
## Порядок учета, хранения и передачи электронных носителей персональных данных

11. Учет всех видов электронных носителей и накопителей персональных данных, используемых в электронно-вычислительной технике (в т.ч дисков, дискет, съемных носителей), осуществляется в журнале учета электронных носителей, содержащих сведения конфиденциального характера.

12. Порядок учета определяется нормативным правовым актом Правительства Тверской области.

## Раздел V
## Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

13. По окончании указанных в разделе III сроков хранения персональных данных, они физически уничтожаются с целью невозможности восстановления и дальнейшего использования.

Уничтожение персональных данных, расположенных на жестких дисках компьютеров, а также съемных носителях производится специальными программными средствами, осуществляющими удаление информации без возможности ее восстановления.

Уничтожение персональных данных, расположенных на оптических дисках осуществляется путем физического уничтожения носителя.

14. Для уничтожения персональных данных приказом председателя Комитета по делам молодежи Тверской области создается комиссия, состав которой могут входить:

должностное лицо, ответственное за организацию обработки персональных данных;

руководитель структурного подразделения Комитета по делам молодежи Тверской области, в котором обрабатывались уничтожаемые персональные данные;

председатель (заместитель председателя) Комитета по делам молодежи Тверской области.

15. По результатам работы комиссии составляется акт уничтожения персональных данных на программно-технических средствах ИСПДн (Приложение 1 к Правилам)

Ответственный за организацию
обработки персональных данных

_____

( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 1
к Правилам обработки
персональных данных

Утверждаю

_____

(должность, инициалы, фамилия)

«___» _____ 20__ г.

# АКТ
## уничтожения персональных данных на программно-технических средствах ИСПДн Комитета по делам молодежи Тверской области

Председатель комиссии: _____

(Должность, Ф.И.О)

Члены комиссии:

_____

(Должность, Ф.И.О)

_____

(Должность, Ф.И.О)

_____

(Должность, Ф.И.О)

составили настоящий акт в том, что «__» _____ 20__ г. произведено уничтожение персональных данных, _____

_____

(наименование персональных данных)

находящихся на _____

(наименование ИСПДн и носителя информации)

_____

Персональные данные были уничтожены путем _____

_____

(способ уничтожения информации)

Председатель комиссии: _____ «__» _____ 20__ г.

(подпись)

Члены комиссии:

_____ _____ «__» _____ 20__ г.

(Фамилия, инициалы) (подпись)

_____ _____ «__» _____ 20__ г.

(Фамилия, инициалы) (подпись)

_____ _____ «__» _____ 20__ г.

(Фамилия, инициалы) (подпись)

Приложение 7
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Правила**
**рассмотрения запросов субъектов персональных данных**
**или их представителей в Комитете по делам молодежи Тверской области**

Раздел I
Общие положения

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее Правила) Комитета по делам молодежи Тверской области разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяют порядок обработки поступающих в Комитет по делам молодежи Тверской области обращений субъектов персональных данных.

Раздел II
Порядок работы с обращениями субъектов персональных данных

2. Жалобы и обращения субъектов персональных данных и их представителей в Комитет по делам молодежи Тверской области регистрируются и рассматриваются в порядке, установленном федеральным законодательством и законодательством Тверской области.

3. Комитет по делам молодежи Тверской области в письменной форме сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных.

4. Комитет по делам молодежи Тверской области предоставляет субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также вносит в них необходимые изменения, уничтожает или блокирует соответствующие персональные данные при предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту персональных данных и обработку которых осуществляет Комитет по делам молодежи Тверской области, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых

мерах Комитет по делам молодежи Тверской области уведомляет субъекта персональных данных или его законного представителя.

Ответственный за организацию
обработки персональных данных

_____

( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 8
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Правила**
**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Комитете по делам молодежи Тверской области**

Раздел I
Общие положения

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в Комитете по делам молодежи Тверской области разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Раздел II
Тематика внутреннего контроля

2. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя матрице доступа;

б) соблюдение пользователями информационных систем персональных данных Комитета по делам молодежи Тверской области правил использования паролей;

в) соблюдение пользователями информационных систем персональных данных Комитета по делам молодежи Тверской области требований федерального законодательства и законодательства Тверской области по использованию антивирусной защиты;

г) соблюдение пользователями информационных систем персональных данных Комитета по делам молодежи Тверской области требований федерального законодательства и законодательства Тверской области по работе со съемными носителями персональных данных;

д) соблюдение требований федерального законодательства и законодательства Тверской области ответственными за криптографические средства защиты информации правил работы с ними;

е) соблюдение порядка доступа в помещения Комитета по делам молодежи Тверской области, где расположены элементы информационных систем персональных данных;

ж) соблюдение требований федерального законодательства и законодательства Тверской области по порядку резервирования баз данных и хранения резервных копий;

з) соблюдение порядка работы с аппаратными средствами защиты информации;

и) знание пользователями информационных систем персональных данных порядка своих действий во внештатных ситуациях.

3. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соблюдение правил хранения бумажных носителей с персональными данными;

б) соблюдение порядка доступа к бумажным носителям с персональными данными;

в) соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

## Раздел III
## Порядок проведения внутренних проверок

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям Комитет по делам молодежи Тверской области организует проведение периодических проверок условий обработки персональных данных в соответствии с планом проверок (приложение 1).

5. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных (далее - Ответственный), либо комиссией, создаваемой председателем Комитета по делам молодежи Тверской области.

6. Внутренние проверки проводятся по необходимости в соответствии с поручением председателя Комитета по делам молодежи Тверской области но не реже одного раза в год.

7. Внутренние проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

8. По результатам каждой проверки составляется Протокол проведения внутренней проверки (приложение 2).

9. При выявлении в ходе проверки нарушений, Ответственным либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

10. Протоколы хранятся у Ответственного в течение текущего года. Уничтожение протоколов проводится Ответственным самостоятельно в первом квартале года, следующего за отчетным.

11. О результатах проверки и мерах, необходимых для устранения нарушений, председателю Комитета по делам молодежи Тверской области исполнительного органа власти Тверской области) докладывает Ответственный (председатель комиссии).

Ответственный за организацию
обработки персональных данных

_____

( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 1
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных

Утверждаю

_____
(должность, инициалы и фамилия)
«___» _____ 20__ г.

**План**
**внутренних проверок условий обработки персональных данных**
**Комитета по делам молодежи Тверской области**

| № п/п | Тема проверки | Нормативный документ, предъявляющий требования | Срок проведения | Исполнитель |
|---|---|---|---|---|
| 1. | Соответствие полномочий пользователя требованиям к защите персональных данных | Перечень ИСПДн<br>Перечень должностей служащих…<br>Порядок доступа служащих…<br>Правила обработки персональных данных | | |
| 2. | Соблюдение пользователями ИСПДн парольной политики | Политика информационной безопасности | | |
| 3. | Соблюдение пользователями ИСПДн антивирусной политики | Политика информационной безопасности | | |
| 4. | Соблюдение пользователями ИСПДн правил работы со съемными носителями персональных данных | Политика информационной безопасности | | |

| | | | | |
|---|---|---|---|---|
| 5. | Соблюдение пользователями правил работы с криптографическими средствами защиты информации | Политика информационной безопасности | | |
| 6. | Соблюдение порядка доступа в помещения, где расположены элементы ИСПДн | Порядок доступа служащих в помещения, где ведется обработка персональных данных | | |
| 7. | Соблюдение порядка резервирования баз данных и хранения резервных копий | Политика информационной безопасности | | |
| 8. | Соблюдение порядка работы со средствами защиты информации | Политика информационной безопасности | | |
| 9. | Знание пользователями ИСПДн своих действий во внештатных ситуациях | Политика информационной безопасности | | |
| 10. | Хранение бумажных носителей с персональными данными | Законодательство Российской Федерации | | |
| 11. | Доступ к бумажным носителям с персональными данными | Законодательство Российской Федерации | | |
| 12. | Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными | Порядок доступа служащих в помещения, где ведется обработка персональных данных | | |

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных

Утверждаю
_____
(должность, инициалы и фамилия)
«___» _____ 20__ г.

Протокол
проведения внутренней проверки условий обработки персональных данных
Комитета по делам молодежи Тверской области

Настоящий Протокол составлен в том, что «__» _____20__ г. ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка _____.
тема проверки

Проверка осуществлялась в соответствии с требованиями _____.
название документа

В ходе проверки проверено:
_____.

Выявленные нарушения:
_____.

Меры по устранению нарушений:
_____.

Срок устранения нарушений: _____.

Председатель комиссии: _____ «__» _____ 20__ г.
(подпись)

Члены комиссии:

_____ _____ «__» _____ 20__ г.
(инициалы, фамилия) (подпись)

_____ _____ «__» _____ 20__ г.
(инициалы, фамилия) (подпись)

Приложение 9
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Правила**
**работы с обезличенными персональными данными в Комитете по делам молодежи Тверской области**

Раздел I
Общие положения

1. Настоящие Правила работы с обезличенными персональными данными (далее — Правила) Комитета по делам молодежи Тверской области разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяют порядок работы с обезличенными данными в Комитете по делам молодежи Тверской области.

2. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Раздел II
Условия обезличивания персональных данных

3. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных (далее – ИСПДн) Комитета по делам молодежи Тверской области.и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Способы обезличивания при условии дальнейшей обработки персональных данных:

а) уменьшение перечня обрабатываемых сведений;

б) замена части сведений идентификаторами;

в) обобщение – понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

г) деление сведений на части и обработка в разных ИСПДн;

д) другие способы.

5. Решение о необходимости обезличивания персональных данных принимает председатель Комитета по делам молодежи Тверской области.

Должностные лица Комитета по делам молодежи Тверской области, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания, а после принятия соответствующего решения осуществляют непосредственное обезличивание выбранным способом.

## Раздел III
## Порядок работы с обезличенными персональными данными

6. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

7. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

8. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

а) парольной политики;

б) антивирусной политики;

в) правил работы со съемными носителями (если они используется);

г) правил резервного копирования;

д) правил доступа в помещения, где расположены элементы информационных систем.

9. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

а) правил хранения бумажных носителей;

б) правил доступа к ним и в помещения, где они хранятся.

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 10
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Перечень**
**информационных систем персональных данных**
**Комитета по делам молодежи Тверской области**

| № п/п | Наименование ИСПДн | Категории обрабатываемых персональных данных | Количество субъектов персональных данных | Наличие подключения к сетям | Необходимый уровень защищенности ИСПДн | Примечание |
|---|---|---|---|---|---|---|
| 1 | 2 | | 3 | | 4 | 5 |
| | | | | | | |

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 11
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**ПЕРЕЧЕНЬ**
**персональных данных, обрабатываемых**
**в Комитете по делам молодежи Тверской области в связи с реализацией трудовых отношений**

| N п/п | Наименование ПДн | Вид носителя | Способ обработки | Примечание |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 12
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**ПЕРЕЧЕНЬ**
**персональных данных, обрабатываемых**
**в Комитете по делам молодежи Тверской области в связи с**
**осуществлением государственных функций**

| N п/п | Наименование ПДн | Вид носителя | Способ обработки | Примечание |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 13
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Перечень должностей служащих,
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных в
Комитете по делам молодежи Тверской области**

1. _____;
2. _____;
3. _____;
4. _____;
5. _____;
6. _____;
7. _____;
8. _____.

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 14
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Перечень должностей Комитета по делам молодежи Тверской области замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным**

| № п/п | Должность | Наименование ИСПДн, к которой разрешен доступ | Уровень полномочий (Администратор / Пользователь) | Вид выполняемых функций |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| | | | | |

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 15
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Должностная инструкция**
**ответственного за организацию обработки персональных данных в Комитете по делам молодежи Тверской области**

Раздел I
Общие положения

1. Ответственное лицо за организацию обработки персональных данных (далее – ответственный) – отвечает за организацию обработки персональных данных в информационной (ых) системе(ах) персональных данных (далее – ИСПДн) в Комитете по делам молодежи Тверской области.

2. Ответственный назначается из числа сотрудников приказом председателя Комитета по делам молодежи Тверской области.

3. Ответственный, в рамках исполнения обязанностей по организации обработки персональных данных в ИСПДн подчиняется непосредственно председателю Комитета по делам молодежи Тверской области и осуществляет контроль за выполнением требований нормативных и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Комитета по делам молодежи Тверской области.

4. Методическое руководство работой ответственного осуществляется уполномоченным областным исполнительным органом государственной власти Тверской области в сфере защиты информации.

Раздел II
Обязанности ответственного

5. Ответственный обязан:

а) обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации ИСПДн, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранность;

б) проводить инструктаж и консультации пользователей ИСПДн по соблюдению режима конфиденциальности;

в) организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными носителями информации, выполнению организационных мер по защите

персональных данных, а также принимать участие в проведении проверок уполномоченными структурами;

г) взаимодействовать с должностными лицами уполномоченного областного исполнительного органа государственной власти Тверской области в сфере защиты информации по вопросам обеспечения и выполнения требований федерального законодательства и законодательства Тверской области при обработке персональных данных;

д) организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа;

знать перечень установленных в Комитете по делам молодежи Тверской области аппаратных и программных средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

е) контролировать целостность печатей (логотипов) на устройствах защищенных (допущенных к обработке персональных данных) компьютеров и серверов;

ж) обеспечивать соблюдение сотрудниками Комитета по делам молодежи Тверской области утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава ИСПДн;

з) хранить техническую документацию защищенных компьютеров и серверов, контролировать ее соответствие реальным конфигурациям и вести учет изменений их аппаратно-программной конфигурации;

и) осуществлять контроль за порядком учета, создания, хранения и использования резервных копий документов, содержащих персональные данные;

к) контролировать порядок использования и обеспечения сохранности персональных устройств идентификации пользователей;

л) при выявлении возможных каналов неправомерного вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава ИСПДн, сообщать о них руководителю Комитета по делам молодежи Тверской области и в уполномоченный областной исполнительный орган государственной власти Тверской области в сфере защиты информации;

м) инструктировать сотрудников по вопросам обеспечения безопасности персональных данных и правилам работы с применяемыми средствами зашиты персональных данных.

## Раздел III
## Права ответственного

6. Ответственный имеет право:

а) требовать от пользователей ИСПДн Комитета по делам молодежи Тверской области выполнения установленной технологии обработки

персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

б) участвовать в разработке мероприятий Комитета по делам молодежи Тверской области по совершенствованию безопасности персональных данных;

в) инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности персональных данных, несанкционированного доступа, утраты, порчи защищаемых персональных данных и программных и аппаратных средств из состава ИСПДн;

г) обращаться к председателю Комитета по делам молодежи Тверской области с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности;

д) подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных в Комитете по делам молодежи Тверской области.

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 16
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные**

Уважаемый (ая) _____.
(фамилия, имя, отчество субъекта персональных данных)

Лица, которые намерены вступить в те, или иные правовые отношения с Комитетом по делам молодежи Тверской области не обязаны предоставлять персональные данные, однако, непредоставление данной информации может сделать невозможным продолжение правовых отношений с Комитетом по делам молодежи Тверской области, выполнение юридических и иных обязательств.

Персональные данные хранятся и обрабатываются в Комитете по делам молодежи Тверской области в соответствии с федеральным законодательством и законодательством Тверской области.

Председатель Комитета по делам
молодежи Тверской области _____
(инициалы, фамилия)

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.

Приложение 17
к положению о работе с
персональными данными в
Комитете по делам молодежи
Тверской области

**Порядок**
**доступа служащих Комитета по делам молодежи Тверской области**
**в помещения, в которых ведется обработка персональных данных**

Раздел I
Общие положения

1. Настоящий порядок разработан в соответствии с законодательством Российской Федерации и законодательством Тверской области, и определяет порядок доступа в помещения, где обрабатываются персональные данные и к информационным системам персональных данных (далее – ИСПДн) в Комитете по делам молодежи Тверской области.

2. Перечень сотрудников, допущенных к работе с персональными данными в ИСПДн определяется приказом председателя Комитета по делам молодежи Тверской области.

3. В своей работе сотрудники, допущенные к обработке персональных данных, должны руководствоваться требованиями Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных», правовых документов Правительства Российской Федерации, ФСТЭК России, ФСБ России, а также настоящим порядком.

4. Ответственность за обеспечение безопасности персональных данных и надлежащего режима доступа к ИСПДн возлагается на председателя Комитета по делам молодежи Тверской области.

5. Помещения, в которых обрабатываются персональные данные, должны быть защищены от физического проникновения посторонних лиц. Доступ лиц, не причастных к непосредственной обработке персональных данных в эти помещения должен быть исключен.

6. В помещениях, где обрабатываются персональные данные, должны быть установлены сейфы для хранения съемных носителей информации и машинных документов (распечаток). Ключи от сейфов хранятся у ответственных лиц, назначаемых приказом председателя Комитета по делам молодежи Тверской области.

7. Системы обработки и хранения персональных данных должны быть расположены так, чтобы исключить возможность случайного или преднамеренного доступа к ним неуполномоченных лиц в процессе их обработки.

8. Пользователи ИСПДн обязаны:

пройти инструктаж о соблюдении требований к защите персональных данных;

строго следить за соблюдением режима разграничения доступа, незамедлительно информировать непосредственного руководителя и ответственного за организацию обработки персональных данных о всех случаях утечки или разрушения обрабатываемой в ИСПДн защищаемой информации;

перед началом обработки в ИСПДн персональных данных убедиться в отсутствии в помещении посторонних лиц.

9. Для осуществления контроля и поддержания надлежащего режима обработки персональных данных, руководитель подразделения Комитета по делам молодежи Тверской области, а также ответственный за организацию обработки персональных данных обязаны систематически информировать лиц, осуществляющих обработку защищаемой информации в ИСПДн о необходимости повышения их бдительности и персональной ответственности.

Ответственный за организацию
обработки персональных данных

_____
( инициалы, фамилия)

“____” _____ 20__ г.