



СОВЕТ НАРОДНЫХ ДЕПУТАТОВ ГОРОДА ВЛАДИМИРА

РАСПОРЯЖЕНИЕ

от 31.01.2013

№ 8-р

Об отдельных вопросах обработки и защиты персональных данных в аппарате Совета народных депутатов города Владимира

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

1. Утвердить:

- 1.1. «Правила работы с обезличенными персональными данными в аппарате Совета народных депутатов города Владимира» (приложение № 1);
- 1.2. «Перечень должностей служащих Совета народных депутатов города Владимира, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных» (приложение № 2); • 17.06.2021 17-р.
- 1.3. «Порядок доступа служащих Совета народных депутатов города Владимира в помещения, в которых ведётся обработка персональных данных» (приложение № 3);
- 1.4. «Перечень персональных данных, обрабатываемых в аппарате Совета народных депутатов города Владимира в связи с реализацией служебных (трудовых) отношений, а также для осуществления и выполнения возложенных законодательством Российской Федерации на Совет народных депутатов города Владимира функций, полномочий и обязанностей» (приложение № 4);
- 1.5. «Типовую форму согласия на обработку персональных данных служащих Совета народных депутатов города Владимира, иных субъектов персональных данных, а также типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные» (приложение № 5); • 17.06.2021 17-р.

- 1.6. «Правила обработки персональных данных в аппарате Совета народных депутатов города Владимира» (приложение № 6);
- 1.7. «Правила рассмотрения запросов субъектов персональных данных или их представителей в аппарате Совета народных депутатов города Владимира» (приложение № 7);
- 1.8. «Типовое обязательство служащего Совета народных депутатов города Владимира, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей» (приложение № 8);
- 1.9. «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Совета народных депутатов города Владимира» (приложение № 9); • 17.06.21 17-р
- 1.10. «Перечень должностей служащих Совета народных депутатов города Владимира, замещение которых предусматривает осуществление обработки персональных данных либо осуществления доступа к персональным данным» (приложение № 10). • 17.06.2021 17-р
- 1.11. «Список помещений Совета народных депутатов города Владимира, в которых обрабатываются персональные данные без использования средств автоматизации и с использованием автоматизированных средств, и доступ к ним» (приложение № 11) • 17.06.2021 17-р
- 1.12. «Перечень информационных систем персональных данных Совета народных депутатов города Владимира» (приложение № 12) • 17.06.21 17-р
- 1.13. «Должностную инструкцию лица, ответственного за организацию обработки персональных данных в Совете народных депутатов города Владимира» (приложение № 13)
- 1.14. «Политику Совета народных депутатов города Владимира в отношении обработки персональных данных» (приложение № 14)
- 1.15. «Акт классификации информационной системы персональных данных «Обращения граждан» Совета народных депутатов города Владимира» (приложение № 15) • 17.06.2021 17-р
- 1.16. «Акт классификации информационной системы персональных данных «База данных работники Совета народных депутатов (кадры)» (приложение № 16) • 17.06.2021 17-р
- 1.17. Акт классификации информационной системы персональных данных «База учёта труда и заработной платы» (приложение № 17) • 17.06.2021 17-р
- 2. Утвердить формы учётных журналов:
 - 2.1. «Журнал учета антивирусных проверок автоматизированных мест информационных систем персональных данных Совета народных депутатов города Владимира» (приложение № 18)
 - 2.2. «Журнал учета доступа к работе (учет «логинов») в информационных системах персональных данных Совета народных депутатов города Владимира» (приложение № 19)

2.3. «Журнал учета мероприятий по контролю за соблюдением режима защиты персональных данных в Совете народных депутатов города Владимира» (приложение № 20)

2.4. «Журнал учета съемных носителей персональных данных Совета народных депутатов города Владимира» (приложение № 21)

2.5. «Журнал учета обращений субъектов персональных данных в Совете народных депутатов города Владимира» (приложение № 22)

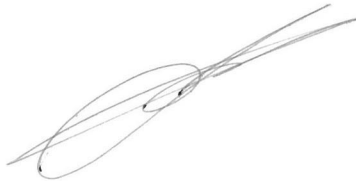
2.6. «Журнал учета проверок, проводимых контролирующими органами в Совете народных депутатов города Владимира» (приложение № 23)

2.7. «Журнал учета процедур резервного копирования в Совете народных депутатов города Владимира» (приложение № 24)

2.8. «Журнал учета средств защиты информации в Совете народных депутатов города Владимира» (приложение № 25)

3. Контроль за исполнением настоящего распоряжения возложить на руководителя аппарата Совета народных депутатов города Владимира (Захаренко А.В.).

Глава города



С.В. Сахаров

ПРАВИЛА работы с обезличенными персональными данными в аппарате Совета народных депутатов города Владимира

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящие Правила работы с обезличенными персональными данными в аппарате Совета народных депутатов города Владимира (далее – Совет) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- 1.2. Настоящие Правила определяют порядок работы с обезличенными данными в Совете.
- 1.3. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

- 2.1. Обезличивание персональных данных может быть проведено с целью ведения статистических или иных исследований, по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
- 2.2. При условии обязательного обезличивания персональных данных осуществляется обработка персональных данных в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
- 2.3. При обработке персональных данных используются следующие способы их обезличивания:
 - 2.3.1. уменьшение перечня обрабатываемых сведений;

- 2.3.3. обобщение;
- 2.3.4. понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
- 2.3.5. деление сведений на части и обработка в разных информационных системах.
- 2.4. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.
- 2.5. Для обезличивания персональных данных могут быть использованы иные способы, не запрещенные законодательством Российской Федерации.
- 2.6. Руководитель аппарата Совета принимает решение о необходимости обезличивания персональных данных и способе обезличивания, сотрудники отдела делопроизводства и кадров, обрабатывающие персональные данные, осуществляют непосредственное обезличивание выбранным способом.

3. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

- 3.1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.
- 3.2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
- 3.3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:
 - 3.3.1. парольной политики;
 - 3.3.2. антивирусной политики;
 - 3.3.3. правил работы со съемными носителями (если они используются);
 - 3.3.4. правил резервного копирования;
 - 3.3.5. правил доступа в помещения, где расположены элементы информационных систем;
- 3.4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
 - 3.4.1. правил хранения бумажных носителей;
 - 3.4.2. правил доступа к ним и в помещения, где они хранятся.

Перечень
должностей служащих Совета народных депутатов города Владимира,
ответственных за проведение мероприятий по обезличиванию обрабатываемых
персональных данных

- Руководитель аппарата Совета народных депутатов города Владимира;
- Заведующий отделом делопроизводства и кадров Совета народных депутатов города Владимира, заместитель руководителя аппарата;
- Консультант отдела делопроизводства и кадров Совета народных депутатов города Владимира;
- Консультант аппарата Совета народных депутатов города Владимира.

21.01.2013 № 8-Р

ПОРЯДОК доступа служащих Совета народных депутатов города Владимира в помещения, в которых ведется обработка персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящий Порядок устанавливает требования к доступу муниципальных служащих (работников) аппарата Совета народных депутатов города Владимира (далее – Совет) в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Совете, и обеспечения соблюдения требований законодательства о персональных данных.
- 1.2. Настоящий Порядок обязателен для применения и исполнения всеми муниципальными служащими (работниками) Совета.
- 1.3. Служебными помещениями, в которых ведется обработка персональных данных, являются кабинеты сотрудников Совета, назначенных на должности, включенные в перечень должностей в аппарате Совета, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (далее – служебные помещения).

2. ТРЕБОВАНИЯ К СЛУЖЕБНЫМ ПОМЕЩЕНИЯМ

- 2.1. В целях обеспечения соблюдения требований к ограничению доступа в служебные помещения Совета обеспечивается:
 - использование служебных помещений строго по назначению;
 - наличие на входах в служебные помещения дверей, оборудованных запорными устройствами;
 - содержание дверей служебных помещений в нерабочее время в закрытом на запорное устройство состоянии;
 - остекление окон в здании Совета и администрации города Владимира, содержание их в нерабочее время в закрытом состоянии;
 - наличие ключей от служебных помещений только у муниципальных служащих (работников) Совета, служебные (рабочие) места которых находятся в данном служебном помещении; нахождение иных лиц в служебном помещении возможно только в присутствии муниципальных служащих (работников) Совета, служебные (рабочие) места которых находятся в данном служебном помещении.
- 2.2. Доступ в служебные помещения муниципальных служащих (работников) Совета, служебные (рабочие) места которых находятся в данном

служебном помещении, допускается только для исполнения должностных обязанностей в соответствии с должностной инструкцией.

2.3. В отсутствие муниципальных служащих (работников) Совета, служебные (рабочие) места которых находятся в данном служебном помещении, в случае возникновения служебной необходимости право доступа в служебное помещение имеет руководитель аппарата Совета.

2.4. Муниципальным служащим (работникам) Совета запрещается передавать ключи от служебных помещений третьим лицам, если иное не установлено законодательством Российской Федерации или правовыми актами представителя нанимателя (работодателя).

3. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ТРЕБОВАНИЙ К ДОСТУПУ В СЛУЖЕБНЫЕ ПОМЕЩЕНИЯ

3.1. Муниципальные служащие (работники) Совета, обнаружившие попытку или факт проникновения посторонних лиц в служебное помещение, немедленно сообщают об этом вышестоящему руководителю, лицу, ответственному за организацию обработки персональных данных в аппарате Совета, и в органы внутренних дел Российской Федерации.

**Перечень персональных данных,
обрабатываемых в аппарате Совета народных депутатов города
Владимира в связи с реализацией служебных (трудовых)
отношений, а также для осуществления и выполнения возложенных
законодательством Российской Федерации на Совет народных
депутатов города Владимира функций, полномочий и обязанностей**

1. Настоящий перечень персональных данных, обрабатываемых в аппарате Совета народных депутатов города Владимира (далее - Совет) в связи с реализацией служебных (трудовых) отношений, а также для осуществления и выполнения возложенных законодательством Российской Федерации на Совет, полномочий и обязанностей, разработан в целях обеспечения выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов.
2. В связи с реализацией служебных (трудовых) отношений Совет обрабатывает следующие персональные данные:
 - фамилия, имя, отчество;
 - сведения об изменении фамилии, имени, отчества;
 - год, число и месяц рождения;
 - место рождения, домашний адрес (адрес регистрации, фактического проживания), телефоны, адрес электронной почты;
 - данные паспорта и (или) иного документа, удостоверяющего личность, сведения, содержащиеся в собственноручно заполненной и подписанной гражданином Российской Федерации при поступлении на муниципальную службу анкете;
 - сведения о гражданстве;
 - сведения о семейном положении, составе семьи и близких родственниках (родителях, супругах, детях, братьях, сестрах);
 - сведения об образовании, квалификации, наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);
 - сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке,

наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);

сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса организации, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения);

сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;

сведения о классном чине муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы;

сведения о прохождении квалификационных экзаменов, аттестации, конкурсов на замещение вакантных должностей муниципальной службы и на включение в кадровый резерв, сведения о включении (исключении) в кадровый резерв, резерв управленческих кадров, а также иные сведения, связанные с прохождением муниципальной службы;

сведения о наградах и званиях;

- сведения о заработной плате, денежном содержании (данные об окладе, надбавках, иных выплатах, налогах, в том числе об исполнении налоговых обязательств, номера счетов для расчета с работниками, и другие сведения);

сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии \ снятии на(с) учет(а) и другие сведения);

данные свидетельств о регистрации актов гражданского состояния, сведения о социальных льготах и о социальном статусе, реквизиты страхового свидетельства государственного пенсионного страхования, полиса обязательного медицинского страхования, сведения об идентификационном номере налогоплательщика, сведения, указанные в распоряжениях, иных документах, издаваемых Советом по личному составу;

сведения о состоянии здоровья, временной нетрудоспособности;

сведения об исполнении обязательств по договорам кредита и иным гражданско-правовым договорам, иные сведения, отражающие деловую репутацию;

сведения о наличии судимости, фактов уголовного преследования;

а также иные персональные данные, содержащиеся в:

решениях о поощрении сотрудника Совета, а также о наложении на него дисциплинарного взыскания;

документах о начале служебной проверки, ее результатах, об отстранении сотрудника Совета от замещаемой должности;

документах, связанных с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если

11

исполнение обязанностей по замещаемой должности связано с использованием таких сведений;

справках о доходах, имуществе и обязательствах имущественного характера;

медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению.

3. Для осуществления и выполнения возложенных законодательством Российской Федерации на Совет функций, полномочий и обязанностей Совет обрабатывает следующие персональные данные:

фамилия, имя, отчество;

год, число и месяц рождения, место рождения;

домашний адрес (адрес регистрации, фактического проживания), телефоны, адрес электронной почты;

данные паспорта и (или) иного документа, удостоверяющего личность, сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки;

сведения о трудовой деятельности;

сведения о серии, номере и дате выдачи страхового свидетельства государственного пенсионного страхования;

сведения об идентификационном номере налогоплательщика;

иные персональные данные, содержащиеся в:

письменном заявлении;

доверенности лица, уполномоченного на подачу заявления, договоре на представительство, документе, удостоверяющем права (полномочия) представителя физического или юридического лица - если с заявлением обращается представитель заявителя (заявителей);

документе, удостоверяющем личность заявителя (заявителей), являющегося физическим лицом, либо личность представителя физического или юридического лица;

документах, поданных для участия в конкурсе на замещение вакантной должности муниципальной службы или на включение в кадровый резерв;

свидетельстве о государственной регистрации физического лица в качестве индивидуального предпринимателя (для индивидуальных предпринимателей), или выписке из государственных реестров о индивидуальном предпринимателе;

иных документах, подлежащих предоставлению в связи с осуществлением и выполнением возложенных законодательством Российской Федерации на Совет функций, полномочий и обязанностей.

**Типовая форма согласия на обработку персональных данных служащих
Совета народных депутатов города Владимира, иных субъектов персональных
данных, а также типовая форма разъяснения субъекту персональных данных
юридических последствий отказа предоставить свои персональные данные**

Главе города Владимира
С.В. Сахарову

(ФИО)

зарегистрированного (ной) по адресу:

паспорт серия _____ № _____,

когда, кем выдан _____

ЗАЯВЛЕНИЕ

В соответствии с требованиями ст.9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», подтверждаю свое согласие на обработку Советом народных депутатов города Владимира (адрес: г.Владимир, ул. Горького, д.36) своих персональных данных с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, прохождении конкурсного отбора, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, оформления доверенностей, безналичных платежей на мой счет, и, в случае необходимости, проведения в отношении меня проверки достоверности представленных мной сведений соответствующими органами.

Согласие дано на обработку следующих персональных данных *(выбрать нужное и/или дополнить необходимыми сведениями)*:

- фамилия, имя, отчество;
- сведения об изменении фамилии, имени, отчества;
- год, число и месяц рождения;
- место рождения, домашний адрес (адрес регистрации, фактического проживания), телефоны, адрес электронной почты;
- данные паспорта и (или) иного документа, удостоверяющего личность, сведения, содержащиеся в собственноручно заполненной и подписанной гражданином Российской Федерации при поступлении на государственную гражданскую службу анкете;
- сведения о гражданстве;

- сведения о семейном положении, составе семьи и близких родственников (родителях, супругах, детях, братьях, сестрах);
- сведения об образовании, квалификации, наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);
- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса организации, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения);
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;
- сведения о классном чине муниципальной службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы;
- сведения о прохождении квалификационных экзаменов, аттестации, конкурсов на замещение вакантных должностей муниципальной службы и на включение в кадровый резерв, сведения о включении (исключении) в кадровый резерв;
- сведения о наградах и званиях;
- сведения о заработной плате, денежном содержании (данные об окладе, надбавках, иных выплатах, налогах, в том числе об исполнении налоговых обязательств, номера счетов для расчета с работниками, и другие сведения);
- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения);
- данные свидетельств о регистрации актов гражданского состояния, сведения о социальных льготах и о социальном статусе, реквизиты страхового свидетельства государственного пенсионного страхования, полиса обязательного медицинского страхования, сведения об идентификационном номере налогоплательщика, сведения, указанные в распоряжениях, иных документах, издаваемых Советом по личному составу;
- сведения о состоянии здоровья, временной нетрудоспособности;
- сведения об исполнении обязательств по договорам кредита и иным гражданско-правовым договорам, иные сведения, отражающие деловую репутацию;
- сведения о наличии судимости, фактов уголовного преследования;
- а также иные персональные данные, содержащиеся в:
 - решениях о поощрении сотрудника Совета, а также о наложении на него дисциплинарного взыскания;
 - документах о начале служебной проверки, ее результатах, об отстранении сотрудника Совета от замещаемой должности;

документах, связанных с оформлением допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по замещаемой должности связано с использованием таких сведений;

справках о доходах, имуществе и обязательствах имущественного характера;

медицинском заключении установленной формы об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению.

Предоставляю Совету право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, распространение (в том числе передачу в соответствии с требованиями законодательства Российской Федерации), обезличивание, блокирование, уничтожение. Даю согласие на получение Советом моих персональных данных у третьей стороны. Совет вправе обрабатывать мои персональные данные следующими способами: автоматизированная, неавтоматизированная и смешанная обработка с передачей по внутренней сети Совета, с передачей по сети Интернет.

Согласие действует в течение срока действия трудового договора и 75 лет после окончания срока его действия. Отзыв настоящего согласия осуществляется в письменной форме путем подачи мной соответствующего заявления.

Я подтверждаю, что ознакомлен(а) с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», своими правами и обязанностями в области защиты персональных данных.

Подпись

(расшифровка подписи)

« ____ » _____ 20__ г.

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

**Разъяснения
юридических последствий отказа предоставить свои персональные данные**

В соответствии с Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», определен перечень персональных данных, которые субъект персональных данных обязан предоставить Совету в связи с поступлением или прохождением муниципальной службы.

Без предоставления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности муниципальной службы.

В случае отзыва Вами ранее данного согласия на обработку персональных данных Совет на основании части 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» вправе продолжить их обработку в связи с тем, что обработка персональных данных необходима для исполнения трудового договора.

Мне, _____,
разъяснены юридические последствия отказа предоставить свои персональные данные Совету народных депутатов города Владимира.

(подпись) / _____
(фамилия, имя, отчество)

« _____ » _____ 20 ____ г.

ПРАВИЛА **обработки персональных данных в аппарате Совета народных** **депутатов города Владимира**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны на основании требований Трудового кодекса Российской Федерации, Федерального закона Российской Федерации от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и других нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой персональных данных, и устанавливают порядок обработки, распространения, и использования персональных данных в аппарате Совета народных депутатов города Владимира (далее - Совет) с использованием средств автоматизации, без них или смешанным способом.

1.2. Совет является оператором персональных данных работников аппарата Совета (лиц, замещающих муниципальные должности, муниципальных служащих и лиц, работающих в Совете по трудовому договору).

1.3. Обработка персональных данных работников аппарата Совета, необходимая для достижения целей, предусмотренных Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» и Трудовым Кодексом Российской Федерации, для осуществления и выполнения возложенных законодательством Российской Федерации на Совет функций, полномочий и обязанностей, производится без письменного согласия субъекта персональных данных.

1.4. Обработка персональных данных граждан, необходимая для достижения целей, предусмотренных Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», для осуществления и выполнения возложенных законодательством Российской Федерации на Совет функций, полномочий и обязанностей, производится без письменного согласия субъекта персональных данных.

1.5. Перечень персональных данных работников аппарата Совета , обрабатываемых Советом, а также перечень должностей сотрудников аппарата Совета, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утверждается Главой города Владимира.

1.6. Сотрудники аппарата Совета должны быть ознакомлены с настоящими Правилами под роспись.

2. УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Общим условием обработки персональных данных является наличие письменного согласия субъектов персональных данных на осуществление такой обработки, если обработка не подпадает в число предусмотренных законодательством исключений, когда такое согласие не требуется.

2.2. Если персональные данные были получены не от субъекта персональных данных, за исключением случаев, когда персональные данные были предоставлены Совету на основании действующего законодательства или если персональные данные являются общедоступными, Совет до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- полное наименование и адрес Совета;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных;
- источник получения персональных данных.

2.3. Сотрудники аппарата Совета, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.4. В случае если Совет на основании договора поручает обработку персональных данных третьему лицу, существенным условием такого договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

2.5. Совет при обработке персональных данных принимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

2.6. В качестве мер, направленных на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, Совет:

18

разрабатываются и утверждаются правовые акты, направленные на выполнение требований, установленных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами:

назначается ответственный за организацию обработки персональных данных;

применяются правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

проводятся проверки условий обработки персональных данных в Совете;

проводится ознакомление сотрудников аппарата Совета с положениями законодательства Российской Федерации о персональных данных;

организуется обучение сотрудников аппарата Совета по вопросам законодательства о персональных данных;

проводится сбор у сотрудников аппарата Совета, непосредственно осуществляющих обработку персональных данных, обязательств о неразглашении персональных данных и прекращении обработки персональных данных в случае прекращения с ним служебных (трудовых) отношений;

проводятся иные мероприятия, предусмотренные нормативными правовыми актами Российской Федерации.

3. СРОК ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Общий срок обработки персональных данных определяется периодом времени, в течение которого Совет осуществляет в отношении персональных данных предусмотренные законодательством Российской Федерации и обусловленные заявленными целями их обработки действия (операции), в том числе хранение персональных данных.

3.2. Течение срока обработки персональных данных начинается с момента их получения Советом и заканчивается:

по достижении заявленных целей обработки;

по факту утраты необходимости в достижении заранее заявленных целей обработки.

3.3. Совет осуществляет хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели их обработки.

4. УТОЧНЕНИЕ, БЛОКИРОВАНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Целью уточнения персональных данных, в том числе обновления и изменения, является обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых Советом.

4.2. Уточнение персональных данных осуществляется Советом по собственной инициативе, по требованию субъекта персональных данных или его представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случаях, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными.

4.3. Целью блокирования персональных данных является временное прекращение обработки персональных данных до момента устранения обстоятельств, послуживших основанием для блокирования персональных данных.

4.4. Блокирование персональных данных осуществляется Советом по требованию субъекта персональных данных или его представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними.

4.5. Уничтожение персональных данных осуществляется Советом:
по достижении цели обработки персональных данных;
в случае утраты необходимости в достижении целей обработки персональных данных;

в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных;

по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случае выявления фактов совершения Советом неправомерных действий с персональными данными, когда устранить соответствующие нарушения не представляется возможным.

4.6. При уничтожении материальных носителей персональных данных составляется акт об уничтожении носителей, содержащих персональные данные.

5. УСТРАНЕНИЕ НАРУШЕНИЙ ЗАКОНОДАТЕЛЬСТВА, ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ, ДОПУЩЕННЫЕ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В случае выявления в деятельности Совета каких-либо нарушений законодательства, допущенных при обработке персональных данных, Совет устраняет такие нарушения в порядке и сроки, установленные федеральными законами.

5.2. Сотрудники аппарата Совета, виновные в нарушении требований законодательства Российской Федерации и локальных актов Совета, регулирующих отношения в сфере обработки персональных данных и обеспечения их безопасности и конфиденциальности, несут уголовную, административную, гражданскую и дисциплинарную ответственность, предусмотренную законодательством Российской Федерации.

6. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ АППАРАТА СОВЕТА

6.1. Персональные данные сотрудников аппарата Совета включают в себя информацию о фамилии, имени, отчестве, паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья (если эти сведения относятся к вопросу о возможности выполнения сотрудником Совета трудовой (служебной) функции), о предыдущих местах их работы, о судимости, о доходах, имуществе и обязательствах имущественного характера муниципальных служащих Совета, а также иные сведения, предусмотренные действующими нормативными правовыми актами Российской Федерации.

6.2. Совет не вправе получать и обрабатывать персональные данные сотрудника Совета о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с реализацией трудовых (служебных) отношений, в соответствии со статьей 24 Конституции Российской Федерации Совет вправе получать и обрабатывать данные о частной жизни сотрудника только с его письменного согласия.

6.3. Целью обработки персональных данных сотрудников аппарата Совета является обеспечение соблюдения Конституции Российской Федерации, положений Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Трудового кодекса Российской Федерации, иных законов и нормативных правовых актов Российской Федерации, содействие сотрудникам в трудоустройстве, прохождении трудовой деятельности и муниципальной службы, обучении и продвижении по службе, должностном росте, обеспечение личной безопасности сотрудников и членов их семей, контроль количества и качества выполняемой работы, обеспечение сохранности принадлежащего ему имущества, учета результатов исполнения им должностных обязанностей и обеспечения сохранности имущества Совета.

6.4. Совет обрабатывает персональные данные сотрудников следующими способами:

- на бумажных носителях;
- в информационных системах персональных данных;
- смешанным способом;
- с передачей и без передачи по локальной сети Совета и по информационно-телекоммуникационной сети «Интернет».

6.5. Получение персональных данных сотрудника Совета осуществляется непосредственно у него самого.

6.6. Сотрудники при поступлении на работу (службу) в Совет предоставляют предусмотренную Трудовым кодексом Российской Федерации и Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» информацию.

6.7. Сотрудники Совета должны быть ознакомлены под роспись с документами Совета, устанавливающими порядок обработки персональных данных сотрудников, а также об их правах и обязанностях в этой области.

6.8. При передаче персональных данных сотрудника аппарата Совета должна соблюдаться следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом;

не сообщать персональные данные сотрудника в коммерческих целях;

предупреждать лиц, получивших персональные данные сотрудника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные сотрудника, обязаны соблюдать режим секретности (конфиденциальности). Данное требование не распространяется на обмен персональными данными сотрудников в порядке, установленном федеральными законами;

осуществлять передачу персональных данных сотрудников в пределах Совета в соответствии с настоящими правилами;

разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные сотрудника, которые необходимы для выполнения конкретной функции;

не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой (служебной) функции;

передавать персональные данные сотрудника представителям сотрудника в порядке, установленном Трудовым кодексом РФ и Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», и ограничивать эту информацию только теми персональными данными сотрудника, которые необходимы для выполнения указанными представителями их функции.

6.9. Сотрудники Совета вправе:

получать свободный бесплатный доступ к своим персональным данным, знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных федеральными законами;

требовать от Совета уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Совета персональных данных;

требовать от Совета извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Совета при обработке и защите его персональных данных;

осуществлять иные права, установленные Трудовым кодексом Российской Федерации, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30.05.2005 № 609, и иными нормативными правовыми актами Российской Федерации.

7. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ, НЕ ЯВЛЯЮЩИХСЯ СОТРУДНИКАМИ СОВЕТА

7.1. Целями обработки персональных данных физических лиц, не являющихся сотрудниками аппарата Совета (далее - граждане), являются реализация конституционного права граждан на обращение в государственные органы, оказание Советом государственных услуг и осуществление возложенных на Совет государственных функций.

7.2. Совет обрабатывает персональные данные граждан следующими способами:

- на бумажных носителях;
- в информационных системах персональных данных;
- смешанным способом;
- с передачей и без передачи по локальной сети Совета области и по информационно-телекоммуникационной сети Интернет.

7.3. Получение персональных данных осуществляется непосредственно от граждан, обратившихся в Совет.

7.4. Доступ к персональным данным граждан третьих лиц возможен исключительно в случаях, предусмотренных законодательством Российской Федерации. В противном случае такой доступ может быть предоставлен им исключительно на основании письменного согласия субъекта персональных данных.

7.5. Обработка, в том числе хранение персональных данных граждан, осуществляется Советом до достижения соответствующих целей обработки персональных данных.

Приложение
к Правилам обработки персональных данных
в аппарате Совета народных депутатов города Владимира

А К Т
об уничтожении носителей,
содержащих персональные данные

г. Владимир

«__» _____ 20__ г.

Настоящий Акт составлен в том, что комиссией в составе:

(должность)	-	(ФИО)
(должность)	-	(ФИО)
(должность)	-	(ФИО)

произведено уничтожение носителей, содержащих персональные данные сотрудников.

Уничтожение произведено путем _____.

Опись носителей:

№	Наименование	Количество листов

(ФИО)	(подпись)	«__» _____ 20__ г. (дата)
-------	-----------	------------------------------

(ФИО)	(подпись)	«__» _____ 20__ г. (дата)
-------	-----------	------------------------------

(ФИО)	(подпись)	«__» _____ 20__ г. (дата)
-------	-----------	------------------------------

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их
представителей в аппарате Совета народных депутатов города Владимира

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации» и Трудовым Кодексом Российской Федерации и определяют порядок обработки поступающих в аппарат Совета народных депутатов города Владимира (далее – Совет) обращений субъектов персональных данных.

1.2. Настоящие Правила распространяются на должностных лиц Совета, которые в рамках исполнения своих должностных обязанностей осуществляют прием и регистрацию обращений (запросов) субъектов персональных данных, ведут личный прием граждан, осуществляют рассмотрение обращений (запросов), подготовку и направление ответов на них.

1.3. В целях настоящих Правил используются следующие основные понятия:

- субъект персональных данных – физическое лицо, определенное или определяемое на основании любой относящейся к нему информации;
- представитель субъекта персональных данных – лицо, действующее от имени и в интересах субъекта персональных данных по его поручению на основании надлежащим образом оформленной доверенности или в силу закона.

2. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Советом;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Советом способы обработки персональных данных;
- полное наименование и место нахождения Совета, сведения о лицах (за исключением работников Совета), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании

договора с Советом или на основании федерального закона;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных настоящими Правилами;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Совета, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

2.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в соответствии с частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.3. Если субъект персональных данных считает, что Совет осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Совета в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

2.4. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. ПОРЯДОК РАБОТЫ С ОБРАЩЕНИЯМИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Прием и регистрация запросов (обращений) субъектов персональных данных осуществляется Советом в порядке, установленном для приема и регистрации входящей корреспонденции.

3.2. Запрос субъекта персональных данных или его представителя должен содержать:

номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе,

сведения, подтверждающие участие субъекта персональных данных в

отношениях с Советом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Советом,

подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.3. Субъект персональных данных вправе требовать от Совета уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.4. При получении запроса (обращения) субъекта персональных данных служащие Совета, ответственные за прием и регистрацию входящей корреспонденции, в тот же день осуществляют регистрацию такого запроса. Зарегистрированный запрос субъекта персональных данных направляется главе города Владимира для распределения исполнителям.

3.5. Совет в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Совет дает в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

3.7. Совет обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными,

Совет обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Совет обязан уничтожить такие персональные данные. Совет обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
служащего Совета народных депутатов города Владимира, непосредственно
осуществляющего обработку персональных данных,
в случае расторжения с ним трудового договора прекратить обработку
персональных данных, ставших известными ему в связи исполнением
должностных обязанностей

Я, _____,
проживающий по адресу: _____

паспорт серия _____ № _____, выданный (кем и
когда) _____
предупрежден(а) о том, что на период исполнения мною должностных
обязанностей _____,
(должность)

предусматривающих работу с персональными данными сотрудников Совета
народных депутатов города Владимира и иных субъектов персональных данных,
мне будет предоставлен доступ к указанной информации.

Настоящим добровольно принимаю на себя обязательства:

не передавать (в любом виде) и не разглашать третьим лицам и работникам
Совета народных депутатов города Владимира, не имеющим на это право в силу
выполняемых ими должностных обязанностей, информацию, содержащую
персональные данные сотрудников (граждан) (за исключением собственных
данных), которая мне доверена (будет доверена) или станет известной в связи с
исполнением должностных обязанностей;

в случае попытки третьих лиц или работников Совета народных депутатов
города Владимира, не имеющих на это право, получить от меня информацию,
содержащую персональные данные, немедленно сообщать об этом факте своему
непосредственному или (в случае отсутствия непосредственного) вышестоящему
руководителю;

не использовать информацию, содержащую персональные данные с целью
получения выгоды;

выполнять требования законодательства Российской Федерации,
регламентирующие вопросы защиты интересов субъектов персональных данных,
порядок обработки и защиты персональных данных;

после прекращения моих прав на допуск к информации, содержащей
персональные данные (переход на должность, не предусматривающую доступ к

персональным данным, прекращение трудового договора, изменение должностных обязанностей и др.), не обрабатывать, не разглашать и не передавать третьим лицам и неуполномоченным на это работникам Совета народных депутатов города Владимира, известную мне информацию, содержащую персональные данные, а также передать руководителю структурного подразделения (своему руководителю) или иному сотруднику по указанию руководителя структурного подразделения (своего руководителя) все носители, содержащие персональные данные, которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей в Совете народных депутатов города Владимира;

об утрате или недостатке документов или иных носителей, содержащих персональные данные, ключей от хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки сведений немедленно сообщить своему руководителю.

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

_____ / _____

«__» _____ Г.

**ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ
СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ,
УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ «О
ПЕРСОНАЛЬНЫХ ДАННЫХ», ПРИНЯТЫМИ В СООТВЕТСТВИИ С
НИМ НОРМАТИВНЫМИ ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ
АКТАМИ СОВЕТА НАРОДНЫХ ДЕПУТАТОВ ГОРОДА ВЛАДИМИРА**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в аппарате Совета народных депутатов города Владимира (далее – Совет) разработаны в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», принятых в соответствии с ним нормативных правовых актов Российской Федерации и распространяются на муниципальных служащих аппарата Совета (далее - муниципальные служащие) и лиц, замещающих в аппарате Совета должности, не являющиеся должностями муниципальной службы (далее - иные работники Совета).

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным:
Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе»;
Трудовым кодексом Российской Федерации;
постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
постановлением Правительства РФ от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
иными нормативными правовыми актами, регламентирующими порядок обработки персональных данных.

2. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

- 2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Совете проводятся периодические проверки условий обработки персональных данных.
- 2.2. Проверки условий обработки персональных данных проводятся комиссией, состав которой утверждается Главой города Владимира (далее - комиссия).
- 2.3. Основанием для проведения проверки является поручение Главы города Владимира.
- 2.4. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса, осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных, изучения документов, а также с использованием иных, не противоречащих федеральным законам и другим нормативным актам Российской Федерации, способов исследования фактических обстоятельств в течение одного месяца со дня возникновения основания для проведения проверки.
- 2.5. По результатам проверки большинством голосов членов комиссии принимается решение. В течение пяти рабочих дней после завершения проверки составляется Акт проведения внутренней проверки (далее - Акт) по форме согласно приложению. С Актом должны быть ознакомлены сотрудники, участвующие в процессе обработки персональных данных, в отношении которых проводилась проверка.
- 2.6. При выявлении в ходе проверки нарушений в Акте делается запись о мероприятиях по устранению нарушений и сроках исполнения. Срок устранения нарушений устанавливается комиссией и не может быть более одного месяца со дня составления Акта.
- 2.7. Акты проведения внутренних проверок хранятся у председателя комиссии в течение трех лет с даты проведения проверки, после чего подлежат уничтожению.
- 2.8. Информация о результатах проверки и мерах, необходимых для устранения нарушений, направляется Главе города Владимира в течение двух рабочих дней после составления Акта.

Приложение 1
к «Правилам осуществления внутреннего контроля
соответствия обработки персональных данных требованиям
к защите персональных данных в Совете народных депутатов города Владимира»

**Акт
проведения внутренней проверки условий обработки персональных
данных в аппарате Совета народных депутатов города Владимира**

___ ” _____ г. _____ г. _____

На основании пункта 4 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», руководствуясь Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Совете народных депутатов _____ города _____ Владимира, утвержденными _____, в период с _____ по _____

комиссией для проведения проверок условий обработки персональных данных в аппарате Совета народных депутатов города Владимира в составе:
Председатель комиссии (должностное лицо):

(Ф.И.О., должность)

Члены комиссии:

(Ф.И.О., должность)

(Ф.И.О., должность)

(Ф.И.О., должность)

проведена внутренняя проверка условий обработки персональных данных в аппарате администрации Владимирской области.

В ходе проверки установлено:

4

Выявленные нарушения:

_____.

Меры по устранению нарушений:

_____.

Срок устранения нарушений: _____.

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:

Должность _____ И.О. Фамилия

Должность _____ И.О. Фамилия

Должность _____ И.О.
Фамилия

**Перечень
должностей в Совете народных депутатов города Владимира, замещение
которых предусматривает осуществление обработки персональных
данных либо осуществление доступа
к персональным данным**

1. Глава города Владимира;
2. Заместитель главы города Владимира;
3. Председатель комитета
4. Руководитель аппарата Совета народных депутатов города Владимира;
5. Заведующий отделом
6. Консультант
7. Главный специалист
8. Ведущий специалист
9. Инспектор по контролю за исполнением поручений главы города

СПИСОК ПОМЕЩЕНИЙ

Совета народных депутатов города Владимира, в которых обрабатываются персональные данные без использования средств автоматизации и с использованием автоматизированных средств, и доступ к ним

1. СПИСОК ПОМЕЩЕНИЙ, В КОТОРЫХ ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1.1. г.Владимир, ул.Горького, д.36

- кабинет № 308
- кабинет № 309
- кабинет № 310
- кабинет № 408
- кабинет № 411
- кабинет № 416
- кабинет № 417
- кабинет № 501
- кабинет № 502
- кабинет № 503
- кабинет № 504
- кабинет № 506
- кабинет № 507
- кабинет № 508
- кабинет № 509
- кабинет № 509а
- кабинет № 510
- кабинет № 511
- кабинет № 512
- кабинет № 513
- кабинет № 515
- кабинет № 609

1.2. г.Владимир, ул.Горького, д.40

- кабинет № 202
- кабинет № 203

2. СПИСОК СОТРУДНИКОВ, ИМЕЮЩИХ ДОСТУП В ПОМЕЩЕНИЯ

№ п/п	ФИО	Должность	Подразделение	№ кабинета
1.		Глава города		609
2.		Заместитель главы города		512
3.		Председатель комитета (депутат на постоянной		507

		основе)		
4.		Председатель комитета		509
5.		Руководитель аппарата	Аппарат Совета	511
6.		Заведующий отделом	Отдел делопроизводства и кадров	308
7.		Консультант		309
8.		Главный специалист, заведующий канцелярией		310
9.		Ведущий специалист		513
10.		Консультант	Аппарат Совета	309
11.		Консультант		309
12.		Заведующий отделом	Отдел по работе со СМИ	408
13.		Консультант		408
14.		Заведующий отделом	Отдел бухгалтерского учёта и отчётности	510
15.		Главный специалист		510
16.		Заведующий отделом	Юридический отдел	504
17.		Консультант		502
18.		Консультант		502
19.		Заведующий отделом	Отдел финансового контроля	202
20.		Консультант		203
21.		Главный специалист		203
22.		Главный специалист		203
23.		Заведующий отделом	Отдел международных и региональных связей	416
24.		Консультант		515
25.		Ведущий специалист		417
26.		Ведущий специалист		417
27.		Консультант	Аппарат Совета	411
28.		Консультант		411
29.		Консультант		501
30.		Консультант		501
31.		Консультант		503
32.		Консультант		506
33.		Консультант		508
34.		Инспектор по контролю за исполнением поручений главы города		508
32.		Главный специалист		509a
33.		Консультант		515
34.		Консультант	515	

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ СОВЕТА НАРОДНЫХ ДЕПУТАТОВ Г. ВЛАДИМИРА

База данных	Цель обработки	Средства обработки	Категории субъектов персональных данных	Срок хранения	Порядок уничтожения	Ответственные за ПД – администраторы, пользователи	Помещения, в которых обрабатываются ПД
ИСПДн «Обращения граждан»	сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных	Автоматизированные, Средства Microsoft Office	граждане, обращающиеся в Совет народных депутатов: ФИО, дата рождения, адрес, контактный телефон, адрес электронной почты	5 лет	Бумажные носители уничтожаются путем сожжения, съемные НЖМД и USB-носители уничтожаются форматированием или физическим повреждением, дискеты и диски – простым физическим повреждением. После уничтожения НПД составляется акт уничтожения		
ИСПДн «База данных работники Совета народных депутатов» (кадры)	сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание,	Автоматизированные, Средства Microsoft Office	физические лица, состоящие в трудовых отношениях с Советом народных депутатов (сотрудники) ФИО Паспортные данные	75 лет	Бумажные носители уничтожаются путем сожжения, съемные НЖМД и USB-носители уничтожаются форматированием или физическим		

	блокирование, уничтожение персональных данных		<p>Дата рождения Адрес проживания Отпуска Премии Перевод на другую должность Имущественное положение Характеристики Аттестация Образование Повышение квалификации ИНН Документы воинского учёта Полис обязательного медицинского страхования</p>	повреждением, дискеты и диски – простым физическим повреждением. После уничтожения НПД составляется акт уничтожения	
ИСПДн «База учета труда и заработной платы»		Автоматизированные, АС «Парус»	<p>ФИО Паспортные данные Дата рождения Адрес проживания Зарплата Номер счета Должность Место работы СНИЛС Состав семьи</p>	уമാжные носители уничтожаются путем сожжения, съемные НЖМД и USB-носители уничтожаются форматированием или физическим повреждением, дискеты и диски – простым физическим повреждением. После уничтожения НПД составляется акт уничтожения	

**ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ЛИЦА, ОТВЕТСТВЕННОГО ЗА
ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОВЕТЕ
НАРОДНЫХ ДЕПУТАТОВ ГОРОДА ВЛАДИМИРА**

1. Ответственный за организацию обработки персональных данных в Совете народных депутатов города Владимира (далее - Ответственный за обработку персональных данных в Совете) назначается главой города из числа муниципальных служащих Совета народных депутатов города Владимира.

2. Ответственный за обработку персональных данных Совета в своей работе руководствуется законодательством Российской Федерации в области персональных данных и настоящим Распоряжением.

3. Ответственный за обработку персональных данных Совета обязан:

3.1. организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных, обрабатываемых в Совете от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

3.2. осуществлять внутренний контроль за соблюдением муниципальными служащими Совета требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

3.3. доводить до сведения муниципальных служащих Совета положения законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.4. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов в Совете;

3.5. в случае нарушения в Совете требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

4. Ответственный за обработку персональных данных вправе:

4.1. иметь доступ к информации, касающейся обработки персональных данных в Совете и включающей:

4.1.1. цели обработки персональных данных;

4.1.2. категории обрабатываемых персональных данных;

4.1.3. категории субъектов, персональные данные которых обрабатываются;

4.1.4. правовые основания обработки персональных данных;

4.1.5. перечень действий с персональными данными, общее описание используемых в Совете способов обработки персональных данных;

4.1.6. описание мер, предусмотренных статьями 18.1 и 19 Федерального закона "О персональных данных", в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

4.1.7. дату начала обработки персональных данных;

4.1.8. срок или условия прекращения обработки персональных данных;

4.1.9. сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

4.1.10. сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации;

4.2. привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в Совете, иных муниципальных служащих Совета.

5. Ответственный за обработку персональных данных в Совете несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в Совете в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение № 14
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

ПОЛИТИКА
Совета народных депутатов города Владимира
в отношении обработки персональных данных

г. Владимир
2013 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Термины и определения

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

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

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в

информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.2. Назначение и правовая основа документа

Политика Совета народных депутатов города Владимира (далее – Совет) определяет систему взглядов на проблему обеспечения безопасности персональных данных и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Совет в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности персональных данных.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский, Уголовный и Трудовой кодексы Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности персональных данных Совета позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

2. ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами системы безопасности персональных данных в Совете являются:

- информационные ресурсы с ограниченным доступом, содержащие персональные данные;
- процессы обработки персональных данных в информационных системах персональных данных Совета, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки персональных данных.

3. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности персональных данных Совета являются:

- Совет, как собственник информационных ресурсов;
- руководство и сотрудники Совета, в соответствии с возложенными на них функциями;
- граждане, обращающиеся в Совет.

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им персональным данным (их доступности);
- достоверности (полноты, точности, адекватности, целостности) персональных данных;
- конфиденциальности (сохранения в тайне) персональных данных;
- защиты от навязывания им ложных (недостоверных, искаженных) персональных данных;
- разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с персональными данными;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи персональных данных;
- защиты персональных данных от незаконного распространения.

3.2. Цели защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Совета от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на персональные данные, их носители, процессы обработки и передачи.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств персональных данных:

- доступности персональных данных для легальных пользователей (устойчивого функционирования информационных систем Совета, при котором пользователи имеют возможность получения необходимых персональных данных и результатов решения задач за приемлемое для них время);

- целостности и аутентичности (подтверждение авторства) персональных данных, хранимых и обрабатываемых в информационных системах Совета и передаваемой по каналам связи;

- конфиденциальности - сохранения в тайне определенной части персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности персональных данных обеспечивается соответствующими множеству значимых угроз методами и средствами.

3.3. Основные задачи системы обеспечения безопасности персональных данных

Для достижения основной цели защиты и обеспечения указанных свойств персональных данных система обеспечения информационной безопасности Совета должна обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Совета;

- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление

негативного влияния и ликвидация последствий нарушения безопасности информации;

- защиту от вмешательства в процесс функционирования информационных систем Совета посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Совета (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;

- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых в информационных системах Совета программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.4. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационных систем Совета (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Совета по вопросам обеспечения безопасности информации;

- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
- наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Совета;
- четким знанием и строгим соблюдением всеми пользователями информационных систем Совета требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Совета;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Совета;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- эффективным контролем над соблюдением пользователями информационных ресурсов Совета требований по обеспечению безопасности информации;
- юридической защитой интересов Совета при взаимодействии с внешними организациями (связанном с обменом персональными данными) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Построение системы обеспечения безопасности персональных данных Совета и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность (экономическая целесообразность);
- персональная ответственность;
- минимизация полномочий;
- исключение конфликта интересов;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

4.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных Совета в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не

должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях.

Все пользователи информационных систем Совета должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

4.2. Системность

Системный подход к построению системы защиты информации в Совете предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Совета, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

4.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.4. Непрерывность защиты

Обеспечение безопасности персональных данных - процесс, осуществляемый руководством Совета, администраторами безопасности информационных систем и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств

защиты, сколько процесс, который должен постоянно идти на всех уровнях внутри Совета и каждый сотрудник Совета должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Совета.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

4.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

4.6. Преимущество и совершенствование

Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преимущественности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Совета и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.7. Разумная достаточность (экономическая целесообразность)

Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Совета. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока персональные данные находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

4.8. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.9. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным

должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.10. Исключение конфликта интересов (разделение функций)

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находиться под строгим независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования персональными данными и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Совета. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение правонарушений. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

4.11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Совета. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности администраторов безопасности информационных систем персональных данных.

Важным элементом эффективной системы обеспечения безопасности персональных данных в Совете является высокая культура работы с информацией. Руководство Совета несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей

персоналу на всех уровнях важность обеспечения информационной безопасности Совета. Все сотрудники Совета должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

4.12. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Советом своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры Совета;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

4.13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.14. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со

знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

4.15. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

4.16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты персональных данных специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Совета (администраторами безопасности информационных систем персональных данных).

4.17. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных, на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения

средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные сотрудниками Совета должны немедленно доводиться до руководителя аппарата Совета и оперативно устраняться. Вопросы, которые кажутся незначительными, когда отдельные процессы рассматриваются изолированно, при рассмотрении их наряду с другими аспектами могут указать на отрицательные тенденции, грозящие перерасти в крупные недостатки, если они не будут своевременно устранены.

5. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

5.1. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационных систем Совета подразделяются на:

- правовые (законодательные);
- морально-этические;
- технологические;
- организационные (административные);
- физические;
- технические (аппаратурные и программные).

5.1.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с персональными

данными, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационных систем Совета.

5.1.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или Совета в целом. Морально-этические нормы бывают как неписанные, так и писанные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

5.1.3. Технологические меры защиты

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

5.1.4. Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки персональных данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить

возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5.2. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности персональных данных (отражающую подходы к защите персональных данных) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

С практической точки зрения политику в области обеспечения безопасности персональных данных в Совете целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Совета в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности персональных данных, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности персональных данных и детализирует (регламентирует) эти правила:

- каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных;
- кто имеет права доступа к персональным данным, кто и при каких условиях может читать и модифицировать персональные данные и т.д.

Политика нижнего уровня должна:

- предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;
- определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к персональным данным;

– выбирать программно-технические (аппаратные) средства противодействия НСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

5.3. Регламентация доступа в помещения

Компоненты информационных систем Совета должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Во время обработки персональных данных в таких помещениях должен присутствовать только персонал, допущенный к работе с персональными данными. Запрещается прием посетителей в помещениях, когда осуществляется обработка персональных данных.

По окончании рабочего дня, помещения, в которых размещаются компоненты информационных систем Совета, должны запираются на ключ.

В случае оснащения помещений средствами охранной сигнализации, а также автоматизированной системой приема и регистрации сигналов от этих средств, прием-сдача таких помещений под охрану осуществляется на основании специально разрабатываемой инструкции.

5.4. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы (матрицы) доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Совета и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком.

Уровень полномочий каждого пользователя определяется индивидуально, соблюдая следующие требования:

- каждый сотрудник пользуется только предписанными ему правами по отношению к персональным данным, с которыми ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационным ресурсам, в обязательном порядке, должно согласовываться с администратором безопасности информационных систем персональных данных.

Все сотрудники Совета и обслуживающий персонал должны нести персональную ответственность за нарушения установленного порядка обработки персональных данных, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый сотрудник (при приеме на работу) должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению персональных данных Совета.

Обработка персональных данных в компонентах информационных систем Совета должна производиться в соответствии с утвержденными технологическими инструкциями.

5.5. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест сотрудников Совета,

с которых возможен доступ к ресурсам информационных систем, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационных систем и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.6. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения персональных данных, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.7. Подбор и подготовка персонала, обучение пользователей

Пользователи информационных систем Совета, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки персональных данных в Совете.

Обеспечение безопасности персональных данных возможно только после выработки у пользователей определенной культуры работы, т.е. норм, обязательных для исполнения всеми, кто работает с информационными ресурсами Совета. К таким нормам можно отнести запрещение любых умышленных или неумышленных действий, которые нарушают нормальную работу компонентов информационных систем Совета, вызывают дополнительные затраты ресурсов, нарушают целостность хранимой и обрабатываемой информации, нарушают интересы законных пользователей, владельцев или собственников.

Все пользователи информационных систем Совета должны быть ознакомлены с организационно - распорядительными документами по обеспечению безопасности персональных данных Совета, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению

безопасности персональных данных. Доведение требований указанных документов до лиц, допущенных к обработке защищаемых персональных данных, должно осуществляться под роспись.

5.8. Ответственность за нарушения установленного порядка пользования ресурсами информационных систем Совета

Мера ответственности персонала за действия, совершенные в нарушение установленных правил обеспечения безопасной работы с персональными данными, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Совета.

Для реализации принципа персональной ответственности пользователей за свои действия необходимы:

- индивидуальная идентификация пользователей и инициированных ими процессов, т.е. установление за ними идентификатора (login, Username), на базе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- проверка подлинности пользователей (аутентификация) на основе паролей;
- реакция на попытки несанкционированного доступа (сигнализация, блокировка и т.д.).

5.9. Средства обеспечения безопасности персональных данных

Для обеспечения информационной безопасности Совета используются следующие средства защиты:

- физические средства;
- технические средства;
- средства идентификации и аутентификации пользователей;
- средства разграничения доступа;
- средства обеспечения и контроля целостности;
- средства оперативного контроля и регистрации событий безопасности.

Средства защиты должны применяться ко всем ресурсам информационных систем Совета, независимо от их вида и формы представления информации в них.

5.9.1. Физические средства защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым персональным данным, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для обеспечения физической безопасности компонентов информационных систем Совета необходимо осуществлять ряд организационных и технических мероприятий, включающих: проверку оборудования, предназначенного для обработки персональных данных, на:

- наличие специально внедренных закладных устройств;
- введение дополнительных ограничений по доступу в помещения, предназначенные для хранения и обработки персональных данных;
- оборудование систем информатизации устройствами защиты от сбоя электропитания и помех в линиях связи.

5.9.2. Технические средства защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

- средства разграничения доступа к данным;

- средства регистрации доступа к компонентам информационных систем и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств (Advantor, Touch Memory, Smart Card и т.п.);
- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нем.

5.9.3. Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами информационных систем Совета посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

- путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);
- путем проверки знания ими паролей;

— путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.9.4. Средства разграничения доступа

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к компонентам информационной среды Совета и элементам системы защиты персональных данных (физический доступ);
- к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.);
- к операционной системе, системным программам и программам защиты.

5.9.5. Средства обеспечения и контроля целостности

Средства обеспечения целостности включают в свой состав средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

Средства контроля целостности информационных ресурсов системы предназначены для своевременного обнаружения модификации или искажения ресурсов системы. Они позволяют обеспечить правильность функционирования системы защиты и целостность хранимой и обрабатываемой информации.

Контроль целостности информации и средств защиты, с целью обеспечения неизменности информационной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной модификации персональных данных должен обеспечиваться:

- средствами разграничения доступа (в помещения, к документам, к носителям информации, к серверам, логическим устройствам и т.п.);
- средствами электронной подписи;
- средствами подсчета контрольных сумм (для используемого программного обеспечения).

5.9.6. Средства оперативного контроля и регистрации событий безопасности

Средства объективного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, их характер, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации. Средства контроля и регистрации должны предоставлять возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов);
- получения твердой копии (печати) журнала регистрации событий безопасности;
- упорядочения журналов, а также установления ограничений на срок их хранения;
- оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в журнале должна фиксироваться следующая информация:

- дата и время события;
- идентификатор субъекта, осуществляющего регистрируемое действие;
- действие (тип доступа).

5.10. Контроль эффективности системы защиты

Контроль эффективности защиты персональных данных осуществляется с целью своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Приложение № 15
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

АКТ КЛАССИФИКАЦИИ
информационной системы персональных данных
«Обращения граждан»
Совета народных депутатов города Владимира

г. Владимир
2013 г.

Комиссия, назначенная распоряжением главы города Владимира № ___ от ___. ___. 2013, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями совместного приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» определила:

- 1. Категория персональных данных, обрабатываемых в информационной системе (X_{пд}) – **2**
- 2. Объём обрабатываемых персональных данных (X_{пдн}) – **2**
- 3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относится к: **типовой**
- 4. Структура информационной системы: **локальная**
- 5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
- 6. Режим обработки персональных данных в информационной системе: **многопользовательский**
- 7. Разграничение прав доступа пользователей: **без разграничения**
- 8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**

Исходя из анализа исходных данных ИСПДн, на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается **2 класс**.

Председатель комиссии: А.В. Захаренко

Члены комиссии:

- В.Н. Петров
- М.Ю. Черкасов
- С.Д. Шутов
- Н.В. Путова
- И.В. Гречина

71

Приложение № 16
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

АКТ КЛАССИФИКАЦИИ
информационной системы персональных данных «База
данных работники Совета народных депутатов»
(кадры)

г. Владимир
2013 г.

Комиссия, назначенная распоряжением главы города Владимира № ___ от ___. ___. 2013, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями совместного приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» определила:

1. Категория персональных данных, обрабатываемых в информационной системе ($X_{пд}$) – **2**
2. Объём обрабатываемых персональных данных ($X_{пдн}$) – **3**
3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относится к: **типовой**
4. Структура информационной системы: **локальная**
5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
6. Режим обработки персональных данных в информационной системе: **однопользовательский**
7. Разграничение прав доступа пользователей: **без разграничения**
8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**

Исходя из анализа исходных данных ИСПДн, на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается **3 класс**.

Председатель комиссии:

А.В. Захаренко

Члены комиссии:

В.Н. Петров

М.Ю. Черкасов

С.Д. Шутов

Н.В. Путова

И.В. Гречина

Приложение № 17
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

АКТ КЛАССИФИКАЦИИ
информационной системы персональных данных «База
учёта труда и заработной платы»

г. Владимир
2013 г.

Комиссия, назначенная распоряжением главы города Владимира № ___ от ___. ___. 2013, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями совместного приказа ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» определила:

- 1. Категория персональных данных, обрабатываемых в информационной системе (X_{пд}) – **3**
- 2. Объём обрабатываемых персональных данных (X_{пдн}) – **3**
- 3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относится к: **типовой**
- 4. Структура информационной системы: **локальная**
- 5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
- 6. Режим обработки персональных данных в информационной системе: **однопользовательский**
- 7. Разграничение прав доступа пользователей: **без разграничения**
- 8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**

Исходя из анализа исходных данных ИСПДн, на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается **3 класс**.

Председатель комиссии: А.В. Захаренко

Члены комиссии:

- В.Н. Петров
- М.Ю. Черкасов
- С.Д. Шутов
- Н.В. Путова
- И.В. Гречина

ЖУРНАЛ

**учета антивирусных проверок автоматизированных мест информационных систем персональных
данных Совета народных депутатов города Владимира**

Срок хранения:

Начат «__» _____ 2013г.

Окончен «__» _____ 201г.

На _____ листах

Владимир, 2013г.

ЖУРНАЛ

**учета доступа к работе (учет «логинов») в информационных системах персональных данных Совета
народных депутатов города Владимира**

Срок хранения:

Начат «__» _____ 2013г.

Окончен «__» _____ 201_ г.

На _____ листах

Владимир, 2013г.

ЖУРНАЛ

учета мероприятий по контролю за соблюдением режима защиты персональных данных
в Совете народных депутатов города Владимира

Срок хранения:

Начат «_» _____ 2013г.

Окончен «_» _____ 201_г.

На _____ листах

Владимир, 2013г.

ЖУРНАЛ

учета съемных носителей персональных данных Совет народных депутатов города Владимира

Срок хранения:

Начат «__» _____ 2013г.

Окончен «__» _____ 201_г.

На _____ листах

Владимир, 2013г.

81

ЖУРНАЛ

учета обращений субъектов персональных данных в Совете народных депутатов города Владимира

Срок хранения:

Начат «__» ____ 2013г.

Окончен «__» ____ 201_г.

На ____ листах

Владимир, 2013г.

ЖУРНАЛ

учета проверок, проводимых контролирующими органами в Совете народных депутатов города Владимира

Срок хранения:

Начат «01» сентября 2013г.

Окончен «__» _____ 201_г.

На _____ листах

Владимир, 2013г.

Сведения о проводимых проверках

1	Дата начала и окончания проверки	
2	Общее время проведения проверки (для субъектов малого и среднего предпринимательства, в часах)	
3	Наименование органа государственного контроля (надзора), наименование органа муниципального контроля	
4	Дата и номер распоряжения или приказа о проведении проверки	
5	Цель, задачи и предмет проверки	
6	Вид проверки (плановая или внеплановая): для плановой проверки – ссылка на ежегодный план проведения проверок; для внеплановой проверки в отношении субъектов малого или среднего предпринимательства – дата и номер решения прокурора о согласовании проведения проверки	
7	Дата и номер акта, составленного по результатам проверки, дата его вручения представителю юридического лица, индивидуальному предпринимателю	
8	Выявленные нарушения обязательных требований (указываются содержание выявленного нарушения со ссылкой на положение нормативного правового акта, которым установлено нарушение требование, допустившее его лицо)	
9	Дата, номер и содержание выданного предписания, протокола об административных правонарушениях	
10	Фамилия, имя, отчество (в случае, если имеется), должность должностного лица (должностных лиц), проводящего(их) проверку	
11	Фамилия, имя, отчество (в случае, если имеется), должности экспертов, представителей экспертных организаций, привлеченных к проведению проверки	
12	Подпись должностного лица (лиц), проводившего проверку	

ЖУРНАЛ

учета процедур резервного копирования в Совете народных депутатов г. Владимира

Срок хранения:

Начат «__» _____ 2013 г.

Окончен «__» _____ 201_ г.

На _____ листах

Владимир, 2013 г.

87

ЖУРНАЛ

учета средств защиты информации в Совете народных депутатов города Владимира

Срок хранения:

Начат «__» _____ 2013 г.

Окончен «__» _____ 201__ г.

На _____ листах

Владимир, 2013 г.



ПРЕДСЕДАТЕЛЬ СОВЕТА НАРОДНЫХ ДЕПУТАТОВ ГОРОДА ВЛАДИМИРА

РАСПОРЯЖЕНИЕ

от 17.06.2021

№ 17-р

О внесении изменений в распоряжение главы города Владимира от 31.01.2013 №8-р «Об отдельных вопросах обработки и защиты персональных данных в аппарате Совета народных депутатов города Владимира»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», пунктом 2 ст.27 Устава муниципального образования город Владимира:

1. Внести следующие изменения в распоряжение главы города от 31.01.2013 № 8-р «Об отдельных вопросах обработки и защиты персональных данных в аппарате Совета народных депутатов города Владимира»:

1.1. Приложение № 2 «Перечень должностей муниципальных служащих Совета народных депутатов города Владимира, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных» изложить в редакции согласно приложению № 1 к настоящему распоряжению;

1.2. Приложение № 5 «Типовая форма согласия на обработку персональных данных муниципальных служащих Совета народных депутатов города Владимира, иных субъектов персональных данных, а также Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные» изложить в редакции согласно приложению № 2 к настоящему распоряжению;

1.3. Приложение № 9 «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» принятыми в соответствии с ним нормативными правовыми актами Совета народных депутатов города Владимира» изложить в редакции согласно приложению № 3 к настоящему распоряжению;

1.4. Приложение № 10 «Перечень должностей в Совете народных депутатов города Владимира, замещение, которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным» изложить в редакции согласно приложению №4 к настоящему распоряжению;

1.5. Приложение №11 «Список помещений Совета народных депутатов города Владимира, в которых обрабатываются персональные данные без использования средств автоматизации и с использованием автоматизированных средств, и доступ к ним» изложить в редакции согласно приложению № 5 к настоящему распоряжению;

1.6. Приложение № 12 «Перечень информационных систем персональных данных Совета народных депутатов города Владимира» изложить в редакции согласно приложению № 6 к настоящему распоряжению;

1.7. Приложение № 15 «Акт классификации информационной системы персональных данных «Обращения граждан» Совета народных депутатов города Владимира» изложить в редакции согласно приложению № 7 к настоящему распоряжению;

1.8. Приложение № 16 «Акт классификации информационной системы персональных данных «База учета труда и заработной платы» Совета народных депутатов города Владимира» изложить в редакции согласно приложению № 8 к настоящему распоряжению;

1.9. Приложение № 17 «Акт классификации информационной системы персональных данных «База данных работников Совета народных депутатов» (кадры) Совета народных депутатов города Владимира», изложить в редакции согласно приложению № 9 к настоящему распоряжению.

2. Контроль за исполнением настоящего распоряжения возложить на заместителя председателя Совета народных депутатов города Владимира Пышнину Л.В.

Председатель Совета



Н.Ю. Толбухин

ЗАВИЗИРОВАНО

Руководитель аппарата Совета

« 17 » июня 2021 г.

И.А. Момот

Заведующий юридическим отделом

« 17 » июня 2021 г.

В.Н. Петров

Приложение № 1 к распоряжению
председателя Совета народных депутатов
города Владимира
от 17.06.2021 № 17-р

Приложение № 2
к распоряжению главы города
Владимира
от 31.01.2013 № 8-р

Перечень
должностей муниципальных служащих Совета народных депутатов города
Владимира,
ответственных за проведение мероприятий по обезличиванию обрабатываемых
персональных данных

Руководитель аппарата;

Консультант юридического отдела (ответственный за работу с кадрами);

Консультант группы консультантов аппарата (ответственный за работу с
информационными технологиями).

Приложение № 2
к распоряжению председателя
Совета народных депутатов
города Владимира
от 17.06.2021 № 17-р
Приложение № 5
к распоряжению главы
города Владимира
от 31.01.2013 № 8-р

Типовая форма согласия
на обработку персональных данных муниципальных служащих
Совета народных депутатов города Владимира, иных субъектов персональных
данных, а также типовая форма разъяснения субъекту персональных данных
юридических последствий отказа предоставить свои персональные данные
Типовая форма согласия
на обработку персональных данных муниципальных служащих
Совета народных депутатов города Владимира, иных субъектов персональных
данных

1. Я, _____,
(фамилия, имя, отчество (при наличии))
зарегистрированный(ная) по адресу _____

паспорт, серия _____ № _____, выдан _____

(кем и когда выдан)

свободно, своей волей и в своем интересе даю согласие уполномоченным
должностным лицам Совета народных депутатов города Владимира (далее —
СНД г.Владимира), зарегистрированного
по адресу: 600000, г.Владимир, ул.Горького, д.36, на обработку (любое
действие (операцию) или совокупность действий (операций), совершаемых с
использованием средств автоматизации или без использования таких средств с
персональными данными, включая сбор, запись, систематизацию, накопление,
хранение, уточнение (обновление, изменение), извлечение, использование,
передачу (распространение, предоставление, доступ), обезличивание,
блокирование, удаление, уничтожение) следующих персональных данных:

- 1) фамилия, имя, отчество (при наличии) (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения, сведения о том, когда, где и по какой причине они изменялись);
- 2) личная фотография;
- 3) собственноручная подпись;
- 4) дата рождения (число, месяц, год рождения);
- 5) место рождения;
- 6) сведения о гражданстве (в том числе предыдущие гражданства, иные гражданства);
- 7) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи;
- 8) вид, серия, номер документа, удостоверяющего личность гражданина

Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи;

9) адрес и дата регистрации (снятия с регистрационного учета) по месту жительства (месту пребывания), адрес фактического проживания, адреса прежних мест жительства;

10) номера контактных телефонов (домашнего (при наличии), служебного, мобильного (при наличии)), сведения об иных способах связи с субъектом персональных данных (при наличии), в том числе сведения об адресе электронной почты в информационно-телекоммуникационной сети Интернет (при наличии);

11) реквизиты страхового свидетельства обязательного пенсионного страхования, содержащиеся в нем сведения;

12) страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

13) реквизиты удостоверений (документов), подтверждающих имеющиеся государственные и иные льготы (гарантии, компенсации, пособия), содержащиеся в них сведения;

14) идентификационный номер налогоплательщика;

15) реквизиты страхового медицинского полиса обязательного медицинского страхования, содержащиеся в нем сведения;

16) реквизиты свидетельств государственной регистрации актов гражданского состояния, содержащиеся в них сведения;

17) сведения о семейном положении, о составе семьи, в том числе о гражданах, находящихся (находившихся) на иждивении, о родителях (усыновителях), детях, включая усыновленных (удочеренных), братьях, сестрах и других близких родственниках, о супруге (бывшем или бывшей супруге) и его (ее) родителях (усыновителях), детях, включая усыновленных (удочеренных), братьях и сестрах, в том числе сведения: степень родства, фамилии, имена, отчества (при наличии), даты рождения, места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), включая усыновленных (удочеренных) детей, а также мужа (жены), в том числе сведения: фамилии, имена, отчества (при наличии), даты рождения, места рождения, места работы и домашние адреса бывших мужей (жен), сведения о выполняемой работе с начала трудовой деятельности;

18) реквизиты бумажной трудовой книжки (трудовых книжек) (при наличии) и вкладыша к трудовой книжке (вкладышах к трудовой книжке) (при наличии), содержащиеся в ней (в них) сведения;

19) сведения, содержащиеся в электронной трудовой книжке;

20) сведения о воинском учете и реквизиты документов воинского учета, а также сведения, содержащиеся в документах воинского учета;

21) сведения об образовании, в том числе о профессиональном образовании (когда, какие образовательные и (или) иные организации окончил, наименование указанных организаций, реквизиты документов об образовании,

направление подготовки, квалификация и специальность по документам об образовании);

22) сведения о профессиональной переподготовке и (или) повышении квалификации (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке или о повышении квалификации, квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения);

23) сведения об ученой степени, ученом звании (когда присвоены, номера дипломов, аттестатов);

24) сведения о владении государственным языком, иностранными языками и языками народов Российской Федерации, степени владения (читаю и перевожу со словарем, читаю и могу объясняться, владею свободно);

25) сведения из заключения (справок) медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на муниципальную службу и ее прохождению;

26) сведения о прохождении муниципальной службы (государственной гражданской службы), в том числе: дата, основания поступления на муниципальную службу (государственную гражданскую службу) и назначения на должность муниципальной службы (государственной гражданской службы), дата, основания назначения, перевода, перемещения на иную должность муниципальной службы (государственной гражданской службы), наименование замещаемых должностей муниципальной службы (государственной гражданской службы) с указанием структурных подразделений, размера денежного содержания, результатов аттестации на соответствие замещаемой должности муниципальной службы (государственной гражданской службы), а также сведения о прежних местах службы (работы, обучения), периодах службы (работы, обучения), наименовании должностей;

27) сведения, содержащиеся в трудовом договоре (служебном контракте, контракте), дополнительных соглашениях к трудовому договору (служебному контракту, контракту);

28) кем и когда присвоены классный чин федеральной гражданской службы, дипломатический ранг, воинское или специальное звание, классный чин правоохранительной службы, классный чин гражданской службы субъекта Российской Федерации, квалификационный разряд государственной службы, квалификационный разряд или классный чин муниципальной службы;

29) сведения о пребывании за границей;

30) сведения о близких родственниках (отце, матери, братьях, сестрах и детях), а также мужьях (женах), в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (при наличии), с какого времени проживают за границей);

31) сведения о наличии либо отсутствии судимости, в том числе у лиц, состоящих с субъектом персональных данных в родстве или свойстве;

32) сведения об организации, осуществляющей образовательную

деятельность, в которой реализуют право на образование дети;

33) сведения о форме, номере и дате оформления допуска к государственной тайне, ранее имевшемся и (или) имеющемся, в том числе оформленном за период службы или работы, а также к иным конфиденциальным сведениям;

34) сведения о государственных наградах, иных наградах и знаках отличия (в том числе кем и когда награжден), о применении иных видов поощрений, привлечении к дисциплинарной и (или) иным видам юридической ответственности;

35) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;

36) сведения о доходах, расходах, об имуществе и обязательствах имущественного характера;

37) сведения о состоянии здоровья, о травматизме (болезнях), инвалидности, полученных в период прохождения муниципальной службы (государственной службы, осуществления работы) или обучения, в том числе о группе инвалидности, степени инвалидности, о причине наступления болезни или инвалидности (в связи с получением ранения, контузии, увечья, в результате несчастного случая либо служебной или трудовой деятельности), о сроке действия установленной инвалидности, о назначенных (выплаченных) страховых и компенсационных выплатах, о прохождении диспансеризации;

38) биометрические персональные данные, не являющиеся фотографией, в том числе антропометрическая, дактилоскопическая, геномная информация, а также специальные категории персональных данных - в случаях, предусмотренных законодательством Российской Федерации;

39) сведения о жилищном положении;

40) сведения о счетах в банках и кредитных организациях (наименование банка или кредитной организации, номер счета и дата открытия);

41) реквизиты банковских карт (номер банковской карты).

2. Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на муниципальную службу, ее прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации полномочий, возложенных на СНД г.Владимира действующим законодательством Российской Федерации, в том числе:

1) организации проверки персональных данных, сообщенных о себе при приеме на работу, проверки сведений о доходах, расходах, об имуществе и обязательствах имущественного характера;

2) отражения информации в кадровых документах;

3) ведения реестра муниципальных служащих СНД г.Владимира;

4) начисления заработной платы;

5) начисления и уплаты предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование;

6) представления СНД г.Владимира установленной законодательством Российской Федерации отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд Российской Федерации (ПФР), сведений налога на доходы физических лиц (НДФЛ) в Федеральную налоговую службу (ФНС России), сведений в Фонд социального страхования Российской Федерации (ФСС);

7) предоставления сведений в банк (кредитную организацию) для оформления банковской карты и перечисления на нее заработной платы;

8) предоставления налоговых вычетов;

9) размещение сведений о муниципальном служащем на официальном сайте органов местного самоуправления города Владимира;

10) формирование кадрового резерва, резерва управленческих кадров, осуществления работы с ним;

11) подготовки документов для прохождения медицинского осмотра;

12) предоставления информации в медицинские учреждения, страховые компании;

13) предоставления информации в организации, осуществляющие образовательную деятельность, при направлении на повышение квалификации;

14) контроля качества выполняемой мной работы;

15) оформления и выдачи служебных удостоверений, пропусков;

16) обеспечения сохранности имущества СНД г.Владимира.

3. Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы (работы) в СНД г.Владимира, нахождения в кадровом резерве;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных СНД г.Владимира вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в СНД г.Владимира в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на СНД г.Владимира полномочий и обязанностей.

4. Дата начала обработки персональных данных: « ____ » _____ 20__ г.
Настоящее согласие заполнено и подписано мною собственноручно.

« ____ » _____ 20__ г. _____ / _____ /

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

Разъяснения юридических последствий отказа предоставить свои персональные
данные

1. Мне, _____,

(указываются полностью фамилия, имя, отчество (при наличии):
муниципального служащего; кандидата на включение в кадровый резерв
муниципальной службы; работника, замещающего должности в СНД
г.Владимира, не являющимися должностями муниципальной службы;
руководителя муниципального учреждения (предприятия) города Владимира,
лица, претендующего на замещение данной должности)

_____ ,
(наименование и реквизиты документа, удостоверяющего личность: серия,
номер, дата выдачи, наименование органа и код подразделения органа (при
наличии), выдавшего документ)

зарегистрированному(ой) по адресу: _____

разъяснены юридические последствия отказа предоставить свои персональные
данные (далее - персональные данные) СНД г. Владимира, а равно подписать
согласие на обработку персональных данных по типовой форме такого
согласия, предусмотренного для муниципальных служащих СНД г.Владимира, а
также иных субъектов персональных данных, или отзыва указанного согласия.

2. Я предупрежден(а) о том, что в случае моего отказа предоставить
персональные данные СНД г. Владимира не сможет осуществлять их обработку.

3. Мне также известно, СНД г.Владимира
для осуществления и выполнения возложенных законодательством Российской
Федерации функций, полномочий и обязанностей в соответствии
с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных
данных» вправе продолжить обработку персональных данных без моего
согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6,
части 2 статьи 10 и части 2 статьи 11 вышеуказанного Федерального закона.

4. Настоящее разъяснение заполнено и подписано мною собственноручно.

(подпись)

(инициалы, фамилия)

Приложение № 3
к распоряжению председателя Совета
народных депутатов города Владимира
от 17.06.2021 № 17-р
Приложение № 9 к распоряжению
главы города Владимира
от 31.01.2013 № 8-р

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами.

1. Общие положения

1.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в аппарате Совета народных депутатов города Владимира (далее - Совет) разработаны в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», принятых в соответствии с ним нормативных правовых актов Российской Федерации и распространяются на муниципальных служащих аппарата Совета (далее - муниципальные служащие) и лиц, замещающих в аппарате Совета должности, не являющиеся должностями муниципальной службы (далее - иные работники Совета).

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным: Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Федеральным законом от 02.03.2007 № 25-ФЗ «О муниципальной службе»; Трудовым кодексом Российской Федерации; постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; иными нормативными правовыми актами, регламентирующими порядок обработки персональных данных.

2. Порядок проведения внутренних проверок

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Совете проводятся периодические проверки условий обработки персональных данных.

2.2. Проверки условий обработки персональных данных проводятся комиссией, состав которой утверждается Председателем Совета (далее - комиссия).

2.3. Основанием для проведения проверки является поручение Председателя Совета.

2.4. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса, осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных, изучения документов, а также с использованием иных, не противоречащих федеральным законам и другим нормативным актам Российской Федерации, способов исследования фактических обстоятельств в течение одного месяца со дня возникновения основания для проведения проверки.

2.5. По результатам проверки большинством голосов членов комиссии принимается решение. В течение пяти рабочих дней после завершения проверки составляется Акт проведения внутренней проверки условий обработки персональных данных в аппарате Совета народных депутатов города Владимира (далее - Акт) по форме согласно приложению. С Актом должны быть ознакомлены сотрудники, участвующие в процессе обработки персональных данных, в отношении, которых проводилась проверка.

2.6. При выявлении в ходе проверки нарушений в Акте делается запись о мероприятиях по устранению нарушений и сроках исполнения. Срок устранения нарушений устанавливается комиссией и не может быть более одного месяца со дня составления Акта.

2.7. Акты проведения внутренних проверок хранятся у председателя комиссии в течение трех лет с даты проведения проверки, после чего подлежат уничтожению.

2.8. Информация о результатах проверки и мерах, необходимых для устранения нарушений, направляется Председателю Совета в течение двух рабочих дней после составления Акта.

Приложение
к «Правилам осуществления внутреннего контроля
соответствия обработки персональных данных требованиям
к защите персональных данных в Совете народных депутатов города Владимира»

Акт
проведения внутренней проверки условий обработки персональных
данных в аппарате Совета народных депутатов города Владимира

« _____ » _____ г. _____

На основании пункта 4 части 1 статьи 18.1 Федерального закона от
27.07.2006 № 152-ФЗ «О персональных данных», руководствуясь Правилами
осуществления внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных в Совете народных
депутатов города Владимира, утвержденными

_____, в период с
_____ по _____

комиссией для проведения проверок условий обработки персональных
данных в аппарате Совета народных депутатов города Владимира в составе:
Председатель комиссии (должностное лицо):

(Ф.И.О., должность)

Члены комиссии:

(Ф.И.О., должность)

(Ф.И.О., должность)

(Ф.И.О., должность)

проведена внутренняя проверка условий обработки персональных данных в
аппарате Совета народных депутатов города Владимира

В ходе проверки установлено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Председатель комиссии: _____

(Ф.И.О., должность)

Члены комиссии: _____

(Ф.И.О., должность)

(Ф.И.О., должность)

(Ф.И.О., должность)

(Ф.И.О., должность)

Приложение № 4 к распоряжению
председателя Совета народных депутатов
города Владимира
от 17.06.2021 № 17-р
Приложение № 10
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

Перечень
должностей в Совете народных депутатов города Владимира, замещение которых
предусматривает осуществление обработки персональных данных либо
осуществление доступа к персональным данным

- Руководитель аппарата;
- Заведующий юридическим отделом;
- Заведующий отделом бухгалтерского учета и отчетности;
- Консультант отдела бухгалтерского учета и отчетности;
- Консультант юридического отдела (ответственный за работу с кадрами);
- Консультант группы консультантов аппарата (ответственный за работу с информационными технологиями);
- Консультант группы консультантов аппарата (ответственный за работу с обращениями граждан);

Приложение №5 к распоряжению
председателя Совета народных депутатов города Владимира
от 17.06.2021 № 17-р

Приложение № 11
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

Список помещений

Совета народных депутатов города Владимира, в которых обрабатываются персональные данные без использования средств автоматизации и с использованием автоматизированных средств, и доступ к ним

1. Список помещений, в которых обрабатываются персональные данные

1. 1. г.Владимир, ул.Горького, д.36

- кабинет № 309
- кабинет № 411
- кабинет № 501
- кабинет № 502
- кабинет № 504
- кабинет № 506
- кабинет № 507
- кабинет № 508
- кабинет № 510
- кабинет № 511
- кабинет № 512
- кабинет № 513
- кабинет № 514
- кабинет № 515

2. Список сотрудников, имеющих доступ в помещения

№п/п	ФИО	Должность	Подразделение	№кабинета
1	Толбухин Николай Юрьевич	Председатель Совета народных депутатов города Владимира		512
2	Пышонина Лариса Васильевна	Заместитель председателя Совета народных депутатов города Владимира		514
3	Момот Ирина Александровна	Руководитель аппарата		507
4	Петров Владимир Николаевич	Заведующий отделом	Юридическим отделом	504
5	Ильина Марина Александровна	Консультант	Юридический отдел	515
6	Солодова Галина Александровна	Консультант	Юридический отдел	515
7	Замыслаева Ольга Васильевна	Заведующий отделом	Отдел бухгалтерского учета и отчетности	510

8	Усоева Наталья Анатольевна	Консультант	Отдел бухгалтерского учета и отчетности	510
9	Борисов Юрий Юрьевич	Заведующий отделом	Отдел по работе с общественностью,, СМИ. Социальными сетями	411
10	Шелоханова Анна Александровна	Консультант	Группа консультантов аппарата	513
11	Путова Наталья Владимировна	Консультант	Группа консультантов аппарата	511
12	Седов Алексей Олегович	Консультант	Группа консультантов аппарата	309
13	Бочкарева Галина Васильевна	Консультант	Группа консультантов и специалистов комитетов	506
14	Маркин Александр Владимирович	Консультант	Группа консультантов и специалистов комитетов	508
15	Нечаев Андрей Иванович	Консультант	Группа консультантов и специалистов комитетов	501
16	Агафонова Милана Николаевна	Консультант	Группа консультантов и специалистов комитетов	502
17	Малороссиянцева Екатерина Владимировна	Консультант	Группа консультантов и специалистов комитетов	515
18	Виноградова Валентина Викторовна	Главный специалист	Группа консультантов и специалистов комитетов	502

Приложение № 6 к распоряжению
председателя Совета народных
депутатов от 17.06.2021 № 17-р

Приложение № 12 к распоряжению
главы города Владимира от
31.01.2013 № 8-р

Перечень
информационных систем персональных данных
Совета народных депутатов города Владимира

Наименование информационной системы персональных данных (ИСПДн)	Адрес размещения системы	Наименование подсистемы ИСПДн	Перечень персональных данных	Цель обработки персональных данных
«Работники Совета Народных депутатов города Владимира»	600017, г.Владимир, ул.Горького, 36	1С: Предприятие. Кадровый учет Обращения граждан	Фамилия, имя, отчество; должность; год рождения; образование; адрес места жительства; паспортные данные; ИНН; СНИЛС; семейное положение; сведения о составе семьи; сведения о несовершеннолетних детях, контактный телефон, адрес электронной почты	Ведение кадрового учета и программа обращение граждан
		1С: Предприятие. Бухгалтерия государственного учреждения	Фамилия, имя, отчество; должность; год рождения; образование; адрес места жительства; паспортные данные; ИНН, воинский учет, СНИЛС, полис, семейное положение; сведения о составе семьи, аттестации. сведения о несовершеннолетних детях, отпуска, премии	Ведение бухгалтерского учета
		1С- КАМИН: Зарплата для бюджетных учреждений	Фамилия, имя, отчество; должность; образование; сведения о заработной плате; год рождения;	Ведение бухгалтерского учета, начисление заработной платы

			адрес места жительства; паспортные данные; ИНН; СНИЛС; номер телефона; номера банковских счетов; семейное положение; сведения о составе семьи; сведения о несовершеннолетних детях	
		Система «СБИС»	Фамилия, имя, отчество; должность; сведения о сумме полученного дохода; адрес места жительства; паспортные данные; ИНН; СНИЛС	Представление отчетности
		Система «Сбербанк Бизнес Онлайн»	Фамилия, имя, отчество; номер телефона; номера банковских счетов; сведения о сумме полученного дохода; адрес места жительства; год рождения; паспортные данные	Открытие банковских счетов, выпуск банковских карт, перечисление заработной платы
		Печать удостоверений	Фамилия, имя, отчество; должность	Выдача служебных удостоверений

Приложение № 7 к распоряжению
председателя Совета народных депутатов
города Владимира
от 17.06.2021 № 17-р
Приложение № 15
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

Акт классификации
информационной системы персональных данных «Обращение граждан» Совета
народных депутатов города Владимира

г.Владимир
2021г.

Комиссия, назначенная распоряжением председателя Совета народных депутатов города Владимира № _____ от _____.20__ г, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»:

- 1. Категория персональных данных, обрабатываемых в информационной системе (X_{плд})-2
- 2. Объем обрабатываемых персональных данных (X_{плд})-2
- 3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относиться к : **типовой**
- 4. Структура информационной системы: **локальная**
- 5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
- 6. Режим обработки персональных данных в информационной системе: **однопользовательский**
- 7. Разграничение прав доступа пользователей: **без разграничения**
- 8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**
Исходя из анализа исходных данных ИСПДн,на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается 2 класс.

Председатель комиссии: _____

Члены комиссии: _____

Приложение №8 к распоряжению
председателя Совета народных депутатов
города Владимира
от 17.06.2021 № 17-р
Приложение № 16
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

АКТ КЛАССИФИКАЦИИ
информационной системы персональных данных «База учета труда и заработной
платы» Совета народных депутатов города Владимира

г.Владимир
2021г.

Комиссия, назначенная распоряжением председателя Совета народных депутатов города Владимира № _____ от __. __. 20__ г, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»:

- 1. Категория персональных данных, обрабатываемых в информационной системе (X_{пд})-**3**
- 2. Объем обрабатываемых персональных данных (X_{пдн})-**3**
- 3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относиться к : **типовой**
- 4. Структура информационной системы: **локальная**
- 5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
- 6. Режим обработки персональных данных в информационной системе: **однопользовательский**
- 7. Разграничение прав доступа пользователей: **без разграничения**
- 8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**
Исходя из анализа исходных данных ИСПДн,на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается 3 класс.

Председатель комиссии: _____

Члены комиссии: _____

Приложение №9 к распоряжению
председателя Совета народных депутатов
города Владимира
от 17.06.2021 № 17-Д
Приложение № 17
к распоряжению главы города Владимира
от 31.01.2013 № 8-р

Акт классификации
информационной системы персональных данных «База данных работников Совета
народных депутатов» (кадры)

г.Владимир
2021г.

Комиссия, назначенная распоряжением председателя Совета народных депутатов города Владимира № _____ от __. __. 20__ г, рассмотрев исходные данные информационной системы персональных данных (ИСПДн) «Обращения граждан», в соответствии с требованиями Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»:

- 1. Категория персональных данных, обрабатываемых в информационной системе (X_{плд})-**2**
- 2. Объем обрабатываемых персональных данных (X_{плн})-**3**
- 3. Информационная система персональных данных, по заданным оператором характеристикам безопасности относиться к : **типовой**
- 4. Структура информационной системы: **локальная**
- 5. Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена: **имеет подключения**
- 6. Режим обработки персональных данных в информационной системе: **однопользовательский**
- 7. Разграничение прав доступа пользователей: **без разграничения**
- 8. Местонахождения информационных систем персональных данных: **целиком в пределах Российской Федерации**
Исходя из анализа исходных данных ИСПДн,на основе исследования актуальности угроз и определения методов защиты от них, ИСПДн комиссией присваивается 3 класс.

Председатель комиссии: _____

Члены комиссии: _____

