Для служебного пользования
Экз. № _____

ГЛАВА МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
МЭР ГОРОДА АРХАНГЕЛЬСКА

Р А С П О Р Я Ж Е Н И Е

от 11 августа 2009 г. № 1095р-ДСП

Об использовании персональных данных и обеспечении их безопасности в мэрии города

В соответствии с федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.03.2007 № 25-ФЗ "О муниципальной службе в Российской Федерации", Трудовым кодексом Российской Федерации, Указом Президента Российской Федерации от 30.05.2005 № 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела", постановлениями Правительства Российской Федерации от 17.11.2007 № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", в целях регулирования отношений, связанных с использованием персональных данных и обеспечением их безопасности в мэрии города:

1. Утвердить прилагаемые:

Положение о персональных данных субъектов персональных данных мэрии города;

Перечень должностных лиц мэрии города, имеющих доступ к персональным данным;

Положение об организации проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных мэрии города.

2. Руководителям отраслевых (функциональных) и территориальных органов мэрии города ознакомить работников с настоящим распоряжением и организовать работу с персональными данными в соответствии с его требованиями.

3. Контроль за исполнением распоряжения возложить на заместителя мэра города - руководителя аппарата Гармашова В.С.

Мэр города **В.Н. Павленко**

лф 05.08.09
Общий отдел мэрии г.Архангельска. Заказ 015. 11.04.2003

УТВЕРЖДЕН
распоряжением мэра
города Архангельска
от 11.08.2009 № 1095р-ДСП

ПЕРЕЧЕНЬ
должностных лиц мэрии города, имеющих доступ к персональным данным

1. Мэр города, начальник управления муниципальной службы и кадров мэрии города - в полном объеме информации.

2. Заместители мэра города - в полном объеме информации о муниципальных служащих мэрии города, работниках, осуществляющих техническое обеспечение деятельности отраслевых (функциональных) и территориальных органов мэрии города (далее - работниках), руководителях муниципальных унитарных предприятий и муниципальных учреждений города по подчиненности.

3. Руководители отраслевых (функциональных) и территориальных органов мэрии города - в полном объеме информации о подчиненных муниципальных служащих и работниках, руководителях подведомственных муниципальных унитарных предприятий и муниципальных учреждений.

4. Муниципальные служащие департамента образования, департамента здравоохранения и социальной политики, департамента муниципального имущества, департамента финансов и казначейского исполнения бюджета, управления культуры и молодежной политики, управления по физической культуре и спорту, управления муниципальной службы и кадров мэрии города, ведущие кадровое делопроизводство, - в объеме информации, необходимой для ведения кадровой работы.

5. Муниципальные служащие департамента образования, департамента здравоохранения и социальной политики, департамента муниципального имущества, департамента финансов и казначейского исполнения бюджета, управления культуры и молодежной политики, управления по физической культуре и спорту, отдела учета и отчетности мэрии города, осуществляющие начисления (выплаты) заработной платы (пенсий, компенсаций, премий и т.п.), - в объеме информации, необходимой для выполнения их функций.

6. Муниципальные служащие департамента здравоохранения и социальной политики мэрии города, ведущие обработку специальных категорий персональных данных, - в объеме информации, необходимой для выполнения их функций.

7. Муниципальные служащие (работники) департамента организационной работы, информационных ресурсов и систем мэрии города, уполномоченные для выполнения функций администраторов информационных ресурсов и безопасности, - в объеме информации, необходимой для выполнения этих функций.

8. Муниципальные служащие управления военно-мобилизационной работы и административных органов, уполномоченные для ведения работы по воинскому учету, бронированию и оформления допуска к сведениям, составляющим государственную тайну, - в объеме информации, необходимой для выполнения указанных функций.

9. Муниципальные служащие муниципально-правового департамента - в объеме информации, необходимой для выполнения их функций.

10. Муниципальные служащие органов мэрии города, в части персональных данных, содержащихся в договорах гражданско-правового характера, - в объеме информации, необходимой для выполнения их функций.

_____

Для служебного пользования
Экз. №

УТВЕРЖДЕНО
распоряжением мэра
города Архангельска
от 11.08.2009 № 1095р-ДСП

ПОЛОЖЕНИЕ
о персональных данных субъектов персональных данных мэрии города

I. Общие положения

1.1. Настоящее Положение определяет порядок использования и обеспечения защиты персональных данных (далее - ПДн) субъектов ПДн при их обработке в мэрии города.

Использование ПДн - действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

Операторами, организующими и (или) осуществляющими обработку ПДн, а также определяющими цели и содержание обработки ПДн в мэрии города, являются:

мэрия города и ее отраслевые (функциональные) и территориальные органы (далее – органы мэрии города):

департамент образования мэрии города;

департамент здравоохранения и социальной политики мэрии города;

департамент муниципального имущества мэрии города;

департамент финансов и казначейского исполнения бюджета мэрии города;

управление культуры и молодежной политики мэрии города;

управление по физической культуре и спорту.

Субъекты ПДн мэрии города - муниципальные служащие мэрии города, работники, осуществляющие техническое обеспечение деятельности органов мэрии города, руководители муниципальных унитарных предприятий и муниципальных учреждений города, иные граждане Российской Федерации, использование ПДн которых осуществляется мэрией города с целью реализации полномочий органа местного самоуправления и требований законодательства Российской Федерации.

1.2. Положение разработано в соответствии с федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.03.2007 № 25-ФЗ "О муниципальной службе в Российской Федерации", Трудовым кодексом

Российской Федерации, Указом Президента Российской Федерации от 30.05.2005 № 609 "Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела", постановлением Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.3. Требования настоящего Положения являются обязательными для исполнения во всех органах мэрии города, являющихся операторами ПДн, или осуществляющими обработку и (или) использование ПДн.

1.4. Субъекты ПДн должны быть ознакомлены под роспись с документами оператора (работодателя), устанавливающими порядок работы с ПДн и их использования, а также их права и обязанности в этой области.

II. Порядок работы с ПДн и их использования

2.1. Основным требованием при использовании ПДн является обеспечение их конфиденциальности.

Конфиденциальность ПДн - обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Указанное требование не распространяется на обезличенные и общедоступные ПДн.

2.2. Официальными формами и системами, содержащими, накапливающими и обеспечивающими обработку ПДн субъектов ПДн в мэрии города, являются:

личное дело;

трудовая книжка;

личная карточка муниципального служащего или работника (унифицированная форма № Т-2ГС или Т-2);

базы (массивы данных) автоматизированных систем, содержащие ПДн;

иные материальные носители, содержащие ПДн.

2.3. О намерении осуществлять обработку ПДн и их использовании (далее-использование ПДн) оператор обязан уведомить уполномоченный орган по защите прав субъектов ПДн (Управление Россвязькомнадзора по Архангельской области и Ненецкому автономному округу) в сроки и порядке, установленные Федеральным законом "О персональных данных", за исключением случаев, предусмотренных законодательством Российской Федерации.

О всех изменениях сведений, представленных в уведомлении, оператор обязан в течение десяти рабочих дней с момента их возникновения уведомить этот орган.

2.4. Любые операции с ПДн осуществляются только с согласия и в письменной форме субъекта ПДн, за исключением случаев, предусмотренных статьей 6 Федерального закона "О персональных данных".

Субъект ПДн принимает решение о представлении своих ПДн и согласии их использования в мэрии города по своей воле и в своем интересе.

Примерная форма согласия субъекта ПДн приведена в приложении № 1 к настоящему Положению.

Письменное согласие субъекта ПДн рекомендуется хранить в его личном деле, при отсутствии такового, порядок хранения определяет оператор.

2.5. Доступ к ПДн:

2.5.1. Доступ субъекта ПДн к его ПДн предоставляется оператором при его обращении либо при получении запроса субъекта ПДн.

Сведения о ПДн должны быть представлены субъекту ПДн в доступной форме, в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

В случаях, предусмотренных законодательством Российской Федерации, право субъекта ПДн на доступ к своим ПДн может быть ограничено.

2.5.2. Мэр города определяет перечень должностных лиц, допускаемых к ПДн субъектов ПДн в силу их должностных обязанностей и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих данных.

2.5.3. Доступ работников, осуществляющих непосредственную работу с ПДн и их использование, к соответствующим ПДн осуществляется оператором на основании утвержденного им или уполномоченным лицом списка согласно приложению № 2 к настоящему Положению.

Один экземпляр указанного списка, а при необходимости и копии должностных инструкций, представляются в отдел по защите информации управления военно-мобилизационной работы и административных органов мэрии города.

2.5.4. Допуск к информационным системам ПДн осуществляется в соответствии с Положением о доступе к информационным ресурсам в локальной вычислительной сети мэрии города, утвержденным постановлением мэра города от 30.06.2008 № 28, и на основании выше-названных документов.

2.6. Работа с ПДн должна осуществляться в следующем порядке:

1) получение ПДн (при необходимости - письменного согласия на их обработку);

2) проверка достоверности ПДн;

3) накопление ПДн: ввод в базу данных, учет, систематизация;

4) контроль обеспечения сохранности: разграничение доступа, резервное копирование, ревизия (восстановление);

5) комбинирование: анализ, выдача по запросу, обновление (дополнение, изменение, блокирование);

6) архивное хранение: описание, экспертиза ценности, передача на постоянное хранение (уничтожение).

2.7. Субъект ПДн имеет право:

доступа и ознакомления со своими ПДн, включая безвозмездное получение копии любой записи, содержащей его ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации;

требовать от оператора уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели их использования, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав;

получения подтверждения факта использования ПДн оператором, а также целей их использования;

отзыва у оператора согласия на использование (обработку) своих ПДн;

определять законных представителей для защиты своих прав;

обжаловать в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке неправомерные действия или бездействия оператора при использовании ПДн и их защите;

на получение от оператора информации, касающейся использования его ПДн, в том числе содержащей:

сведения об операторе, о месте его нахождения, о наличии у оператора ПДн, относящихся к соответствующему субъекту ПДн;

способы обработки ПДн, применяемые оператором;

сведения о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ;

перечень используемых ПДн и источник их получения;

сроки использования ПДн, в том числе и сроки их хранения;

сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой использование его ПДн.

2.8. Субъект ПДн обязан:

представлять достоверные сведения о себе;

в срок, не превышающий 5 дней, сообщать оператору или уполномоченному им лицу изменения своих ПДн.

2.9. Оператор обязан:

при организации работы с ПДн и их использовании принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий;

использовать ПДн для достижения только заявленных целей или в целях обеспечения выполнения требований, предусмотренных законодательством Российской Федерации;

при организации работы с ПДн и их использовании получать ПДн только от субъекта ПДн;

разрешать доступ к ПДн субъектов ПДн только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн, которые необходимы для выполнения ими конкретных функций;

представлять доказательства получения согласия субъекта ПДн на использование его ПДн, а в случае использования общедоступных ПДн - доказывать, что они являются общедоступными;

при получении письменного согласия субъекта ПДн на использование его ПДн разъяснить ему порядок принятия решения, в том числе и на основании исключительно автоматизированной обработки ПДн, и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

При наличии возражений оператор обязан рассмотреть их в течение семи рабочих дней со дня их получения и уведомить субъекта ПДн о результатах их рассмотрения;

в предусмотренных федеральным законодательством случаях обязательного представления субъектом ПДн своих ПДн разъяснить ему юридические последствия отказа их представления;

определять и утверждать список лиц, уполномоченных для работы с ПДн и их использования;

предупреждать лиц, получивших ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от них подтверждения того, что это правило соблюдено;

предоставлять субъекту ПДн доступ к его ПДн или иную информацию, касающуюся их использования и обработки, в объеме и в порядке, предусмотренном законодательством Российской Федерации и настоящим Положением;

при получении ПДн не от субъекта ПДн, за исключением случаев, если они были представлены оператору на основании федерального закона или если ПДн являются общедоступными, до начала их использования представить субъекту ПДн следующую информацию:

наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

цель использования (обработки) ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные федеральным законодательством права субъекта ПДн;

при получении ПДн у третьей стороны оператор обязан уведомить об этом субъекта ПДн и получить его письменное согласие на их использование (обработку);

в случае отзыва субъектом ПДн своего согласия прекратить обработку его ПДн и уничтожить их в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством Российской Федерации или соглашением между оператором и субъектом ПДн. Об уничтожении ПДн оператор обязан уведомить субъекта ПДн;

при обращении или по запросу субъекта ПДн либо уполномоченного органа по защите прав субъектов ПДн по выявленным фактам недостоверных ПДн или неправомерных действий с ними оператора, осуществить блокирование ПДн, относящихся к соответствующему субъекту ПДн, с момента такого обращения или получения запроса на период проверки. При подтверждении факта недостоверности ПДн на основании документов, представленных субъектом ПДн либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов уточнить ПДн и снять их блокирование.

При выявлении неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, устранить допущенные нарушения. При невозможности устранения нарушений в указанный срок - уничтожить ПДн.

Об устранении допущенных нарушений или об уничтожении ПДн оператор обязан уведомить субъекта ПДн, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн, и указанный орган;

при достижении цели использования ПДн незамедлительно прекратить их обработку и уничтожить в срок, не превышающий трех рабочих дней с даты достижения цели, если иное не предусмотрено законодательством Российской Федерации. Уведомить об этом субъекта ПДн.

2.10. Оператору запрещается:

получать, использовать и приобщать к личному делу или иному материальному носителю ПДн субъекта ПДн, не установленные законодательством Российской Федерации;

передавать ПДн субъекта ПДн третьей стороне без его письменного согласия, за исключением случаев, установленных законодательством Российской Федерации;

принимать решения, порождающие юридические последствия в отношении субъекта ПДн, на основании данных автоматизированной обработки ПДн, за исключением случаев:

наличия письменного согласия субъекта ПДн;

предусмотренных федеральными законами, устанавливающими ее цель, условия получения ПДн и круг субъектов, ПДн которых подлежат обработке, а также полномочия оператора по мерам обеспечения соблюдения прав и законных интересов субъекта ПДн.

III. Обеспечение сохранности и защиты ПДн

3.1. Ответственность за организацию защиты ПДн и обеспечение их сохранности возлагается на оператора.

3.2. Защита ПДн субъектов ПДн от несанкционированного доступа и использования, а также обеспечение сохранности материальных носителей ПДн, обеспечивается оператором за счет средств и в порядке, установленном законодательством Российской Федерации.

3.3. Исключение возможности несанкционированного доступа к ПДн (материальным носителям ПДн) и обеспечение их сохранности достигается:

раздельным хранением ПДн (их материальных носителей), использование которых осуществляется в различных целях (не допускается фиксация на одном материальном носителе персональных данных, цели использования которых заведомо не совместимы);

запретом доступа к ПДн (материальным носителям) без специального разрешения оператора;

определением органов и должностных лиц мэрии города, уполномоченных на использование ПДн;

хранением материальных носителей ПДн в специально оборудованных и опечатываемых шкафах, сейфах;

определением оператором должностных лиц, ответственных за учет, обеспечение сохранности и иные действия с ПДн;

строгим учетом материальных носителей ПДн;

определением сроков и порядка хранения материальных носителей ПДн;

ограничением и контролем за несанкционированным доступом посторонних лиц в помещения (к объектам), в которых располагаются (хранятся) материальные носители ПДн или электронные средства их обработки (помещения, предназначенные для их хранения, оборудуются для опечатывания и сдаются в нерабочее время под охрану, определяется список лиц, уполномоченных для их вскрытия и сдачи под охрану);

соблюдением порядка выдачи материальных носителей ПДн (их выдача осуществляется уполномоченным лицом под роспись);

определением полномочий по внесению изменений в личное дело, трудовую книжку, личную карточку субъекта ПДн и иные носители ПДн (уполномоченные лица определяются оператором);

запретом нахождения посторонних лиц в помещениях, в которых хранятся или используются ПДн в период их обработки;

выполнением организационно-технических мероприятий по защите ПДн, предусмотренных для информационных систем ПДн, при их обработке с использованием средств автоматизации;

строгим выполнением требований законодательства Российской Федерации, определяющего порядок обработки, распространения (передачи) и соблюдения конфиденциальности ПДн.

3.4. Работа с ПДн без использования средств автоматизации должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (их материальных носителей) и установить перечень лиц, использующих ПДн либо имеющих к ним доступ.

3.5. Непосредственно выполнение обязанностей по исключению несанкционированного доступа к ПДн, обеспечение их сохранности и конфиденциальности возлагается на лиц, допущенных к ПДн и их использующих.

Для служебного пользования
Экз. № ____

УТВЕРЖДЕНО
распоряжением мэра
города Архангельска
от 11.08.2009 № 1095р-ДСП

ПОЛОЖЕНИЕ
об организации проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных мэрии города

I. Общие положения

1.1. Настоящее Положение устанавливает порядок проведения работ по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в информационных системах ПДн (далее - ИСПДн) мэрии города, определяет структуру системы защиты ПДн (далее - СЗПДн), ее состав, а также порядок определения способов, мер и средств защиты ПДн.

1.2. Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 17.11.2007 № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и Положением о порядке организации и проведения работ по защите конфиденциальной информации в мэрии города и ее структурных подразделениях, утвержденным постановлением мэра города от 08.06.2004 № 164-ДСП, с целью обеспечения деятельности отраслевых (функциональных) и территориальных органов мэрии города (далее - органы мэрии города), организующих и (или) осуществляющих обработку ПДн.

1.3. Положение предназначено для использования руководителями органов мэрии города, операторами ИСПДн, специалистами по обеспечению безопасности информации, организующими и осуществляющими обработку ПДн в ИСПДн.

ИСПДн - информационная система, представляющая собой совокупность ПДн, содержащихся в массивах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы

звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.4. Действие настоящего Положения не распространяется на ИСПДн, обрабатывающие ПДн, отнесенные в установленном порядке к сведениям, составляющим государственную тайну.

II. Организация работы по обеспечению безопасности ПДн в ИСПДн

2.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и осуществление на этапах разработки (модернизации) ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и уклонение от угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы с целью минимизации ущерба от возможной реализации таких угроз.

2.2. Организация обеспечения безопасности ПДн в ИСПДн должна осуществляться в следующем порядке и предусматривать:

оценку обстановки;

обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

разработку замысла обеспечения безопасности ПДн;

выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла обеспечения безопасности ПДн;

планирование мероприятий по защите ПДн;

организацию и проведение работ по созданию СЗПДн в рамках разработки (модернизации) ИСПДн или ее элементов, в том числе с привлечением специализированных сторонних организаций, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн. Порядок привлечения сторонних организаций к разработке и эксплуатации СЗПДн определен Положением о порядке организации и проведения работ по защите конфиденциальной информации в мэрии города и ее структурных подразделениях, утвержденным постановлением мэра города от 08.06.2004 № 164-ДСП;

разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;

развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;

доработку СЗПДн по результатам опытной эксплуатации.

2.2.1. Оценка обстановки основывается на результатах комплексного обследования ИСПДн, в ходе которого:

определяется информация, содержащая ПДн, и ее материальные носители;

осуществляется ее категорирование по важности;

определяется необходимость защиты (обеспечения безопасности) ПДн.

При оценке обстановки должна учитываться степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн. Рекомендуемый порядок ее проведения представлен в приложении № 1 к настоящему Положению.

2.2.2. Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России, обязательными к применению стандартами и на основании Основных мероприятий по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн, утвержденных заместителем директора ФСТЭК России 15.02.2008.

2.2.3. При разработке замысла обеспечения безопасности ПДн осуществляется выбор основных способов защиты ПДн.

Рекомендуемый порядок формирования замысла представлен в приложении № 2 к настоящему Положению.

2.2.4. При выборе целесообразных способов обеспечения безопасности ПДн, обрабатываемых в ИСПДн, определяются организационные меры и технические (аппаратные, программные и программно-аппаратные) средства защиты ИСПДн.

2.2.5. К основным вопросам управления относятся:

распределение функций управления доступом к ПДн и их обработкой между должностными лицами;

определение порядка изменения правил доступа к защищаемой информации;

определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;

определение порядка проведения контрольных мероприятий и действий по их результатам.

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться

оператором, специализированными подразделениями (отделом по защите информации управления военно-мобилизационной работы и административных органов мэрии города) или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

2.2.6. При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн наряду с настоящим Положением в обязательном порядке разрабатываются:

Требования по обеспечению безопасности ПДн при обработке в ИСПДн;

должностные инструкции пользователям ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;

рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

2.2.7. Испытания СЗПДн проводятся в процессе развертывания и ввода в опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн.

III. Основные мероприятия по организации обеспечения безопасности ПДн при обработке в ИСПДн

3.1. Безопасность ПДн при их обработке в автоматизированных ИСПДн обеспечивается путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты ПДн, развертываемой в ИСПДн в процессе ее создания или модернизации.

3.2. СЗПДн включает организационные меры и технические средства защиты информации (в том числе криптографические средства, средства предотвращения несанкционированного доступа (далее - НСД), утечки информации по техническим каналам и программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн.

3.3. Для функционирующих ИСПДн доработка (модернизация) СЗПДн должна проводиться в случае, если:

изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн);

изменился состав угроз безопасности ПДн в ИСПДн;

изменился класс ИСПДн.

3.4. Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

1) организация обеспечения безопасности ПДн;

2) классификация ИСПДн;

3) мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн.

3.4.1. Организация обеспечения безопасности ПДн осуществляется путем проведения мероприятий, определенных Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17.11. 2007 № 781.

3.4.1.1. Модель угроз безопасности ПДн разрабатывается в соответствии с Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн и на основе Базовой модели угроз безопасности ПДн при их обработке в ИСПДн, утвержденных заместителем директора ФСТЭК России 15.02.2008.

Выявление и оценка актуальности угроз безопасности ПДн при их обработке в ИСПДн осуществляется персонально по каждой системе, в конкретных условиях и составляют основу для планирования и осуществления мероприятий, направленных на обеспечение безопасности ПДн при их обработке в ИСПДн.

3.4.1.2. Комплекс организационных и технических мероприятий (технических средств защиты) СЗПДн должен предусматривать обеспечение безопасности ПДн от следующих угроз:

уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн;

утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);

перехвата при передаче по проводным (кабельным) линиям связи;

хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;

непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неатропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

3.4.2. Классификация ИСПДн проводится специальной комиссией мэрии города по ходатайству руководителей органов мэрии города, организующих и (или) осуществляющих обработку ПДн, в соответствии с

совместным приказом ФСТЭК России, ФСБ России и Министерства информационных технологий и связи РФ от 13.02.2008 № 55/86/20 "Об утверждении порядка проведения классификации информационных систем персональных данных", с учетом категорий и объёма накапливаемых, обрабатываемых и распределяемых с их использованием ПДн.

Классификация ИСПДн проводится на этапе их создания или в ходе эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн, с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

ИСПДн может присваиваться один из следующих классов:

класс 1 (К1) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПДн;

класс 2 (К2) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов ПДн;

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

класс 4 (К4) - ИСПДн, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПДн.

3.4.3. Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн включают:

мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;

мероприятия по закрытию технических каналов утечки ПДн при их обработке в информационных системах;

мероприятия по защите ПДн от НСД и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

IV. Требования к обеспечению безопасности ПДн при обработке в ИСПДн

4.1. Методы и способы защиты информации в ИСПДн устанавливаются ФСТЭК и ФСБ Российской Федерации в пределах их полномочий.

4.2. При обработке ПДн в ИСПДн должно быть обеспечено:

а) обмен ПДн при их обработке в информационных системах должен осуществляться по каналам связи, защита которых обеспечивается путем

реализации соответствующих организационных мер и (или) путем применения технических средств;

б) технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям по обеспечению защиты информации (иметь сертификат соответствия предъявляемым требованиям по обеспечению защиты информации);

в) размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

г) лица, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, должны допускаться к соответствующим ПДн на основании списка, утвержденного оператором или уполномоченным им лицом;

д) запросы пользователей информационной системы на получение ПДн, а также факты предоставления ПДн по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений.

Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного им лица;

ж) средства защиты информации, предназначенные для обеспечения безопасности ПДн при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров;

з) средства защиты информации, применяемые в ИСПДн, в установленном порядке должны пройти процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации;

и) проведение иных мероприятий, определенных Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17.11.2008 № 781.

4.3. Для разработки и осуществления мероприятий по обеспечению безопасности ПДн при их обработке в информационной системе оператором (руководителем органа мэрии города) может назначаться должностное лицо (работник) или подразделение органа мэрии города, ответственное за обеспечение безопасности ПДн.

4.4. При обнаружении нарушений порядка предоставления ПДн оператор или уполномоченное лицо незамедлительно приостанавливают предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.

4.5. Обязанности по организации и обеспечению реализации необходимых организационных и технических мероприятий по защите ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними возлагаются на оператора.

Непосредственное выполнение этих мероприятий возлагается на работников, осуществляющих обработку (использование) ПДн.

V. Порядок разработки и ввода в эксплуатацию СЗПДн

5.1. В ходе разработки (модернизации) и ввода в эксплуатацию СЗПДн предусматриваются следующие стадии:

предпроектная стадия, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание (модернизацию);

стадия проектирования (разработки проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

5.1.1. На предпроектной стадии по обследованию ИСПДн проводятся следующие мероприятия:

первичное (предпроектное) обследование ИСПДн, включающее в себя сбор данных об объекте (ах) и осуществляемых видах деятельности;

устанавливается необходимость обработки ПДн в ИСПДн;

определяется перечень ПДн, подлежащих защите от НСД;

определяются условия расположения ИСПДн относительно границ контролируемой зоны (КЗ);

определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИСПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

определяются режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;

определяется класс ИСПДн;

уточняется степень участия персонала в обработке ПДн, характер их взаимодействия между собой;

определяются (уточняются) угрозы безопасности ПДн к конкретным условиям функционирования (разрабатывается частная модель угроз).

По результатам предпроектного обследования, с учетом установленного класса ИСПДн, задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

обоснование разработки СЗПДн;

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

класс ИСПДн;

ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн;

конкретизацию мероприятий и требований к СЗПДн;

перечень предполагаемых к использованию сертифицированных средств защиты информации;

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

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

5.1.2. На стадии проектирования и создания ИСПДн (СЗПДн) проводятся следующие мероприятия:

разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

разработка раздела технического проекта на ИСПДн в части защиты информации;

строительно-монтажные работы в соответствии с проектной документацией;

использование серийно выпускаемых технических средств обработки, передачи и хранения информации;

разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

использование сертифицированных технических, программных и программно-технических средств защиты информации и их установка;

сертификация по требованиям безопасности информации программных средств защиты информации в случае, когда на рынке отсутствуют требуемые сертифицированные средства защиты информации;

разработка и реализация разрешительной системы доступа пользователей к обрабатываемой на ИСПДн информации;

определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации, их обучение по направлению обеспечения безопасности ПДн;

разработка эксплуатационной документации на ИСПДн и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов);

выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

5.1.3. На стадии ввода в действие ИСПДн (СЗПДн) осуществляются:

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

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки ПДн;

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

организация охраны и физической защиты помещений ИСПДн, исключающих несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

оценка соответствия ИСПДн требованиям безопасности ПДн.

5.1.3.1. Основанием для оценки достаточности принятых мер и соответствия ИСПДн требованиям по обеспечению безопасности ПДн является:

для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация) по требованиям безопасности информации;

для ИСПДн 3 класса - декларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению оператора);

для ИСПДн 4 класса - оценка соответствия проводится по решению оператора.

Приложение № 1

к Положению о персональных данных субъектов персональных данных мэрии города

_____
(наименование (должность) оператора)

_____
(фамилия, имя, отчество оператора)

_____
(адрес оператора)

ЗАЯВЛЕНИЕ (согласие)

Я, _____
(фамилия, имя, отчество)

Адрес места жительства _____
(город, улица, дом, корпус, квартира)

_____

Документ, удостоверяющий личность _____ _____ _____
(наименование) (серия) (номер)

_____ _____
(кем выдан) (дата выдачи)

даю свое согласие на обработку моих персональных данных (далее - ПДн) в целях обеспечения реализации полномочий органа местного самоуправления (иного органа) и обязательств, связанных с обеспечением выполнения трудового договора, предоставлением социальных гарантий, защитой моего здоровья (указывается при необходимости), а также в иных, предусмотренных законодательством Российской Федерации случаях (или указать их подробно).

_____
(наименование целей предоставления персональных данных)

Мое согласие распространяется на ПДн, содержащиеся в заявлениях и документах, предоставляемых мной оператору (лицу, уполномоченному для их обработки), и не распространяется на специальные категории ПДн (при необходимости указать иное или перечислить ПДн подробно).

_____
(перечень персональных данных, на обработку которых дается согласие)

Я согласен: на сбор, систематизацию, накопление, хранение, уточнение, использование, обезличивание, блокирование, уничтожение и передачу третьим лицам, в предусмотренных законодательством Российской Федерации случаях моих ПДн, в том числе с применением средств автоматизированной обработки (указывается при необходимости), при условии обработки ПДн в указанных целях и обеспечения их защиты и сохранности оператором.

_____
(перечень действий с персональными данными)

Согласие действует в течение всего срока моей работы в мэрии города (ином органе или указать иной срок).

Мне разъяснены мои права и обязанности, связанные с обработкой ПДн, в том числе мое право отозвать согласие путем направления письменного заявления оператору и последствия его отзыва.

_____
(срок, в течение которого действует согласие, а также порядок его отзыва)

Подпись заявителя_____ Дата _____

Приложение № 2
к Положению о персональных данных субъектов
персональных данных мэрии города

УТВЕРЖДАЮ

Должность оператора,
фамилия и инициалы, дата

СПИСОК
работников, допущенных к обработке персональных данных

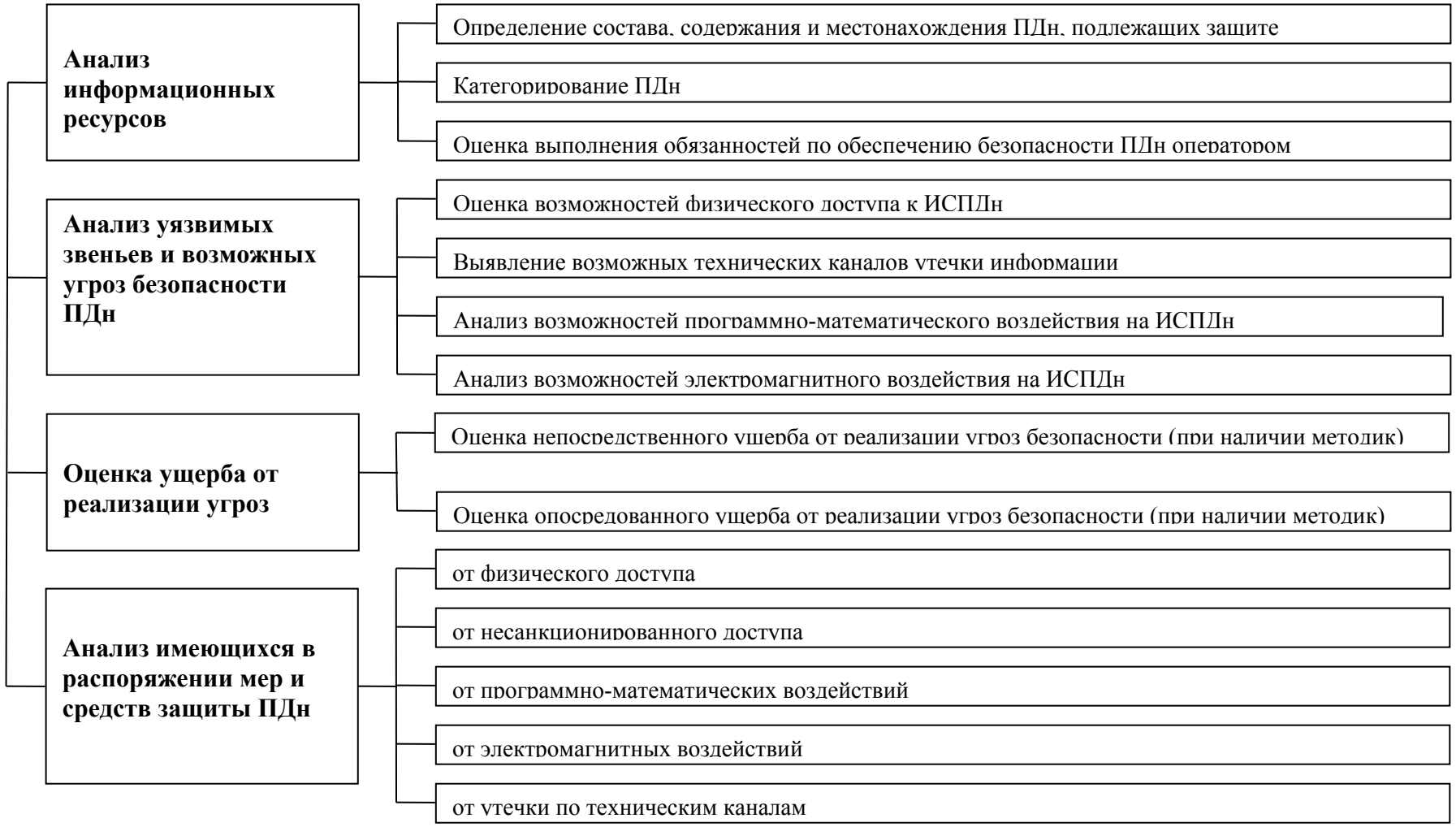
_____
(наименование органа мэрии города)

№ п.п.	Наименование носителей сведений, содержащих ПДн	Должность	Фамилия, имя, отчество	Выполняемые функции (основания)	Контактный телефон	Расположение рабочего места (адрес, № кабинета)	Вид обработки
1	2	3	4	5	6	7	8
1.	Личные дела, трудовые книжки и т.п. ИР: Кадровый учет	Начальник управления муниципальной службы и кадров	Иванов Петр Олегович	Кадровая работа (положение об управлении)	60-72-12	Пл. Ленина,5 каб. № 201	Комбинированная
2.	ИР: Регистр больных …	Главный специалист департамента здравоохранения и социальной политики	Мартынова Анна Ивановна	Ведение регистра (приказ начальника управления от 12.11.2008 № 12)	60-70-11	Пл. Ленина,5 каб. № 312, 201	Автоматизированная
3.	Штатные расписания, ИР: Зарплата	Начальник отдела учета и отчетности	Васильева Наталья Федоровна	Начисление зарплаты и иных выплат (положение об отделе)	60-45-11	Пл. Ленина,5 каб. № 201	Комбинированная
4.	Личные дела, трудовые книжки и т.п.	Главный специалист отдела кадров управления муниципальной службы и кадров	Богданова Светлана Ивановна	Ведение личных дел (должностная инструкция)	60-72-89	Пл. Ленина,5 каб. № 201	Работа с бумажными носителями ПДн

_____

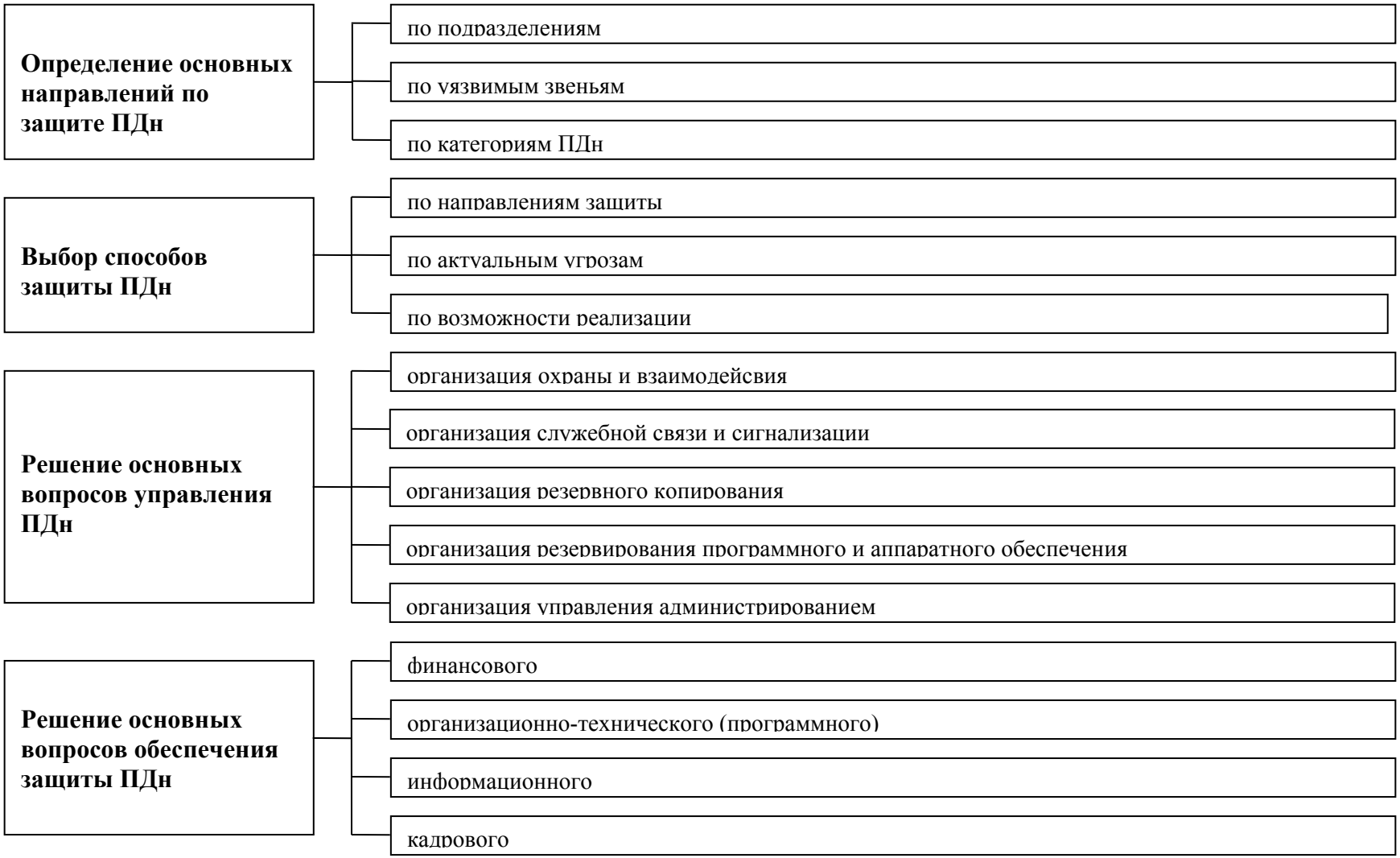
Приложение № 1
к Положению об организации проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных мэрии города

ОЦЕНКА ОБСТАНОВКИ



Приложение № 2
к Положению об организации проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных мэрии города

Определение замысла обеспечения безопасности ПДн при их обработке в ИСПДн



Начальник управления ВМР и АО

Ю.В. Агеев

"____ " _____ 2009 г.

Исп. в 1-ом экз. - в общий отдел
Исп. и отп. Титов
60-71-64
10.07.2009

Начальник управления ВМР и АО

Ю.В. Агеев

"____ " _____ 2009 г.

Отп. 1 экз.- общий отдел
Исп. и отп. Титов
60 71 64
10.07.2009