Приложение 1
к постановлению
Мэрии г. Грозного
от «14» 12 2012г. № 99

Правила обработки персональных данных в Мэрии г. Грозного

1. Общие положения

1. Настоящие Правила обработки персональных данных в Мэрии г. Грозного, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Мэрии г. Грозного разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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», и иными нормативными правовыми актами Российской Федерации, регулирующими отношения в данной сфере деятельности (далее - Правила).

2. Правила устанавливают единый порядок действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными в Мэрии г. Грозного, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в Мэрии г. Грозного.

3. Целью Правил является обеспечение защиты прав и свобод при обработке персональных данных работников Мэрии г. Грозного, а также граждан, обратившихся в Мэрию г. Грозного (далее - субъект персональных данных), установление ответственных должностных лиц Мэрии г. Грозного, имеющих доступ к персональным данным, ответственности за невыполнение норм, регулирующих обработку и защиту персональных данных.

4. В Правилах используются основные понятия, установленные статьей 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее - Федеральный закон №152-ФЗ).

5. Ответственные должностные лица Мэрии г. Грозного, должности которых предусматривают осуществление обработки персональных данных

либо осуществление доступа к персональным данным (далее - ответственные лица Мэрии г. Грозного) определяются распоряжением Мэрии г. Грозного.

6. Обработка персональных данных в Мэрии г. Грозного осуществляется на основе принципов, установленных статьей 5 Федерального закона №152-ФЗ.

7. Мерами, направленными на выявление и предотвращение нарушений,

МЭРИЯ ГОРОДА ГРОЗНОГО

ПОСТАНОВЛЕНИЕ

14.12.2012 г. № 99

О мерах по обеспечению безопасности персональных данных при их обработке в Мэрии г. Грозного

В соответствии с Федеральным законом от 27.07.2012 №152-ФЗ «О персональных данных», 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», Мэрия города Грозного

ПОСТАНОВЛЯЕТ:

1. Утвердить Правила обработки персональных данных в Мэрии г. Грозного согласно приложению 1.

2. Утвердить Модель угроз безопасности персональных данных при их обработке в Мэрии г. Грозного согласно приложению 2.

3. Контроль за исполнением настоящего постановления возложить на заместителя Мэра – руководителя аппарата Мэрии г. Грозного В.Ш. Устраханова.

4. Настоящее постановление вступает в силу со дня его опубликования в грозненской городской газете «Столица плюс» и подлежит размещению на официальном сайте Мэрии г. Грозного.

7) в случае, если для предоставления муниципальной услуги необходимо представление документов и информации об ином лице, не являющемся заявителем, при обращении за получением муниципальной услуги заявитель дополнительно представляет документы, подтверждающие наличие согласия указанных лиц или их законных представителей на обработку персональных данных указанных лиц, а также полномочие заявителя действовать от имени указанных лиц или их законных представителей при передаче персональных данных указанных лиц в Мэрию г. Грозного;

8) запрещается получать, обрабатывать и приобщать к личному делу субъекта персональных данных не установленные Федеральным законом от 02.03.2007 №25-ФЗ «О муниципальной службе в Российской Федерации» и Федеральным законом №152-ФЗ персональные данные;

9) при принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

2. При передаче персональных данных ответственные лица Мэрии г. Грозного обязаны соблюдать следующие требования:

1) не сообщать персональные данные субъекта персональных данных без его письменного согласия для использования их в коммерческих целях;

2) предупреждать лиц, получающих персональные данные субъекта персональных данных, о том, что эти данные должны использоваться только в целях, для которых они сообщены, и требовать от этих лиц подтверждения о соблюдении требований;

3) передавать персональные данные субъекта персональных данных его представителю в порядке, установленном федеральными законами, и ограничивать эту информацию только теми персональными данными субъекта персональных данных, которые необходимы для выполнения представителем его функций.

3. Передача персональных данных от Мэрии г. Грозного иному оператору персональных данных допускается в минимальных объемах, в целях выполнения задач, соответствующих объективной причине сбора этих данных, и только после заключения с этим оператором договора о соблюдении конфиденциальности.

4. Не допускается отвечать на вопросы, связанные с передачей персональных данных по телефону или факсу.

5. Ответственные лица Мэрии г. Грозного при обработке персональных данных с использованием информационных систем обязаны:

- принимать меры, исключающие несанкционированный доступ к используемым программно-техническим средствам;

- вести учет электронных носителей информации (включая резервные и архивные копии), осуществлять хранение документов, содержащих персональные данные, и электронных носителей информации в металлических шкафах или сейфах;

- производить запись персональных данных (отдельных файлов, баз данных) на электронные носители только в случаях, регламентированных порядком работы с данными сведениями;

- соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей;

- принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам;

- работать с информационными системами в объеме своих полномочий, не допускать их превышения;

- обладать навыками работы с антивирусными программами в объеме, необходимом для выполнения функциональных обязанностей и требований по защите информации.

6. При работе на персональном компьютере, в том числе для доступа к информационным системам, запрещается:

- записывать значения кодов и паролей доступа;

- передавать коды и пароли доступа другим лицам;

- пользоваться в работе чужими кодами и паролями доступа;

- производить подбор кодов и паролей доступа других пользователей; записывать на электронные носители с персональными данными посторонние программы и данные;

- копировать данные на неучтенные электронные носители информации;

- выносить электронные носители с персональными данными за пределы Мэрии г. Грозного без согласования с руководством Мэрии г. Грозного;

- покидать рабочее место с включенным персональным компьютером без применения аппаратных или программных средств, блокирования доступа к персональному компьютеру;

- приносить, самостоятельно устанавливать и эксплуатировать на технических средствах любые программные продукты, не принятые к эксплуатации;

- открывать, разбирать, ремонтировать технические средства, вносить изменения в конструкцию, подключать нештатные блоки и устройства;

- передавать технические средства для ремонта и обслуживания сторонним организациям без извлечения носителей, содержащих персональные данные.

7. Все документы, компакт-диски, флеш-накопители, содержащие персональные данные, подлежат уничтожению на основании актов только с применением соответствующих уничтожителей.

8. Мэрия г. Грозного при обработке персональных данных в информационных системах персональных данных обеспечивает:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которых нарушается их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности персональных данных.

9. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

1) настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;

2) охраны и организации режима допуска в помещения Мэрии г. Грозного, предназначенные для обработки персональных данных;

3) организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации информационных систем персональных данных, инструкции пользователя, администратора по организации антивирусной защиты, парольной защиты автоматизированных систем и методических документов.

3. Особенности обработки персональных данных без использования средств автоматизации

1. Обработка и защита персональных данных в информационных системах персональных данных Мэрии г. Грозного без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) осуществляется в соответствии с Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 №687.

2. Неавтоматизированная обработка персональных данных осуществляется на бумажных носителях в виде документов и в электронном виде (файлы, базы данных) на электронных носителях информации.

3. При неавтоматизированной обработке персональных данных:

1) не допускается фиксация на одном бумажном носителе персональных данных цели обработки которых заведомо не совместимы;

2) персональные данные обособляются от иной информации, в частности, путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

3) документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

4) дела с документами, содержащими персональные данные, имеют внутренние описи документов с указанием цели обработки и категории персональных данных.

4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

1) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

2) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

3) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные и технические меры, исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

1) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

2) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

10. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, со сроком хранения.

4. Особенности обработки персональных работников Мэрии г. Грозного

1. Защита персональных данных работников Мэрии г. Грозного обеспечивается мерами, включающими в себя контроль за соблюдением установленных требований, обеспечение режима безопасности в помещениях, в которых ведется обработка персональных данных, содержащихся в личных делах, а также в электронном виде в информационных системах, обеспечение сохранности носителей персональных данных и средств их защиты, исключение несанкционированного проникновения или пребывания в этих помещениях посторонних лиц, контроль за эффективностью предусмотренных мер защиты.

2. Персональные данные и иные сведения, содержащиеся в личных делах работников Мэрии г. Грозного, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации), а в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, - к сведениям, составляющим государственную тайну.

3. Личные дела работников Мэрии г. Грозного хранятся в специальных металлических шкафах, которые в конце рабочего дня опечатываются. Помещения (комнаты), в которых находятся шкафы, оборудованы охранной и пожарной сигнализацией, дверью с запорным устройством. По окончании рабочего дня указанные помещения опечатываются.

4. Личные дела уволенных работников Мэрии г. Грозного хранятся в отделе кадровой политики аппарата Мэрии г. Грозного в течение 10 лет со дня увольнения, после чего передаются на хранение в муниципальный архив.

5. Обработка персональных данных муниципальных служащих Мэрии г. Грозного осуществляется в соответствии с Положением о порядке хранения и использования персональных данных муниципальных служащих Мэрии г. Грозного, утверждённым постановлением Мэрии г. Грозного от 14.10.2010 №71.

5. Заключительные положения

1. Должностные лица Мэрии г. Грозного, виновные в нарушении норм и требований действующего законодательства, регулирующих обработку и защиту персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.

Приложение 2
к постановлению
Мэрии г. Грозного
от «14» 12 2012г. №99

Модель угроз безопасности персональных данных
при их обработке в Мэрии г. Грозного

1. Общие положения

1. Данная частная модель безопасности персональных данных при их обработке в Мэрии г. Грозного (далее – Модель угроз) определяет угрозы безопасности персональных данных при их обработке в информационной системе персональных данных Мэрии г. Грозного (далее – ИСПДн) и разработана на основании:

Базовой модели угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденной 15.02.2008 ФСТЭК Российской Федерации;

Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14.02.2008 ФСТЭК Российской Федерации (далее – Методика);

ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», утверждённым Приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 №374-ст.

2. Перечень угроз, представляющих потенциальную опасность
для персональных данных, обрабатываемых в ИСПДн

Потенциальную опасность безопасности персональных данных (далее – ПДн) при их обработке в ИСПДн представляют:

1. Угрозы утечки информации по техническим каналам:

1) угроза утечки видовой информации;

2) угроза утечки информации по каналу ПЭМИН (побочные электромагнитные излучения и наводки).

2. Угрозы несанкционированного доступа к информации:

1) угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

- кража ПЭВМ;
- кража носителей информации;
- кража ключей и атрибутов доступа;
- кражи, модификации, уничтожения информации;
- вывод из строя узлов ПЭВМ, каналов связи.

2) угрозы хищения, несанкционированной модификации или

блокирования информации за счет несанкционированного доступа (далее - НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):

- действия вредоносных программ (вирусов);

- недекларированные возможности системного программного обеспечения (далее – ПО) и ПО для обработки персональных данных;

- установка ПО не связанного с исполнением служебных обязанностей.

3) угрозы преднамеренных действий внутренних нарушителей:

- доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;

- разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

4) угрозы несанкционированного доступа по каналам связи:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

- угрозы выявления паролей по сети;

- угрозы типа «Отказ в обслуживании»;

- угрозы удаленного запуска приложений;

- угрозы внедрения по сети вредоносных программ.

3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн в ее составе из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:

- утрата ключей и атрибутов доступа;

- непреднамеренная модификация (уничтожение) информации сотрудниками;

- непреднамеренное отключение средств защиты;

- выход из строя аппаратно-программных средств;

- сбой системы электроснабжения;

- стихийное бедствие.

Анализ вероятности реализации, реализуемости, опасности и актуальности угроз представлен в Модели угроз.

3. Определение актуальных угроз безопасности ПДн при обработке в ИСПДн

1. Определение уровня исходной защищенности ИСПДн.

Уровень исходной защищенности ИСПДн определен экспертным методом в соответствии с Методикой. Результаты анализа исходной защищенности приведены в таблице 1.

Таблица 1

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
	+		
2. По наличию соединения с сетями общего пользования:			
		+	
3. По встроенным (легальным) операциям с записями баз ПДн:			
		+	
4. По разграничению доступа к ПДн:			
		+	
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
	+		
6. По уровню обобщения (обезличивания) ПДн:			
			+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
		+	
Характеристики ИСПДн	28,57%	57,14%	14,29%

Таким образом, ИСПДн имеет *средний* (Y_1=*5)* уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню защищенности не ниже «средний».

2. Определение частоты реализации угроз безопасности ПДн.

Частота реализации угроз безопасности ПДн определена экспертным методом в соответствии Методикой и на основании результатов обследования ИСПДн. Результаты определения частоты реализации угроз, приведены в таблице 2.

Таблица 2

Угроза	Анализ реализации мер защиты	Частота (вероятность) реализации угрозы (Значение коэффициента Y_2)	Коэффициент реализуемости угрозы Y. Возможность реализации угрозы
Угрозы утечки информации по техническим каналам			
		низкая вероятность (2)	0,35 средняя
Угрозы НСД			
		низкая вероятность (2)	0,35 средняя
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
		маловероятно (0)	0,25 низкая

3. Определение опасности угроз безопасности ПДн.

Определение опасности угроз безопасности ПДн проведено экспертным методом с учетом результатов обследования ИСПДн. Результаты определения опасности угроз с мнениями экспертов приведены в таблице 3.

Таблица 3

Угроза	Факторы, определяющие опасность угрозы	Показатель опасности угрозы
1	2	3
Угрозы утечки информации по техническим каналам		
		средняя опасность
Угрозы НСД		
		высокая опасность
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн		
		низкая опасность

4. Определение актуальных угроз безопасности ПДн.

Определение актуальных угроз безопасности ПДн проведено экспертным методом в соответствии с Методикой. Результаты приведены в таблице 4.

Таблица 4

Угроза	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Угрозы утечки информации по техническим каналам			
	средняя	средняя	актуальная
Угрозы НСД			
	средняя	высокая	актуальная
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средств защиты ПДн			
	низкая	низкая	неактуальная

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн Мэрии г. Грозного, актуальными являются следующие угрозы безопасности:

- угрозы утечки информации по техническим каналам;
- угрозы несанкционированного доступа к информации.