1. Приказ о назначении ответственного за организацию обработки персональных данных

ПРОЕКТ ПРИКАЗА

О назначении ответственн(ых)ого за
организацию обработки персональных данных
_____

В соответствии с пунктом 1 постановления 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", **приказываю**:

1. Назначить _____ответственн(ых)ого за организацию обработки персональных данных в _____.

2. Утвердить инструкцию лица(м), ответственн(ым)ого за организацию обработки персональных данных (Приложение 1).

3. Контроль за исполнением настоящего Приказа оставляю за собой.

Руководитель _____

2. ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Обработка персональных данных в_____ должна осуществляться на законной основе.

2. Обработка персональных данных в _____ должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

Ответственный за осуществление обработки персональных данных в _____, должен принимать необходимые меры по удалению или уточнению неполных или неточных персональных данных.

7. Мерами, направленными на выявление и предотвращение нарушений, предусмотренных законодательством, являются:

1) осуществление внутреннего контроля соответствия обработки персональных данных нормам Федерального закона 27.07.2006 № 152-ФЗ "О персональных данных" (далее - Федеральный закон) и принятым в соответствии с ним нормативным правовым актам;

2) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых _____мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

3) ознакомление служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, и(или) обучение служащих.

8. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) проведением в установленном порядке процедуры оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер по их недопущению;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

9. Целью обработки персональных данных в _____ является обеспечение соблюдения законов и иных нормативных правовых актов.

10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом, договором, стороной которого является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

11. В случае выявления неправомерной обработки персональных данных, осуществляемой служащим, в срок, не превышающий три рабочих дня с даты этого выявления, он обязан прекратить неправомерную обработку персональных данных.

В случае если обеспечить правомерность обработки персональных данных невозможно, работник в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

Об устранении допущенных нарушений или об уничтожении персональных данных работник обязан уведомить субъекта персональных данных или его представителя, а в случае если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12. В случае достижения цели обработки персональных данных государственный гражданский работник обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между _____и субъектом персональных данных либо если _____ не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных, на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

13. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных работник обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий три рабочих дня с даты поступления указанного отзыва, если иное не предусмотрено соглашением между _____и субъектом персональных данных.

Об уничтожении персональных данных государственный работник обязан уведомить субъекта персональных данных не позднее трех рабочих дней со дня уничтожения.

14. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных выше, работник осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий шесть месяцев, если иной срок не установлен федеральными законами.

3. ПРАВИЛА РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

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

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

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

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

7) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора 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. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Запрос 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 оператором (номер договора, дата заключения договора, условное словесное обозначение и(или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, 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.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае если такие сведения и(или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

4. ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в _____организовывается проведение периодических проверок условий обработки персональных данных.

2. Проверки осуществляются ответственным за организацию обработки персональных данных в _____ либо комиссией, образуемой распоряжением_____.

3. В проведении проверки не может участвовать работник, прямо или косвенно заинтересованный в ее результатах.

4. Проверки соответствия обработки персональных данных установленным требованиям в _____ проводятся на основании утвержденного ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в _____письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне определены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

6. Ответственный за организацию обработки персональных данных в _____ (комиссия) имеет право:

- запрашивать у работников_____, необходимую для реализации полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю _____предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить руководителю _____предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

7. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в _____ (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

8. Проверка должна быть завершена не позднее чем через десять дней со дня принятия решения о ее проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю _____докладывает ответственный за организацию обработки персональных данных либо председатель комиссии в форме письменного заключения.

Контроль за своевременностью и правильностью проведения проверки возлагается на_____.

5. ПРАВИЛА
работы с обезличенными персональными данными

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

2.Настоящие Правила определяют порядок работы с обезличенными данными Организации.

3.Настоящие Правила утверждаются руководителем организации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

2.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;

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

3. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

1.Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.Способы обезличивания при условии дальнейшей обработки персональных данных:

-замена части сведений идентификаторами;

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

-другие способы.

3.Перечень должностей _____, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в Приложении к настоящим Правилам;

-решение о необходимости обезличивания персональных данных принимает руководитель организации;

-руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания;

-сотрудники подразделений, обслуживающих базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

4. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ

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

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

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

-парольной политики;

-антивирусной политики;

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

-правил резервного копирования;

-правил доступа в помещения, где расположены элементы информационных систем;

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

-правил хранения бумажных носителей;

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

6.ПЕРЕЧЕНЬ
информационных систем персональных данных (ИСПДн), в которых должна быть обеспечена безопасность информации

№ п/п	Наименование ИСПДн (ее составной части)	Наименование объекта (полное и сокращенное) Отраслевая принадлежность Адрес объекта	Исходные данные классификации ИСПДн					Уровень защищенности ИСПДн	Примечание
			Структура ИСПДн	Наличие подключений к ССОП и сетям МИО (Интернет)	Режим обработки ПДн	Разграничение доступа пользователей	Нахождение ИСПДн (ее составных частей) в пределах России		
1	2	3	4	5	6	7	8	9	10
1.	Автоматизированная система "Кадры"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	С разграничением прав пользования	Все технические средства находятся на территории Российской Федерации	1	

2.	Автоматизированная система "Смета"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Локальная информационная система	Отсутствует	Многопользовательский	С разграничением прав пользования	Все технические средства находятся на территории Российской Федерации	3	
3.	Автоматизированная система "Назначение пособий по уходу за ребенком до 1,5 лет"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	Без разграничения прав пользования	Все технические средства находятся на территории Российской Федерации	3	
4.	ОГБД	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	Без разграничения прав пользования	Все технические средства находятся на территории Российской Федерации	3	

5.	ЕДВ	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Локальная информационная система	Отсутствует	Многопользовательский	Без разграничения прав пользования	Все технические средства находятся на территории Российской Федерации	3	
6.	Автоматизированная система "Назначение ежемесячного пособия по уходу за ребенком"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	Без разграничения прав пользования	Все технические средства находятся на территории Российской Федерации	2	
7.	Автоматизированная система "Сельское административное образование"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	С разграничением прав пользования	Все технические средства находятся на территории Российской Федерации	4	Обезличенные данные

8.	Автоматизированная система "Семья"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	С разграничением прав пользования	Все технические средства находятся на территории Российской Федерации	1	
9.	Автоматизированная система "Социальный регистр"	Муниципальное образование город Пушкин Администрация муниципального образования. Отрасль – муниципальная служба. 196600, Санкт-Петербург, г. Пушкин, Октябрьский бул., 24	Автоматизированное рабочее место	Отсутствует	Однопользовательский	С разграничением прав пользования	Все технические средства находятся на территории Российской Федерации	1	

7. ПЕРЕЧНИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В _____ В СВЯЗИ С РЕАЛИЗАЦИЕЙ ТРУДОВЫХ ОТНОШЕНИЙ, А ТАКЖЕ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ГОСУДАРСТВЕННЫХ ФУНКЦИЙ

Персональные данные лиц, замещающих должности в _____,
фамилия, имя, отчество;
информация о смене фамилии, имени, отчества;
пол;
дата рождения;
место рождения;
гражданство;
документ, удостоверяющий личность (серия, номер, когда и кем выдан);
сведения из записей актов гражданского состояния;
место жительства и дата регистрации по месту жительства;
номера контактных телефонов;
семейное положение;
состав семьи;
сведения о наличии детей, их возрасте, месте учебы (работы);
сведения, содержащиеся в служебном контракте, гражданско-правовом договоре;
отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах;
сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, квалификации, наименование документа об образовании, его серия и номер, дата выдачи);
сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка);
сведения о профессиональной переподготовке, повышении квалификации, стажировке;
сведения о трудовой деятельности, общем трудовом стаже и стаже государственной гражданской службы;
сведения о замещаемой должности;
сведения о классных чинах, военных и специальных званиях;
сведения о состоянии здоровья и его соответствии выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности;
сведения об отпусках и командировках;
сведения о прохождении аттестации и сдаче квалификационного экзамена;
сведения в 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;
сведения о награждении (поощрении);
материалы служебных проверок, расследований;
сведения о взысканиях;

реквизиты идентификационного номера налогоплательщика (ИНН);
реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);
реквизиты полиса обязательного медицинского страхования;
сведения о доходах, имуществе и обязательствах имущественного характера государственного гражданского служащего и членов его семьи;
сведения о социальных льготах;
информация о доходах, выплатах и удержаниях;
номера банковских счетов;
фото
Персональные данные граждан, включенных в кадровый резерв _____ граждан, не допущенных к участию в конкурсах, и граждан, участвовавших в конкурсах, но не прошедших конкурсный отбор:
фамилия, имя, отчество;
информация о смене фамилии, имени, отчества;
пол;
дата рождения;
место рождения;
гражданство;
документ, удостоверяющий личность (серия, номер, когда и кем выдан);
место жительства и дата регистрации по месту жительства; номера контактных телефонов;
семейное положение;
состав семьи;
сведения о наличии детей, их возрасте, месте учебы (работы);
отношение к воинской обязанности, воинское звание;
состав рода войск, военный билет, приписное свидетельство, сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах;
сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, квалификации, наименование документа об образовании, его серия и номер, дата выдачи);
сведения об уровне специальных знаний (работа на компьютере, знание иностранного языка);
сведения о профессиональной переподготовке, повышении квалификации, стажировке; сведения о трудовой деятельности, общем трудовом стаже и стаже государственной гражданской службы;
сведения о замещаемой должности;
сведения о классных чинах, военных и специальных званиях;
сведения о состоянии здоровья и его соответствии выполняемой работе, наличии группы инвалидности и степени ограничения способности к трудовой деятельности;
сведения о награждении (поощрении);
реквизиты идентификационного номера налогоплательщика;
реквизиты страхового номера индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС);
фото
Персональные данные граждан, обрабатываемые в связи с рассмотрением обращений граждан:
фамилия, имя, отчество;
адрес места жительства;

иные персональные данные, содержащиеся в обращениях граждан
Персональные данные граждан, обрабатываемые при подготовке и оформлении документов по представлению к награждению государственными наградами Российской Федерации, наградами Санкт-Петербурга и присвоению почетных званий Санкт-Петербурга
фамилия, имя, отчество;
пол;
дата рождения;
место рождения;
документ, удостоверяющий личность (серия, номер, когда и кем выдан);
место жительства и дата регистрации по месту жительства;
семейное положение;
состав семьи;
сведения о наличии детей, их возрасте, месте учебы (работы);
сведения о получении профессионального и дополнительного образования (наименование образовательного учреждения, специальность и квалификация по документу об образовании);
сведения о трудовой деятельности;
сведения о замещаемой должности;
сведения о прохождении аттестации и сдаче квалификационного экзамена;
сведения о награждении (поощрении);
иные персональные данные, содержащиеся в представлениях к награждению

8. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ РАБОТНИКОВ_____, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Управление государственной службы и кадров	
	Руководитель управления
	заместитель руководителя управления – Руководитель отдела кадров
сектор по профилактике коррупционных и иных правонарушений	Руководитель сектора
отдел подбора, обучения и оценки персонала	Руководитель отдела
сектор подготовки кадров	Руководитель сектора
сектор наград	Руководитель сектора
отдел государственной и муниципальной службы	консультант, осуществляющий в соответствии с должностным регламентом обязанности ответственного секретаря комиссии по установлению стажа государственной службы и доплате к пенсиям при Губернаторе Санкт-Петербурга
Управление делопроизводства	
отдел по работе с обращениями граждан	Руководитель отдела

9. ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ РАБОТНИКОВ В _____, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

Управление государственной службы и кадров	
	Руководитель управления
	заместитель руководителя управления - Руководитель отдела кадров
отдел кадров	заместитель руководителя отдела
	консультант
	главный специалист
	ведущий специалист
	специалист первой категории
сектор по профилактике коррупционных и иных правонарушений	Руководитель сектора
	главный специалист
отдел подбора, обучения и оценки персонала	Руководитель отдела
	консультант
	главный специалист
сектор подготовки кадров	Руководитель сектора
	главный специалист
отдел государственной и муниципальной службы	консультант, осуществляющий в соответствии с должностным регламентом обязанности ответственного секретаря комиссии по установлению стажа государственной службы и доплате к пенсиям при Губернаторе Санкт-Петербурга
Управление делопроизводства	
отдел по работе с обращениями граждан	Руководитель отдела
	консультант
	главный специалист
	ведущий специалист
	специалист первой категории

10. ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Должностная инструкция ответственного за организацию обработки персональных данных (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан 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", другими нормативными правовыми актами.

2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки персональных данных.

3. Ответственный за организацию обработки персональных данных отвечает за осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений работников соответствующих структурных подразделений положений законодательства Российской Федерации о персональных данных, правовых актов _____по вопросам обработки персональных данных, требований к защите персональных данных, организации приема и обработки обращений и осуществлению контроля за приемом и обработкой таких обращений.

4. Ответственный за организацию обработки персональных данных обязан:

- определить порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- определять порядок и условия применения средств защиты информации;
- анализировать эффективность применения мер по обеспечению безопасности персональных данных;
- контролировать состояние учета машинных носителей персональных данных;
- проверять соблюдение правил доступа к персональным данным;

- контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

5. Ответственный за организацию обработки персональных данных имеет право:

- осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных;

- запрашивать у сотрудников Комитета информацию, необходимую для реализации полномочий;

- требовать от ответственных должностных лиц за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- применять меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю_____ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить руководителю_____ предложения о привлечении к дисциплинарной ответственности работников _____, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

11. ТИПОВОЕ ОБЯЗАТЕЛЬСТВО РАБОТНИКА, НЕПОСРЕДСТВЕННО ОСУЩЕСТВЛЯЮЩЕГО ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, В СЛУЧАЕ РАСТОРЖЕНИЯ С НИМ СЛУЖЕБНОГО КОНТРАКТА ПРЕКРАТИТЬ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, СТАВШИХ ИЗВЕСТНЫМИ ЕМУ В СВЯЗИ С ИСПОЛНЕНИЕМ ДОЛЖНОСТНЫХ ОБЯЗАННОСТЕЙ

Я,

_____,

(фамилия, имя, отчество полностью)

являясь работником_____,

_____

_____,

(указать наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (трудового договора).

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

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

_____ _____ "___" _____ 201_ г.

(фамилия, инициалы) (подпись)

12.Типовая форма согласия на обработку персональных данных,

СОГЛАСИЕ
на обработку персональных данных

Согласие на обработку персональных данных			
(информация о субъекте персональных данных)			
Я			
	(фамилия)	(имя)	(отчество)
(основной документ, удостоверяющий личность)		(номер основного документа, удостоверяющего личность)	
(сведения о дате выдачи указанного документа)		(сведения о выдавшем указанный документ органе)	
зарегистрированный по адресу:			
		(адрес)	
(информация о представителе субъекта персональных данных)			
Я			
	(фамилия)	(имя)	(отчество)
(основной документ, удостоверяющий личность)		(номер основного документа, удостоверяющего личность)	
(сведения о дате выдачи указанного документа)		(сведения о выдавшем указанный документ органе)	
зарегистрированный по адресу:			
		(адрес)	
наименование и реквизиты документа, подтверждающего полномочия представителя: >			
принимаю решение о предоставлении своих персональных данных в составе:			
(перечень персональных данных, на обработку которых дается согласие субъекта персональных данных)			
(в случае обработки специальных категорий персональных данных работника)			
сведения о состоянии здоровья сотрудника в объеме сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции			
сведения о наличии судимости			
(в случае обработки биометрических персональных данных)			

личная подпись
фотография
и даю согласие на их обработку, включающую:
1. сбор
2. запись
3. систематизацию
4. накопление
5. хранение
6. уточнение (обновление)
7. уточнение (изменение)
8. извлечение
9. использование
10. передачу (предоставление)
11. передачу (доступ)
12. обезличивание
13. блокирование
14. удаление
15. уничтожение
(в случае обработки общедоступных персональных данных)
16. передачу (распространение)
персональных данных
(перечень действий с персональными данными, на совершение которых дается согласие)
способами, определяемыми (перечислить договоры, регламенты, правила, инструкции и положения, которые определяют работу в информационных системах персональных данных и программных продуктах таких систем) или
(перечислить способы обработки и в каких информационных системах персональных данных производится обработка персональных данных)
(общее описание используемых оператором способов обработки персональных данных)
своей волей и в своем интересе Комитету по информатизации и связи расположенному по адресу: Смольный, Санкт-Петербург, 191060
(информация о лице, осуществляющем обработку персональных данных по поручению Комитета по информатизации и связи)
(наименование или фамилия, имя, отчество лица, осуществляющего обработку персональных данных по поручению Комитета по информатизации и связи)
(адрес лица, осуществляющего обработку персональных данных по поручению Комитета по информатизации и связи)
с целью:
(цель или цели обработки персональных данных)
создания общедоступного источника персональных данных
на срок:

	(срок, в течение которого действует согласие)

Порядок отзыва согласия:

Отзыв согласия подается в письменном виде лицом, указанным в согласии на обработку персональных данных, лично. Отзыв должен содержать:
- номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- собственноручную подпись субъекта персональных данных;
- сведения о согласии на обработку персональных данных (дата и адрес, по которому давалось согласие).

При подаче лицом, осуществляющим прием такого отзыва, производится удостоверение личности подающего такой отзыв.
Отзыв согласия осуществляется по адресу:

В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекращение обработки персональных данных и уничтожение персональных данных будет произведено в течение 30 дней с момента поступления

Порядок защиты субъектом персональных данных своих прав и законных интересов:

осуществляется в соответствии с требованиями Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ

(в случае если обязанность предоставления персональных данных установлена федеральным законом)

Юридические последствия отказа предоставить свои персональные данные, если обязанность предоставления персональных данных установлена федеральным законом:

(в случае исключительно автоматизированной обработки данных)

Порядок принятия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:

Возможные юридические последствия решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных:

Порядок защиты субъектом персональных данных своих прав и законных интересов

("я возражаю против решения исключительно автоматизированной обработки моих персональных данных" - заполняется собственноручно в случае такого возражения)

Наименование оператора, которому будут передаваться персональные данные

Адрес оператора, которому будут передаваться персональные данные

Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных

Срок, в течение которого действует согласие на передачу

(в случае обработки общедоступных персональных данных)

Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов

(в случае трансграничной передачи персональных данных)								
Наименование оператора, которому будут передаваться персональные данные								
Иностранные государства, которым будут передаваться персональные данные								
Цель передачи персональных данных								
Перечень персональных данных, на передачу которых дается согласие субъекта персональных данных								
Я подтверждаю, что предоставленные мною персональные данные являются полными, актуальными и достоверными								
Я обязуюсь своевременно извещать об изменении предоставленных персональных данных								
"		"		20		г.		
							(личная подпись)	(инициалы, фамилия)
Предоставленные данные соответствуют предъявленным документам, удостоверяющим личность								
"		"		20		г.		
							(должность)	(личная подпись)	(инициалы, фамилия)

ТИПОВАЯ ФОРМА
РАЗЪЯСНЕНИЯ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

РАЗЪЯСНЕНИЕ
субъекту персональных данных юридических последствий отказа представить свои персональные данные
(для государственных служащих)

Мне,_____,
(фамилия, имя, отчество)
разъяснены юридические последствия отказа предоставить свои персональные данные _____.

В соответствии со статьями 26, 42 Федерального закона от 27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации", Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30.05.2005 № 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением или прохождением государственной гражданской службы.

Без представления субъектом персональных данных обязательных для заключения служебного контракта сведений служебный контракт не может быть заключен.

На основании пункта 11 части 1 статьи 33 Федерального закона от

27.07.2004 № 79-ФЗ "О государственной гражданской службе Российской Федерации" служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности гражданской службы.

_____

(дата) (Ф.И.О. полностью, подпись)

(для работников)

В соответствии со статьями 57, 65, 69 Трудового кодекса РФ субъект персональных данных, лицо, поступающее на работу или работающее обязано, представить определенный перечень информации о себе.

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

На основании пункта 11 части 1 статьи 77 Трудового кодекса РФ трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

13. ПОРЯДОК ДОСТУПА РАБОТНИКОВ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЁТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий Порядок доступа в помещения, в которых ведется обработка персональных данных (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в_____, и обеспечения соблюдения требований законодательства о персональных данных.

2. Настоящий Порядок обязателен для применения и исполнения всеми работниками _____.

3. Помещения, в которых ведется обработка персональных данных, должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранной сигнализацией.

4. Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

5. Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в металлических шкафах, оборудованных опечатывающими устройствами.

6. Помещения, в которых ведется обработка персональных данных, запираются на ключ, а в нерабочее время подключаются к охранной сигнализации.

7. Вскрытие и закрытие (опечатывание) помещений, в которых ведется обработка персональных данных, производится работниками, имеющими право доступа в данные помещения.

8. Перед закрытием помещений, в которых ведется обработка персональных данных, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны:

убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть и опечатать шкафы;

отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

закрыть окна;

подключить охранную сигнализацию.

9. Перед открытием помещений, в которых ведется обработка персональных данных, работники, имеющие право доступа в помещения, обязаны:

провести внешний осмотр с целью установления целостности двери и замка;

открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

10. При обнаружении неисправности двери и запирающих устройств работники обязаны:

не вскрывая помещение, в котором ведется обработка персональных данных, доложить непосредственному руководителю;

в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

составить акт о выявленных нарушениях и передать его руководителю _____для организации служебного расследования.

11. Право самостоятельного входа в помещения, где обрабатываются персональные данные, имеют только работники, непосредственно работающие в данном помещении.

Иные работники имеют право пребывать в помещениях, где обрабатываются персональные данные, только в присутствии работников, непосредственно работающих в данных помещениях.

12. При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты.

Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

13. Техническое обслуживание компьютерной и организационной техники, сопровождение программных средств, уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

14. В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в

системах энерго-, водо- и теплоснабжения помещение, в котором ведется обработка персональных данных, вскрывается комиссией в составе не менее двух человек.

15. Ответственность за соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных, возлагается на Руководителей отделов, обрабатывающих персональные данные.

14. ПОЛОЖЕНИЕ ОБ ОСОБЕННОСТЯХ И ПРАВИЛАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Персональные данные - любая информация, относящаяся к сотруднику, учащемуся, родителям учащегося (далее субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", а также требований нормативных правовых актов федеральных органов

исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).
2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.
2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных без использования средств

автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами _____.
2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:
2.4.1. типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование _____ и адрес _____, 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 _____ способов обработки персональных данных;
2.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;
2.4.3. 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;

2.5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение _____или в иных аналогичных целях, должны соблюдаться следующие условия:
2.5.1.необходимость ведения такого журнала должна быть предусмотрена актом _____, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;
2.5.2.копирование содержащейся в таких журналах информации не допускается;
2.5.3.персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.
2.6. 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 (удаление, зачеркивание, стирание).

2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.
3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для

обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом

Приложение 1

Лист ознакомления
с Положением об особенностях и правилах осуществления обработки персональных данных без использования средств автоматизации

Дата ознакомления	ФИО сотрудника, ознакомившегося с документом	Должность сотрудника, ознакомившегося с документом	Подпись сотрудника, ознакомившегося с документом

15.Типовой план периодических проверок условий обработки персональных данных в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям

№ п/п	Дата проведения мероприятий	Краткое описание проверочных мероприятий	Периодичность проверочных мероприятий	Результат проверки	Ф.И.О. ответственного пользователя, подпись	Фамилия и роспись лица, проводившего проверку	Примечание
1		Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны	1 раз в месяц				
2		Проверка выполнения требований по условиям размещения АРМ в помещениях, в которых размещены средства ИСПДн	1 раз в 3 месяца				
3		Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки ПДн	1 раз в 3 месяца				
4		Проверка целостности наклейки на системных блоках и других ТС, участвующих в обработке ПДн	1 раз в месяц				
5		Проверка допуска в помещения, где	1 раз в 3 месяца				

		размещены средства ИСПДн, и осуществляется обработка ПДн					
6		Проверка соответствия реального уровня полномочий по доступу к ПДн различных пользователей, установлен ному в списке лиц, допущенных к бработке ПДн, уровню полномочий	1 раз в 3 месяца				
7		Проверка наличия средств защиты информации в соответствии с указан-ными в Журнале учета средствами защиты информации	1 раз в 3 месяца				
8		Проверка правильности применения средств защиты информации	1 раз в 3 месяца				
9		Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей	1 раз в месяц				
10		Контроль за обновлениями ПО и единообразия применяемого ПО на всех элементах ИСПДн	1 раз в неделю				
11		Проверка соблюдения правил парольной защиты	1 раз в 3 месяца				
12		Проверка работоспособности	1 раз в месяц				

		системы резервного копирования					
13		Проведение мероприятий по проверке организации учета и условий хранения съемных носителей ПДн	1 раз в 3 месяца				
14		Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети Интернет	1 раз в месяц				
15		Проверка знаний персоналом руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях	1 раз в год				
16		Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн	1 раз в 6 месяцев				
17		Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники	1 раз в 3 месяца				

		для обработки ПДн и применения средств защиты (сертификатов соответствия и других документов)					

СОГЛАСОВАНО:
Ответственный за организацию обработки
персональных данных в _____

_____ _____

Руководитель отдела кадров _____
Администратор ИСПДн-

_____ _____

- «____» _____ 201__ года

16. Ведомость ознакомления работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных

№	**Наименование положения законодательства Российской Федерации о персональных данных (в том числе требованиями к защите персональных данных), локального акта по вопросам обработки персональных данных**	**Дата**	**Подпись**
1	Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" -требования	28.03.201___	
2	Постановление 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" -требования	28.03.201___	

Ответственный за организацию обработки персональных данных:

17. Обучение государственных служащих по вопросам обработки персональных данных

Программа обучения предусматривает:

обновление знаний о системе государственного управления с точки зрения системного подхода;

исследование механизма обеспечения безопасности персональных данных при исполнении полномочий в органах государственной власти;

изучение организационно-правовых основ технической защиты конфиденциальной информации и обеспечения безопасности персональных данных;

изучение рекомендаций и основных мероприятий по организации и техническому обеспечению безопасности персональных данных;

практическую отработку навыков выявления угроз и уязвимостей безопасности персональных данных;

формирование навыков обеспечения безопасности персональных данных при их обработке без использования средств автоматизации и хранении вне информационных систем персональных данных.

Форма обучения: программа может реализовываться по очной (дневной), с отрывом от государственной гражданской службы, с частичным отрывом от службы и с использованием возможностей дистанционных образовательных технологий в зависимости потребностей заказчика.

18. ТРЕБОВАНИЯ И МЕТОДЫ ПО ОБЕЗЛИЧИВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящие Требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, (далее - Требования и методы) разработаны в соответствии с подпунктом "з" пункта 1 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, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 № 211.

2. В соответствии со статьей 3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" под обезличиванием персональных данных понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

4. К свойствам обезличенных данных относятся:

полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);

структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);

релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);

семантическая целостность (сохранение семантики персональных данных при их обезличивании);

применимость (возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее - оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах);

анонимность (невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации).

5. К характеристикам (свойствам) методов обезличивания персональных данных (далее - методы обезличивания), определяющим

возможность обеспечения заданных свойств обезличенных данных, относятся:

обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);

вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию субъекта персональных данных);

возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);

совместимость (возможность интеграции персональных данных, обезличенных различными методами);

параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

6. Требования к методам обезличивания подразделяются на:

требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;

требования к свойствам, которыми должен обладать метод обезличивания.

7. К требованиям к свойствам получаемых обезличенных данных относятся:

сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

сохранение структурированности обезличиваемых персональных данных;

сохранение семантической целостности обезличиваемых персональных данных;

анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

8. К требованиям к свойствам метода обезличивания относятся:

обратимость (возможность проведения деобезличивания);

возможность обеспечения заданного уровня анонимности;

увеличение стойкости при увеличении объема обезличиваемых персональных данных.

9. Выполнение приведенных в пунктах 7 и 8 Требований и методов требований обязательно для обезличенных данных и применяемых методов обезличивания.

10. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

11. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);

метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

12. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

семантическая целостность;

применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);

изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);

параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах персональных данных, подлежащих обезличиванию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется установить атрибуты персональных

данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.

13. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.

Метод обеспечивает следующие свойства обезличенных данных:

структурированность;

релевантность;

применимость;

анонимность.

Оценка свойств метода:

обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);

вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);

возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);

параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);

возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).

Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта.

При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).

14. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

релевантность;

семантическая целостность;

применимость.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);

возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);

параметрический объем (определяется числом подмножеств и числом субъектов персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

15. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.

Метод обеспечивает следующие свойства обезличенных данных:

полнота;

структурированность;

релевантность;

семантическая целостность;

применимость;

анонимность.

Оценка свойств метода:

обратимость (метод позволяет провести процедуру деобезличивания);

вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);

изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);

возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);

совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами);

параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);

возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).

Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.

Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

19. Уведомление об обработке (о намерении осуществлять обработку) персональных данных

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

_____

(полное и сокращенное наименования, фамилия, имя, отчество оператора)

_____

(адрес местонахождения и почтовый адрес оператора)

руководствуясь:

_____

(правовое основание обработки персональных данных)

_____

с целью:

_____

(цель обработки персональных данных)

_____

осуществляет обработку:

_____

(категории персональных данных)

_____

принадлежащих:

_____

(категории субъектов, персональные данные которых обрабатываются)

_____

Обработка вышеуказанных персональных данных будет осуществляться путем:

_____

(перечень действий с персональными данными, общее описание используемых оператором способов

_____

обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

_____

(описание мер, предусмотренных ст. ст. 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ

_____

“О персональных данных”, в т.ч. сведения о наличии шифровальных (криптографических)

_____

средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование

_____

юридического лица, ответственных за организацию обработки персональных данных,

_____

и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных:

(при наличии трансграничной передачи персональных данных в процессе их обработки указывается перечень

иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных:

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных

(число, месяц, год)

Срок или условие прекращения обработки персональных данных:

(число, месяц, год или основание (условие), наступление которого повлечет прекращение обработки

персональных данных)

(должность)	(подпись)	(расшифровка подписи)

“___” _____ 201___ г.

20. Политика оператора в отношении обработки персональных данных

1.ВВЕДЕНИЕ

Настоящее Положение определяет политику _____ как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.

1.1 Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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».

1.2 Политика разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных, направленного на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, в частности в целях защиты от несанкционированного доступа и неправомерного распространения персональных данных, обрабатываемых в информационных системах _____.

1.3 Политика действует в отношении информации, которую _____ получает о субъекте персональных данных в процессе предоставления услуг или исполнения договорных обязательств.

1.4 Настоящая Политика раскрывает состав субъектов персональных данных, принципы, порядок и условия обработки персональных данных работников _____ и иных лиц, чьи персональные данные обрабатываются _____, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.5. Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами _____а по защите конфиденциальной информации.

2. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Перечень персональных данных, подлежащих защите в _____, формируется в соответствии с федеральным законодательством о персональных данных и Положением о _____ (Постановление Правительства Санкт-Петербурга от _____)

2.2 Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.3 В зависимости от субъекта персональных данных, _____ обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные государственного служащего _____ - информация, необходимая _____ в связи с трудовыми отношениями и касающиеся конкретного государственного служащего Санкт-Петербурга.
- персональные данные руководителей подведомственных предприятий, необходимые _____ для отражения в отчетных документах о деятельности _____ в соответствии с требованиями федеральных законов, нормативных документов Правительства Санкт-Петербурга и иных нормативных правовых актов.
- персональные данные руководителя или сотрудника юридического лица, являющегося контрагентом _____, необходимые _____ для выполнения своих обязательств в рамках договорных отношений с контрагентом и для выполнения требований законодательства Российской Федерации.
- граждан, обращающихся в _____ в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан в Российской Федерации»

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 _____ осуществляет обработку персональных данных в следующих целях:

- осуществления деятельности, предусмотренной Положением о _____, действующим законодательством Российской Федерации;
- заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством и Положением о _____;
- организации кадрового учета _____, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе

доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных»;

- работой с обращениями граждан в соответствии с Регламентом _____

4. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями законодательства РФ и нормативными документами.

4.2. В _____ создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в _____ данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. ПРАВА

5.1. _____ как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

5.2. Субъект персональных данных имеет право

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых _____ и источник их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его 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 при обработке его персональных данных;

- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных _____ осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям _____;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения, созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

6.2 Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации.

7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. _____ предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.2. В целях координации действий по обеспечению безопасности персональных данных в _____ назначено ответственное лицо за обеспечение безопасности персональных данных.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящая Политика является внутренним документом _____, общедоступной и подлежит размещению на официальном сайте _____.

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на странице по адресу: **http://_____.**

8.3. Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных _____.

8.4. Ответственность должностных лиц _____, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами _____.

21. Приказ о назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе

ПРОЕКТ ПРИКАЗА

О назначении должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказываю:

1. Назначить ответственным за обеспечение безопасности персональных данных в информационной системе _____ (Ф.И.О., должность (должностное лицо из числа заместителей).

2. Выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных возложить на (подразделение или должностное лицо).

3. В срок до _____ назначенным лицам разработать и внедрить:

– план мероприятий по обеспечению защиты персональных данных;

– перечень персональных данных, подлежащих защите и объем персональных данных;

– положение о порядке обработки и обеспечении безопасности персональных данных;

– определить уровни защищенности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) с оформлением акта;

– частную модель угроз для каждой ИСПДн;

– матрицу доступа сотрудников к персональным данным;

–утвердить перечень используемых сертифицированных технических средств защиты информации, эксплуатационной и технической документации к ним;

– порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

– журнал учета машинных носителей конфиденциальной информации;

– журнал регистрации и учета обращений субъектов персональных данных;

– инструкцию администратора безопасности ИСПДн;
– инструкцию пользователя по обеспечению безопасности ИСПДн;
– инструкцию по организации антивирусной защиты в локальной вычислительной сети.

4. Руководителям структурных подразделений в срок до _____ представить ответственному за обеспечение безопасности персональных данных перечень сотрудников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей.

5. Ответственному за выполнение работ по обеспечению безопасности персональных данных организовать учет носителей персональных данных.

6. Запретить сотрудникам, имеющим доступ к персональным данным, использовать для хранения и обработки персональных данных носители информации, не поставленные на учет в установленном порядке.

7. _____ (Ф.И.О., должность) юридического отдела урегулировать вопросы законности обработки персональных данных субъектов, разработать типовую форму письменного согласия субъектов персональных данных на обработку их персональных данных.

8. _____ (Ф.И.О., должность) отдела кадров провести работу по учету персональных данных сотрудников и обеспечить их безопасность при обработке без использования средств автоматизации.

9. Приказ довести до сотрудников, обрабатывающих персональные данные.

10. Контроль за выполнением требований настоящего приказа оставляю за собой.

Руководитель

22. Приказ об организация режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных

ПРОЕКТ ПРИКАЗА

Об организация режима
обеспечения безопасности помещений,
в которых размещены
информационные системы
персональных данных

_____

С целью организации режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", **приказываю:**

1. Утвердить перечень помещений, в которых размещены информационные системы персональных данных, (далее – ИСПДн) согласно приложению №1 к настоящему приказу.
2. Руководителям структурных подразделений в срок до _____ представить ответственному за обеспечение безопасности персональных данных списки сотрудников для организации допуска сотрудников в указанные помещения.
3. Установить, что ответственность за организацию режима обеспечения безопасности помещений и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, и руководитель структурного подразделения.
4. В нерабочее время указанные помещения закрываться на ключ и сдавать под охрану.
5. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с ответственным за обеспечение безопасности персональных данных.
6. Контроль за выполнением настоящего приказа возложить на _____.

Руководитель _____

23. Приказ об утверждении мест хранения персональных данных (материальных носителей)

ПРОЕКТ ПРИКАЗА

Об утверждении мест хранения
персональных данных
(материальных носителей)

Руководствуясь требованиями Федерального Закона от 27.07.2006 № 152 - ФЗ «О персональных данных», в целях защиты персональных данных работников_____,
п р и к а з ы в а ю:

1. Персональные данные (материальные носители) работников, _____хранить в кабинете _____.
2. Для предотвращения уничтожения, блокирования, хищения, модифицирования персональных данных (материальных носителей) работников _____, содержащихся на электронных носителях информации, хранить только на сервере в кабинете _____.
3. На себя, а также на _____ возлагаю персональную ответственность за соблюдение мер по защите персональных данных работников_____ от несанкционированного доступа.
4. Контроль за исполнением приказа оставляю за собой.

Руководитель

С приказом ознакомлен:

24. Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.

Приложение
к приказу от «__» _____ 201__ г. №

Список сотрудников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

№ п/п	ФИО	Должность	Порядковые номера ПДн (в соответствии с «Перечнем ПДн, обрабатываемых в организации, к которым допущен сотрудник	Категории персональных данных				Подпись сотрудника
				специальные	биометрические	общедоступные	иные	
				1	2	3	4	

Руководитель _____

“____” _____ 201__ г.

25. О доступе к содержанию электронного журнала сообщений

ПРОЕКТ ПРИКАЗА

О проведении работ по защите персональных данных при их обработке в информационных системах персональных данных

в_____

Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах и в целях исполнения постановления Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" в_____:

ПРИКАЗЫВАЮ:

1) Организовать ведение электронного журнала сообщений.

2) Доступ к содержанию электронного журнала сообщений возможен исключительно для должностных лиц (работников) _____(или уполномоченного лица), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

3) Журнал вести в электронном виде.

4) Контроль за исполнением настоящего приказа возложить на _____.

Руководитель

26. Приказ об утверждении перечня лиц, осуществляющих обработку персональных данных без использования средств автоматизации.

ПРОЕКТ ПРИКАЗА

В соответствии с постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", приказываю:

1. Утвердить перечень лиц, осуществляющих обработку персональных данных без использования средств автоматизации. (приложение № 1).

2. Внести дополнения в должностные инструкции работников, осуществляющих обработку персональных данных без использования средств автоматизации.

3.Контроль за исполнением приказа оставляю за собой

Руководитель_____

С приказом ознакомлен:

27. Приказ об утверждении мест хранения персональных данных (материальных носителей) для осуществления их обработки без использования средств автоматизации.

ПРОЕКТ ПРИКАЗА

Об утверждении мест хранения
персональных данных

1. В соответствии с постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", приказываю:

2. Персональные данные (материальные носители) _____ хранить в _____в специально отведенном железном шкафу.

3. Возложить на Руководителя _____ персональную ответственность за соблюдение мер по защите от несанкционированного доступа к материальным носителям, содержащим персональные данные Работников _____

4. Руководителю _____ обеспечить раздельное хранение персональных данных (материальных носителей**)**, обработка которых осуществляется в различных целях.

Контроль за исполнением настоящего Приказа возлагаю на себя.

Руководитель_____

С приказом ознакомлен:

28. Ведомость ознакомления лиц о факте обработки ими персональных данных, без использования средств автоматизации и категориях обрабатываемых ими персональных данных

УТВЕРЖДАЮ

«__» _____ 201__ г.

№ п/п	ФИО	Должность	Порядковые номера категорий ПДн (в соответствии с «Перечнем ПДн, обрабатываемых в органе исполнительной власти, к которым допущен сотрудник	Категории персональных данных				Подпись сотрудника
				специальные	биометрические	общедоступные	иные	
				1	2	3	4	

Руководитель _____

“____” _____ 201__ г.

29. О журнале учета, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора

ПРОЕКТ ПРИКАЗА

О ведении журнала учета посетителей

_____

В соответствии с требованиями постановления Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", в учета пропуска посетителей (субъектов персональных данных) на территорию оператора приказываю**:**

1. Начальнику _____организовать ведения журнала учета посетителей, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора.

2. Информацию (фамилия, имя, отчество; документ, удостоверяющий личность), запрашиваемую у субъектов персональных данных, необходимую для пропуска на территорию оператора письменно фиксировать в соответствующих графах «Журнала учета посетителей».

3.Запретить фиксировать в журнале иные персональные данные кроме указанных в настоящем Приказе, фиксировать информацию с нарушением соответствующих граф и форм журнала; фиксировать информацию более одного раза в каждом случае пропуска; копировать содержащуюся в журнале информацию.

4. Листы журнала учета посетителей должны быть прошиты, пронумерованы и скреплены печатью; срок хранения журнала учета посетителей составляет 5 лет.

5.Право доступа к журналу учета посетителей имеют:

-руководитель_____

- заместители_____,

- руководители структурных подразделений,

- представители правоохранительных и надзорных органов в пределах своих полномочий.

6.Персональную ответственность за ведение и сохранность журнала учета посетителей и вносимые в него сведения несут _____;

7.Контроль за соблюдением правил ведения и сохранности журнала осуществляет ответственный за обеспечение безопасности персональных данных.

Руководитель _____

30. Типовая форма журнала учета, содержащего персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию оператора

Журнал учета персональных данных для однократного пропуска субъекта персональных данных на территорию оператора

Журнал начат “ _____ ’ _____ 201___ г.

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201_

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

На _____ листах

Номер пропуска	Номер заявки на выдачу пропуска	ФИО посетителя	Наименование принимающего структурного подразделения	ФИО должностного лица, подписавшего пропуск	Время начала действия пропуска	Вид документа, с которым пропуск действителен	Место посещения	Фактическое время выхода	Отметка о возврате пропуска	Подпись дежурного бюро пропусков
1	2	3	4	5	6	7	8	9	10	11

31. Положение о порядке организации и проведения работ по защите конфиденциальной информации

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201_ г.

Типовая форма
положения о порядке организации и проведения работ по защите конфиденциальной информации

Санкт-Петербург 201__

1. Общие положения

1.1. Настоящее Положение определяет порядок организации и проведения работ по защите конфиденциальной информации в органах исполнительной власти и их подведомственных учреждениях (далее – ОИВ).

1.2. Мероприятия по защите конфиденциальной информации, проводимые в ОИВ, являются составной частью управленческой и иной служебной деятельности и осуществляются во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.3. Информационные системы и ресурсы, являющиеся собственностью государства, находятся в ведении органов исполнительной власти и организаций в соответствии с их компетенцией, подлежат обязательному учету и защите.

В соответствии с требованиями Закона Санкт-Петербурга от 01.07.2009 № 371-70 "О государственных информационных системах Санкт-Петербурга" городские информационные системы должны быть зарегистрированы в реестре информационных систем города Санкт-Петербурга.

1.4. Режим защиты конфиденциальной информации устанавливается собственником информационных ресурсов или уполномоченным лицом в соответствии с законодательством.

Конфиденциальная информация должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты конфиденциальной информации, сертифицируемых в установленном порядке. Обязательной сертификации подлежат средства, в том числе иностранного производства, предназначенные для технической защиты конфиденциальной информации.

1.5.Уровень технической защиты конфиденциальной информации, а также перечень необходимых мер защиты определяется дифференцировано по результатам обследования объекта информатизации, с учетом соотношения затрат на организацию технической защиты конфиденциальной информации и величины ущерба, который может быть нанесен собственнику конфиденциальной информации при ее разглашении, утрате, уничтожении и

искажении. Для сведений, составляющих служебную тайну не ниже требований, установленных данным документом и государственными стандартами Российской Федерации.

Системы и средства информатизации и связи, предназначенные для обработки (передачи) конфиденциальной информации должны быть аттестованы в реальных условиях эксплуатации на предмет соответствия принимаемых мер и средств защиты требуемому уровню безопасности информации.

Проведение любых мероприятий и работ с конфиденциальной информацией, без принятия необходимых мер технической защиты информации не допускается.

1.6. Объектами защиты в органах исполнительной власти и их подведомственных учреждениях являются:

- средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть (ЛВС), средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации, содержащей конфиденциальную информацию - далее основные технические средства и системы (ОТСС);
- технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается конфиденциальной информация - далее вспомогательные технические средства и системы (ВТСС);
- помещения (служебные кабинеты, актовые, конференц-залы и т.п.), специально предназначенные для проведения конфиденциальных мероприятий – защищаемые помещения (ЗП).

1.7. Ответственность за выполнение требований настоящего Положения возлагается на_____, руководителей подразделений (департаментов, управлений, отделов), на руководителей структурного подразделения защиты конфиденциальной информации, а также на специалистов, допущенных к обработке, передаче и хранению в технических средствах информации, содержащей конфиденциальную информацию.

1.8. Непосредственное руководство работами по защите

конфиденциальной информации осуществляет первый заместитель органа исполнительной власти.

2. Охраняемые сведения

2.1. В органе исполнительной власти и их подведомственных учреждениях разрабатывается Перечень сведений конфиденциального характера. Сведения, составляющие конфиденциальную информацию, определяются Перечнем сведений конфиденциального характера в соответствии с Указом Президента РФ от 6.03.1997 № 188.

Перечень сведений конфиденциального характера включает:

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
- Сведения, составляющие тайну следствия и судопроизводства.
- Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений и т.д.).
- Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна).
- Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
- Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна).

Сведения, составляющие служебную тайну, определяются действующим в субъекте Российской Федерации "Перечнем сведений, составляющих служебную информацию ограниченного распространения".

Указанный перечень может включать следующие классы сведений ограниченного распространения:

сведения экономического характера;

сведения по финансовым вопросам;

сведения по науке и технике;

сведения по транспорту и связи;

сведения по вопросам внешней торговли и международных научно-технических связей;

сведения, связанные с обеспечением безопасности органов государственной власти субъекта РФ и органов местного самоуправления.

3. Технические каналы утечки конфиденциальной информации, несанкционированного доступа и специальных воздействий на нее.

3.1. Доступ к конфиденциальной информации, нарушение ее целостности и доступности возможно реализовать за счет:

– несанкционированного доступа к конфиденциальной информации при ее обработке в информационных системах и ресурсах;

– утечки конфиденциальной информации по техническим каналам.

3.2. Детальное описание возможных технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на нее содержится в Модели угроз безопасности информации органа исполнительной власти.

4.Оценка возможностей технических разведок и других источников угроз безопасности конфиденциальной информации

4.1. Для добывания конфиденциальных сведений могут использоваться:

портативная возимая (носимая) аппаратура радио, акустической, визуально-оптической и телевизионной разведки, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН);

автономная автоматическая аппаратура акустической и телевизионной разведки, а также разведки ПЭМИН;

компьютерная разведка, использующая различные способы и средства несанкционированного доступа к информации и специальных воздействий на нее.

Угроза компьютерной разведки объектам защиты возможна в случае подключения АС, обрабатывающим информацию ограниченного доступа к внешним, в первую очередь - глобальным сетям.

Портативная возимая аппаратура разведки может применяться из ближайших зданий и автомобилей на стоянках вблизи зданий органов исполнительной власти и их подведомственных учреждениях.

Портативная носимая аппаратура имеет ограниченные возможности и может быть использована лишь для уточнения данных, или перехвата информации в непосредственной близости от защищаемых объектов.

Автономная автоматическая аппаратура радио, акустической, телевизионной, а также разведки ПЭМИН используется для длительного наблюдения за объектом защиты.

4.2. Несанкционированный доступ к информации и специальные воздействия на нее могут осуществляться при ее обработке на отдельных автоматизированных рабочих местах, в локальных вычислительных сетях, в распределенных телекоммуникационных системах.

4.3. Кроме перехвата информации техническими средствами возможно непреднамеренное попадание защищаемой информации к лицам, не допущенным к ней, но находящимся в пределах КЗ. Это возможно, например, вследствие:

– непреднамеренного прослушивания без использования технических средств конфиденциальных разговоров из-за недостаточной звукоизоляции ограждающих конструкций защищаемых помещений и их инженерно-технических систем;

– случайного прослушивания телефонных разговоров при проведении профилактических работ в сетях телефонной связи;

– некомпетентных или ошибочных действий пользователей и администраторов АС при работе вычислительных сетей;

– просмотра информации с экранов дисплеев и других средств ее отображения.

4.4. Оценка возможностей средств технической разведки осуществляется с использованием нормативных документов ФСТЭК России.

Наиболее опасной для органов исполнительной власти и их подведомственных учреждений является аппаратура портативной (возимой и носимой) разведки электромагнитных излучений и аппаратура акустической речевой разведки, которая может применяться с прилегающей к зданиям

администрации территорий, а также автономная автоматическая аппаратура акустической речевой разведки, скрытно устанавливаемая внутри помещений.

4.5. Оценка возможности НСД к информации в средствах вычислительной техники и автоматизированных системах осуществляется с использованием следующих руководящих документов ФСТЭК России:

Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;

Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по технической защите конфиденциальной информации.

НСД к информации и специальные воздействия на нее реально возможны, если не выполняются требования перечисленных выше документов, дифференцированные в зависимости от степени конфиденциальности обрабатываемой информации, уровня полномочий пользователей по доступу к конфиденциальной информации и режимов обработки данных в автоматизированных системах.

5. Организационные и технические мероприятия по технической защите конфиденциальной информации

5.1. Разработка мер, и обеспечение защиты конфиденциальной информации осуществляются подразделением по защите конфиденциальной информации (службой безопасности) или отдельными специалистами, назначаемыми руководителем органа исполнительной власти для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии ФСТЭК России и ФСБ России на право осуществления соответствующих работ.

5.2. Для защиты конфиденциальной информации, используются сертифицированные по требованиям безопасности технические средства защиты.

5.3. Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

5.4. Ответственность за обеспечение требований по технической защите конфиденциальной информации возлагается на_____, эксплуатирующего объекты информатизации.

5.5. Техническая защита информации в защищаемых помещениях (ЗП).

К основным мероприятиям по технической защите конфиденциальной информации в ЗП относятся:

5.5.1. Определение перечня ЗП по результатам анализа циркулирующей в них конфиденциальной информации и условий ее обмена (обработки), в соответствии с нормативными документами ФСТЭК России.

5.5.2. Назначение сотрудников, ответственных за выполнение требований по технической защите конфиденциальной информации в ЗП, далее сотрудники, ответственные за безопасность информации.

5.5.3. Разработка частных инструкций по обеспечению безопасности информации в ЗП.

5.5.4. Обеспечение эффективного контроля за доступом в ЗП, а также в смежные помещения.

5.5.5. Инструктирование сотрудников, работающих в ЗП о правилах эксплуатации ПЭВМ, других технических средств обработки информации, средств связи с соблюдением требований по технической защите конфиденциальной информации.

5.5.6. Проведение в ЗП обязательных визуальных (непосредственно перед совещаниями) и инструментальных (перед ответственными совещаниями и периодически раз в квартал) проверок на наличие внедренных закладных устройств, в том числе осуществление контроля всех посторонних предметов, подарков, сувениров и прочих предметов, оставляемых в ЗП.

5.5.7. Исключение неконтролируемого доступа к линиям связи, управления и сигнализации в ЗП, а также в смежных помещениях и в коридоре.

5.5.8. Оснащение телефонных аппаратов городской АТС, расположенных в ЗП, устройствами высокочастотной развязки подавления слабых сигналов, а также поддержание их в работоспособном состоянии. Для спаренных

телефонов достаточно одного устройства на линию, выходящую за пределы ЗП.

5.5.9. Осуществление сотрудниками, ответственными за безопасность информации, контроля за проведением всех монтажных и ремонтных работ в выделенных и смежных с ними помещениях, а также в коридорах.

5.5.10. Обеспечение требуемого уровня звукоизоляции входных дверей ЗП.

5.5.11. Обеспечение требуемого уровня звукоизоляции окон ЗП.

5.5.12. Демонтирование или заземление (с обеих сторон) лишних (незадействованных) в ЗП проводников и кабелей.

5.5.13. Отключение при проведении совещаний в ЗП всех неиспользуемых электро- и радиоприборов от сетей питания и трансляции.

5.5.14. Выполнение перед проведением совещаний следующих условий:

окна должны быть плотно закрыты и зашторены;

двери плотно прикрыты;

5.6. Защита информации, циркулирующей в ОТСС и наводящейся в ВТСС.

5.6.1. При эксплуатации ОТСС и ВТСС необходимо неукоснительное выполнение требований, определенных в предписании на эксплуатацию.

5.6.2. При невозможности обеспечения контролируемой зоны заданных размеров рекомендуется проведение следующих мероприятий:

Применение систем электромагнитного пространственного зашумления (СПЗ) в районе размещения защищаемого ОТСС.

Применение средств линейного электромагнитного зашумления (СЛЗ) линий электропитания, радиотрансляции, заземления, связи.

5.6.3. Техническая защита информации в средствах вычислительной техники (СВТ) и автоматизированных системах (АС) от несанкционированного доступа в соответствии с требованиями руководящих документов ФСТЭК (Гостехкомиссии) России должна обеспечиваться путем:

проведения классификации СВТ и АС;

выполнения необходимых организационных мер защиты;

установки сертифицированных программных и аппаратно-технических средств защиты информации от НСД.

защита каналов связи, предназначенных для передачи конфиденциальной

информации.

защиты информации от воздействия программ-закладок и компьютерных вирусов.

5.7. Организация и проведение работ по антивирусной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, при ее обработке техническими средствами определяются настоящим документом, действующими государственными стандартами и другими нормативными и методическими документами ФСТЭК (Гостехкомиссии) России.

Организации антивирусной защиты информации на объектах информатизации достигается путём:

установки и применения средств антивирусной защиты информации;

обновления баз данных средств антивирусной защиты информации;

действий должностных лиц при обнаружении заражения информационно-вычислительных ресурсов программными вирусами.

5.7.1. Организация работ по антивирусной защите информации возлагается на руководителей структурных подразделений и должностных лиц, осуществляющих контроль за антивирусной защитой, а методическое руководство и контроль над эффективностью предусмотренных мер защиты информации на руководителя подразделения по защите конфиденциальной информации (ответственного) ОИВ.

5.7.2. Защита информации от воздействия программных вирусов на объектах информатизации должна осуществляться посредством применения средств антивирусной защиты. Порядок применения средств антивирусной защиты устанавливается с учетом следующих требований:

обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации носителей информации, информационных массивов, программных средств общего и специального назначения;

периодическая проверка пользователями жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе носителей информации перед началом работы с ними на отсутствие программных вирусов;

внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;

восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

5.7.3. К использованию допускается только лицензированные, сертифицированные по требованиям ФСТЭК России антивирусные средства.

5.7.4. Порядок применения средств антивирусной защиты во всех случаях устанавливается с учетом следующих требований:

Входной антивирусный контроль всей поступающей на внешних носителях информации и программных средств любого назначения.

Входной антивирусный контроль всей информации поступающей с электронной почтой;

Входной антивирусный контроль всей поступающей информации из сети I№ter№et;

Выходной антивирусный контроль всей исходящей информации на любых внешних носителях и/или передаваемой по локальной сети на другие рабочие станции/сервера, а также передача информации посредством электронной почты;

Периодическая антивирусная проверка на отсутствие компьютерных вирусов на жестких дисках рабочих станций и серверов;

Обязательная антивирусная проверка используемых в работе внешних носителей информации;

Постоянный антивирусный контроль на рабочих станциях и серверах с использованием резидентных антивирусных мониторов в автоматическом режиме;

Обеспечение получения обновлений антивирусных программ в автоматическом режиме, включая обновления вирусных баз и непосредственно новых версий программ;

Внеплановая антивирусная проверка внешних носителей и жестких дисков рабочих станций и серверов на отсутствие компьютерных вирусов в случае подозрения на наличие компьютерного вируса;

Восстановление работоспособности программных и аппаратных средств, а так же непосредственно информации в случае их повреждения компьютерными вирусами.

5.7.5.Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

5.7.6. При обнаружении на носителе информации или в полученных файлах программных вирусов пользователи докладывают об этом в подразделение по защите конфиденциальной информации или ответственному сотруднику, и принимают меры по восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, поставить в известность подразделение информационно-технической службы органа власти по защите конфиденциальной информации и принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

При функционировании АРМ в качестве рабочей станции вычислительной сети производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

Ликвидация последствий воздействия программных вирусов осуществляется подготовленными представителями подразделения информационно-технической службы органа власти по защите конфиденциальной информации.

5.7.7. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения рабочих станций, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

5.7.8. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.7.9. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах возлагается на системного администратора органа исполнительной власти.

5.8.1. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8.2 Формирование личных паролей пользователей осуществляется централизованно. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

5.8.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

5.8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его

полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению администратора безопасности уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4 настоящей Инструкции.

5.8.6 Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором Touch Memory).

5.8.7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности подразделения, периодический контроль – на специалиста по защите информации или ответственного сотрудника.

6. Обязанности и права должностных лиц

6.1. Руководство технической защитой конфиденциальной информации в органе исполнительной власти возлагается на заместителя ОИВ.

6.2. Руководители подразделений органа исполнительной власти организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях подчиненных им подразделений.

6.3. Руководитель структурного подразделения по технической защите конфиденциальной информации (ответственный сотрудник) осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю в органе исполнительной власти.

6.4. Владельцы и пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.5. Руководители подразделений, владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием

сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются заместителю органа исполнительной власти (через структурное подразделение по технической защите конфиденциальной информации или ответственного сотрудника).

6.6. Заместитель органа исполнительной власти имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7. Планирование работ по технической защите конфиденциальной информации и контролю.

7.1. В органе исполнительной власти составляются годовые планы работ по технической защите конфиденциальной информации и контролю. Сроки разработки, представления и утверждения планов устанавливаются руководителем органа исполнительной власти.

7.2. В годовые планы по защите информации включаются:

подготовка проектов распорядительных документов по вопросам организации технической защиты информации в органе исполнительной власти, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах, в ЗП;

аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите конфиденциальной информации;

проведение периодического контроля состояния технической защиты информации;

мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

мероприятия по совершенствованию технической защиты информации на объектах органа исполнительной власти.

7.3. Контроль выполнения планов и отчетность по ним возлагается на структурное подразделение по технической защите конфиденциальной информации или ответственного сотрудника.

8. Контроль состояния технической защиты конфиденциальной информации.

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня органа исполнительной власти и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется:

ФСТЭК России (силами Управления ФСТЭК России Северо-Западному федеральному округу);

ФСБ России (силами Управления Федеральной службы безопасности Российской Федерации по городу Санкт-Петербургу и Ленинградской области);

Комиссией по контролю за состоянием работ по технической защите информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга - по графику проверок;

Структурным подразделением по технической защите конфиденциальной информации или ответственным сотрудником и пользователем – непрерывно.

8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, постановлений и распоряжений Губернатора Санкт-Петербурга, Правительства Санкт-Петербурга, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

9. Аттестация рабочих мест

9.1. Аттестации на соответствие требованиям по технической защите конфиденциальной информации в реальных условиях эксплуатации подлежат системы и средства информатизации и связи, предназначенные для обработки и передачи конфиденциальной информации, а также помещения, предназначенные для ведения конфиденциальных переговоров. Указанная аттестация проводится в соответствии с "Положением по аттестации объектов информатизации по требованиям безопасности информации", утвержденным Председателем Гостехкомиссии России 25.11.1994

9.2. По результатам аттестации выдается "Аттестат соответствия", получение которого дает право использования аттестованных систем и средств для обработки и передачи информации, составляющей конфиденциальную или служебную тайну, и ведения конфиденциальных переговоров в аттестованных помещениях.

Переаттестация систем и средств информатизации, связи и помещений проводится по истечении срока действия "Аттестата соответствия", при изменении мер технической защиты информации, условий технической защиты или применяемых технологий обработки и передачи информации.

10. Взаимодействие с предприятиями, учреждениями и организациями

10.1. При проведении совместных работ администрации Колпинского района с предприятиями, учреждениями и организациями должна быть обеспечена техническая защита конфиденциальной информации (служебной тайны), независимо от места проведения работ.

10.2. В технических заданиях на выполнение совместных работ с использованием конфиденциальной информации, должны быть предусмотрены требования (или меры) по ее технической защите, которые должны выполняться каждой из сторон. Технические задания на выполнение совместных работ согласовываются с подразделениями по технической защите конфиденциальной информации органа исполнительной власти или ответственным сотрудником и взаимодействующих предприятий (учреждений, организаций).

10.3. Организация технической защиты информации возлагается на руководителей совместных работ, а ответственность за обеспечение технической защиты информации - на исполнителей работ (пользователей)

при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

32. Перечень сведений конфиденциального характера, подлежащих защите, в том числе персональных данных и лист ознакомления к нему

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
перечня сведений конфиденциального характера, подлежащих защите, в том числе персональных данных и лист ознакомления к нему в ____

Санкт-Петербург 201__

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ

сведений конфиденциального характера, в том числе персональных данных органа исполнительной власти

№ п/п	Наименование сведений	Примечание
	Сведения, раскрывающие систему, средства защиты информации ЛВС организации от НСД, а также значения действующих кодов и паролей.	
	Сводный перечень работ организации на перспективу, на год (квартал).	
	Требования по обеспечению сохранения служебной тайны при выполнении работ в организации.	
	Порядок передачи служебной информации ограниченного распространения другим организациям.	
	Персональные данные субъектов ПДн: ФИО; Дата рождения; Контактный телефон; Адрес прописки; Адрес фактического проживания; Паспортные данные; Данные о состоянии здоровья (история болезни).	Обработка в АИС «»
	Персональные данные сотрудников: Фамилия, имя, отчество; Место, год и дата рождения; Адрес по прописке; Паспортные данные (серия, номер паспорта, кем и когда выдан); Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность); Информация о трудовой деятельности до приема на работу; Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения); Адрес проживания (реальный); Телефонный номер (домашний, рабочий, мобильный); Семейное положение и состав семьи	Обработка в АИС « »

	(муж/жена, дети); Информация о знании иностранных языков; Форма допуска; Оклад; Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета); ИНН; Данные об аттестации работников; Данные о повышении квалификации; Данные о наградах, медалях, поощрениях, почетных званиях; Информация о приеме на работу, перемещении по должности, увольнении; Информация об отпусках; Информация о командировках; Информация о болезнях; Информация о негосударственном пенсионном обеспечении.	

Лист ознакомления

Фамилия, Имя, Отчество	Должность	Дата ознакомления, роспись

33. Приказ о создании комиссии по классификации автоматизированных систем, обрабатывающих конфиденциальную информацию

ПРОЕКТ ПРИКАЗА

О создании комиссии по классификации автоматизированных систем, обрабатывающих конфиденциальную информацию

В целях выполнения "Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2012 № 282 и проведения классификации автоматизированных систем, обрабатывающих конфиденциальную информацию, **приказываю:**

1. Утвердить состав Комиссии по классификации _____ (Приложение № 1).
2. Комиссии провести классификацию автоматизированных систем, обрабатывающих конфиденциальную информацию до _____201___ в соответствии с требованиями руководящих документов ФСТЭК России с оформлением акта классификации АС.
3. При проведении классификации руководствоваться требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» Гостехкомиссия России, 1992.
4. Контроль за выполнением настоящего приказа оставляю за собой.

ПРИЛОЖЕНИЕ № 1

к приказу от _____ 201__г. № ___

С О С Т А В
КОМИССИИ
ПО КЛАССИФИКАЦИИ
_____

Председатель Комиссии – руководитель _____

Члены Комиссии:

_____
_____
_____
_____
_____
_____

34. Акт классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации

УТВЕРЖДАЮ

_____

(руководитель)

_____

(подпись)

«__» _____ 201__г.

Типовая форма акта
классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации

_____

(наименование автоматизированной системы)

Комиссия в составе:
председатель:_____

члены комиссии:_____

_____

рассмотрев исходные данные на автоматизированную систему (АС) _____,

(наименование автоматизированной системы)

условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д.) и в соответствии с руководящими документами ФСТЭК России (Гостехкомиссии) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

РЕШИЛА:

Установить АС

_____

(наименование автоматизированной системы)

класс защищенности _____.

Председатель

_____

Члены комиссии:

35. Перечень сотрудников (матрица доступа) допущенных к сведениям конфиденциального характера (персональным данным).

УТВЕРЖДАЮ

_____
«__» _____ 201__ г.

Типовая форма

Перечень сотрудников (матрица доступа) допущенных к сведениям конфиденциального характера (персональным данным).

Санкт-Петербург 201__

Перечень сотрудников (матрица доступа) допущенных к сведениям конфиденциального характера (персональным данным) в_____

№ п/п	Наименование АРМ	Здание, № помещения	Условное имя пользователя (группы)	Наименование защищаемых информационных ресурсов (логические диски, каталоги, программы, устройства и т.п.)	Тип доступа	Примечание
1	АРМ 1	Смольного 214, к. 345	Администратор	С:\Каталог 1	чтение	
					запись	
					выполнение	
				С:\Каталог 2	чтение	
					запись	
					выполнение	
				FDD	чтение	
					запись	
					выполнение	
				Сканер	сканирование	
				DVD-RW	чтение	
					запись	
					выполнение	
				Принтер	печать	
				Программные средства	инсталляция, изменение	
				ОС, СЗИ	настройки	
	АРМ 2	Смольного 214, к. 310	Пользователь 1	С:\Каталог 1	чтение	
					запись	
				Принтер	печать	
				Программные средства	выполнение	
				ОС, СЗИ	загрузка	

36. Список лиц, допущенных в защищаемое помещение

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
списка лиц, допущенных в защищаемое помещение №_____

№ п/п	№ отдела	Должность	Фамилия и инициалы
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

Руководитель _____

“____” _____ 201__ г.

37. Приказ об организации режима обеспечения безопасности помещений, предназначенных для обработки конфиденциальной информации

ПРОЕКТ ПРИКАЗА

Во исполнение Федерального закона №152-ФЗ от 27.07.2006 «О персональных данных», с учетом норм «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», утвержденных приказом Гостехкомиссии России от 30.08.2006 № 282, **приказываю**:

1. Утвердить перечень помещений, предназначенных для обработки конфиденциальной информации (далее – защищаемое помещение) согласно приложению № 1 к настоящему приказу.
2. Руководителям структурных подразделений в срок до _____ представить ответственному за обеспечение защиты информации списки сотрудников для организации допуска сотрудников в указанные помещения.
3. Установить, что ответственность за режим безопасности в защищаемом помещении и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, и руководитель структурного подразделения.
4. В нерабочее время указанные помещения закрываться на ключ и сдавать под охрану.
5. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации органа исполнительной власти.
6. Неукоснительно выполнять предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.
7. Контроль за соблюдением требований по защите информации возложить на Отдел _____.

8. Контроль за выполнением настоящего приказа возложить на _____.

Руководитель _____

Приложение №1 к приказу

от ____. _____ 201_ г.
№ _____

Перечень помещений

№ п/п	Наименование помещения	Адрес и место расположения
1	Зал совещаний, помещение № 13	ул. Смольного д.5
2	Кабинет первого заместителя руководителя, помещение № 1	ул. Смольного д.5

С ПРИКАЗОМ ОЗНАКОМЛЕН(А): _____ /_____/

(подпись)

«___» _____ 201__ года

С ПРИКАЗОМ ОЗНАКОМЛЕН(А): _____ /_____/

(подпись)

«___» _____ 201__ года

38. Приказ о назначении администратора защиты (безопасности) информации

ПРОЕКТ ПРИКАЗА

О назначении администратора
защиты (безопасности) информации

В соответствии с «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2012 № 282, **приказываю**:

1. Назначить администратором защиты (безопасности) (далее-администратор безопасности информации) в _____.
2. Возложить на администратора безопасности информации следующие функции:

администрирование информационных систем персональных данных (АС);

администрирование средств антивирусной защиты информационных систем персональных данных (АС);

администрирование средств и систем защиты персональных данных в информационных системах персональных данных (АС).

3. Утвердить инструкцию администратора безопасности информации.
4. Контроль за выполнением требований настоящего приказа возложить на руководителя_____.

Руководитель

ИНСТРУКЦИЯ
администратора безопасности информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации (в том числе персональных данных (ПДн), обрабатываемой в информационных системах ПДн (ИСПДн) _____, далее - (администратора безопасности).

1.2. Действие настоящей Инструкции распространяется на структурные подразделения _____.

1.3. Администратор безопасности назначается приказом руководителя _____ из числа подготовленных работников подразделения информационной безопасности (ИБ).

1.4. Администратор безопасности по вопросам обеспечения безопасности информации подчиняется руководителю подразделения ИБ, являющемуся структурным подразделением, назначаемым ответственным за обеспечение безопасности информации в _____.

1.5. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн _____.

1.6. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн _____в вопросах обеспечения безопасности информации.

1.7. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн _____.

1.8. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн _____, состояние и поддержание установленного уровня защиты информации, обрабатываемой в ИСПДн _____.

2. ЗАДАЧИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн _____ от несанкционированного доступа (НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;

- установка средств защиты информации и контроль выполнения правил их эксплуатации;

- сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн _____;

- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;

- оперативное реагирование на нарушения требований по ИБ в ИСПДн _____ и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;

- текущий контроль технологического процесса автоматизированной обработки ПДн;

- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;

- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в структурных подразделениях _____ и территориальных органах _____;

- методическую помощь всем работникам _____ и территориальных органов _____ по вопросам обеспечения безопасности ПДн.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Администратор безопасности обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн _____.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн _____ согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн _____ при обработке ПДн.

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние защиты ИСПДн _____.

3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.9. Контролировать физическую сохранность технических средств обработки информации.

3.10. Контролировать исполнение пользователями ИСПДн _____ введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации.

3.11. Контролировать исполнение пользователями правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.13. Не допускать установку, использование, хранение и размножение в ИСПДн _____ программных средств, не связанных с выполнением функциональных задач.

3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ИСПДн _____.

3.15. Оказывать помощь пользователям ИСПДн _____ в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.16. Периодически представлять руководству отчет о состоянии защиты ИСПДн _____ и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн _____, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн _____ требованиям безопасности информации <1>.

<1> Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных", Постановление Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", нормативно-правовые акты и методические документы ФСТЭК России и ФСБ России по защите персональных данных при их обработке в информационных системах персональных данных.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ИСПДн _____ работников, осуществивших НСД к защищаемым ресурсам ИСПДн или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн _____.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями _____ и территориальных органов _____ телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн _____ при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом _____ и территориальных органов _____ по вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Запрашивать и получать от Руководителей и специалистов структурных подразделений _____ и территориальных органов _____ информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в _____.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет ответственность <2>:

<2> Виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

5.1. За организацию защиты информационных ресурсов и технических средств ИСПДн _____.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн _____.

5.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. ДЕЙСТВИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НСД

6.1. К попыткам НСД относятся:

- сеансы работы с телекоммуникационными ресурсами _____ и территориальных органов _____ незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн _____ с использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор безопасности обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:
- доложить руководству подразделения ИБ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
- известить Руководителя структурного подразделения _____ и/или территориальных органов _____, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
- проанализировать характер НСД;
- по решению руководства подразделения ИБ осуществить действия по выяснению причин, приведших к НСД;
- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

39. Инструкция по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных)

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
инструкции по порядку учета и хранению машинных носителей конфиденциальной информации (персональных данных)

Санкт-Петербург 201__

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2015 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых органом исполнительной власти (далее наименование ОИВ) для использования в ИС.

1.2. Действие настоящего Положения распространяется на сотрудников органа исполнительной власти, подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

1. **Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
2. **АРМ** – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
3. **ИБ** – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
4. **ИС** – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
5. **Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.
6. **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
7. **ПК** – персональный компьютер.
8. **ПО** – Программное обеспечение вычислительной техники.
9. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

Пользователь – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей информации

3.1. Под использованием носителей информации в ИС _____ понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью органа исполнительной власти и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным _____ носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4.Машинные носители конфиденциальной информации предоставляются сотрудникам _____ по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника _____ производственной необходимости.

4. Порядок учета, хранения и обращения с машинными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении машинные носители с конфиденциальной информацией (персональными данными) в _____подлежат учёту.

4.2. Каждый машинных носитель с записанной на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу машинных носителей конфиденциальной информации (персональных данных) осуществляет администратор ИС. Факт выдачи съемного носителя фиксируется в журнале учета носителей конфиденциальной информации.

4.4. Сотрудники _____ могут получать машинный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета.

По окончании работ пользователь сдает машинный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.5. При использовании сотрудниками носителей конфиденциальной информации необходимо:

4.5.1. Соблюдать требования настоящей Инструкции.

4.5.2. Использовать машинные носители информации исключительно для выполнения своих служебных обязанностей.

4.5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции.

4.5.4. Бережно относится к машинным носителям конфиденциальной информации.

4.5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами, в том числе хранение носителя в сейфе.

4.5.6. Извещать администраторов ИС о фактах утраты (кражи) машинных носителей конфиденциальной информации.

4.6. При использовании машинных носителей конфиденциальной информации запрещено:

4.6.1. Использовать машинные носители конфиденциальной информации в личных целях.

4.6.2. Передавать машинные носители конфиденциальной информации другим лицам (за исключением администраторов ИС).

4.6.3. Хранить машинные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

4.6.4. Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому либо в других помещениях (местах).

4.7. Любое взаимодействие (обработка, прием, передача информации), инициированное сотрудником органа исполнительной власти между ИС и неучтенными (личными) носителями информации, рассматривается как **несанкционированное** (за исключением случаев, оговоренных с администраторами ИС заранее). Администратор ИС оставляет за собой право блокировать или ограничивать использование носителей информации.

4.8. Информация об использовании сотрудником _____ машинных носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена ответственному лицу за организацию обработки персональных данных и _____.

4.9. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей конфиденциальной информации

инициализируется служебная проверка, проводимая комиссией, состав которой утвержден _____.

4.10. По факту выясненных обстоятельств составляется акт расследования инцидента и передается председателю _____ для принятия мер согласно действующему законодательству.

4.11. Информация, хранящаяся на машинных носителях конфиденциальной информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

4.12. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на машинные носители записываются только предназначенные адресатам данные. Отправка конфиденциальной информации (персональных данных) адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

4.13. Вынос машинных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.14. В случае утраты или уничтожения машинных носителей конфиденциальной информации (персональных данных) либо разглашении содержащихся в них сведений, об этом немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты носителя составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей конфиденциальной информации (персональных данных).

4.15.Машинные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по прилагаемой форме.

4.16. В случае увольнения или перевода работника в другое структурное подразделение, предоставленные ему машинные носители конфиденциальной информации изымаются.

5.Ответственность

5.1. Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством.

40. Журнал учета машинных носителей конфиденциальной информации (персональных данных)

Типовая форма
журнала учета машинных носителей конфиденциальной информации
(персональных данных)

_____

(наименование организации)

Журнал начат “ _____ ’ _____ 201___ г.

_____
(должность)

_____ / / (Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201_

_____
(должность)

_____ / / (Ф.И.О. должностного лица)

На листах

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/ дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
	1	2	3	4	5	6	7	8	9
1									
2									
3									
…									

41. Приказ о назначении ответственного за обеспечение функционирования и безопасность криптосредств, в случае их использования для безопасности персональных данных при их обработке в информационных системах персональных данных

ПРОЕКТ ПРИКАЗА

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", **приказываю**:

1. Назначить ответственным за обеспечение функционирования и безопасности криптосредств при их использовании для безопасности персональных данных при их обработке в информационных системах персональных данных (далее–ответственный пользователь) _____.

2. Ответственному пользователю осуществлять контроль за соблюдением правил пользования криптографическими средствами защиты информации и условиями их использования, указанными в правилах пользования на них.

3. Контроль за выполнением требований настоящего приказа возложить на _____.

Руководитель

42. Приказ о назначении (структурного подразделения) должностного лица ответственных за защиту информации

ПРОЕКТ ПРИКАЗА

О назначении (структурного подразделения) должностного лица ответственных за защиту информации

Во исполнение "Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2012 № 282, **приказываю**:

1. Назначить ответственным за защиту информации _____ Руководителя _____ структурное подразделение**)**_____

2. Назначить ответственным за функционирование технических средств защиты информации _____ (приложение) в _____

3. Назначить ответственным за эксплуатацию _____руководителя Отдела _____

4. Назначенным лицам разработать:

– Приказ о создании комиссии по классификации автоматизированных систем, обрабатывающих конфиденциальную информацию.

– План мероприятий по обеспечению защиты конфиденциальной информации.

– Перечень сведений конфиденциального характера, подлежащих защите.

– Положение о порядке организации и проведения работ по защите конфиденциальной информации.

– Модель угроз и модель вероятного нарушителя.

– Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

– Порядок резервирования и восстановления работоспособности

ТС и ПО, баз данных и СЗИ.

– Инструкцию администратора безопасности АС.

– Инструкцию пользователя по обеспечению безопасности АС.

5. Контроль за соблюдением требований по защите информации _____ возложить на Отдел _____.

6. Контроль за выполнением настоящего приказа возложить на _____.

Руководитель _____

43. Приказ о назначении комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных

ПРОЕКТ ПРИКАЗА

В соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных» и требованиями постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказываю:

1. Утвердить состав Комиссии по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) (Приложение № 1).

В срок до _____Комиссии определить уровень защищенности персональных данных при их обработке в ИСПДн с оформлением акта.

При определении уровня защищенности персональных данных Комиссии руководствоваться требованиями Постановления Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Контроль за выполнением настоящего приказа оставляю за собой.

ПРИЛОЖЕНИЕ № 1

к приказу от _____ 201_ № ___

С О С Т А В
КОМИССИИ
по определению уровня защищенности персональных данных при их обработке в информационных системах персональных данных

_____

Председатель Комиссии – руководитель _____

Члены Комиссии:

_____
_____
_____
_____
_____
_____
_____

44. Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных

Санкт-Петербург 201__

СОДЕРЖАНИЕ

Назначение и область действия

Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ определяет действия (далее – Инструкция), связанные с функционированием ИСПДн органа исполнительной власти _____, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачей данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

Действие настоящей Инструкции распространяется на всех пользователей органа исполнительной власти, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости, но не реже раза в два года.

Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн _____ (указать наименование ИСПДн).

Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности _____ (указать наименование ИСПДн). Порядок реагирования на инцидент.

В настоящем документе под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн,

предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- В результате непреднамеренных действий пользователей.

- В результате преднамеренных действий пользователей и третьих лиц.

- В результате нарушения правил эксплуатации технических средств ИСПДн.

- В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

Все действия в процессе реагирования на Инцидент должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники органа исполнительной власти (Администратор безопасности, Администратор и Оператор ИСПДн), предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;

- системы обеспечения отказоустойчивости;

- системы резервного копирования и хранения данных;

- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;

- системы вентиляции и кондиционирования;

- системы резервного питания.

Все критичные помещения органа исполнительной власти (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться

технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

Носители должны храниться не менее года, для возможности восстановления данных.

Ответственность

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности информации в органе исполнительной власти.

45. ИНСТРУКЦИЯ О ДЕЙСТВИЯХ ЛИЦ, ДОПУЩЕННЫХ К ИНФОРМАЦИИ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

(ПРОЕКТ)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет действия работников _____ (далее - _____) в случае возникновения нештатных ситуаций в процессах обработки персональных данных в информационных системах персональных данных (ИСПДн) _____.

1.2. Положения инструкции обязательны для исполнения всеми должностными лицами территориального органа _____ в части выполнения вмененных им обязанностей.

1.3. Общими требованиями ко всем работникам _____ и территориальных органов _____ в случае возникновения нештатной ситуации являются:

- работник, обнаруживший нештатную ситуацию, немедленно ставит в известность своего непосредственного руководителя и администратора информационной безопасности;
- администратор информационной безопасности (далее - администратор безопасности) обязан проводить анализ ситуации и, в случае невозможности исправить положение, ставит в известность руководство _____ (территориальных органов _____). Кроме этого, администратор безопасности для локализации (блокирования) проявлений угроз информационной безопасности может привлекать пользователей ИСПДн _____, а также уполномоченного работника, ответственного за сопровождение технических средств ИСПДн;
- по факту возникновения нештатной ситуации и выяснению причин ее проявления проводится служебное расследование.

2. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДН ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

2.1. Сбой программного обеспечения.

2.1.1. Администратор безопасности совместно с уполномоченным работником подразделения информационных технологий (далее - подразделение информационных технологий (ИТ) выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О

произошедшем инциденте администратор безопасности сообщает руководителю подразделения информационной безопасности (далее - подразделение информационной безопасности (ИБ)) для принятия решения по существу.

2.2. Отключение электропитания технических средств ИСПДн.

2.2.1. Администратор безопасности совместно с уполномоченным работником подразделения ИТ проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.

2.3. Выход из строя технических средств ИСПДн (серверов, рабочих станций).

2.3.1. Уполномоченный работник подразделения ИТ совместно с администратором безопасности выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн (замене рабочей станции).

2.3.2. О выходе из строя сервера (рабочей станции) уполномоченный работник подразделения ИТ, ответственный за эксплуатацию сервера (рабочей станции), сообщает руководителю подразделения ИТ.

2.3.3. При необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.

2.4. Потеря данных.

2.4.1. При обнаружении потери данных уполномоченный работник подразделения ИТ проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования).

2.4.2. При необходимости уполномоченным работником подразделения ИТ производится восстановление программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте уполномоченный работник подразделения ИТ сообщает администратору безопасности. Администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.

2.5. Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн _____.

2.5.1. При обнаружении вредоносной программы (ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, и уполномоченным работником подразделения ИТ и администратором безопасности проводится анализ

состояния рабочей станции (сервера).

2.5.2. В результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции (сервера) данные могут быть потеряны. После успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения.

2.5.3. После ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта.

2.5.4. По факту появления ВП в локальной вычислительной сети Группой реагирования на инциденты ИБ проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем подразделения ИБ.

2.6. Утечка информации.

2.6.1. При обнаружении утечки информации ставится в известность администратор безопасности и начальник структурного подразделения. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн _____ и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

2.7. Взлом операционной системы средств автоматизации ИСПДн (несанкционированное получение доступа к ресурсам операционной системы).

2.7.1. При обнаружении взлома сервера ставится в известность руководитель подразделения ИТ и руководитель подразделения ИБ.

2.7.2. По возможности производится временное отключение сервера от локальной вычислительной сети _____ (территориального органа _____) для проверки на наличие ВП. Возможен временный переход на резервный сервер.

2.7.3. Уполномоченным работником подразделения ИТ проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Уполномоченным работником подразделения ИТ проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу.

2.7.4. В случае необходимости уполномоченным работником подразделения ИТ производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта.

2.7.5. По результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и

восстановлению программного обеспечения и данных на других информационных узлах ИСПДн.

2.8. Попытка несанкционированного доступа (НСД).

2.8.1. При попытке НСД уполномоченным работником подразделения ИТ и администратором безопасности проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД.

2.8.2. Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, уполномоченным работником подразделения ИТ устанавливаются такие обновления.

2.8.3. По факту попытки НСД Группой реагирования на инциденты ИБ проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается руководителем подразделения ИБ.

2.8.4. В случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

2.9. Компрометация ключевой информации (паролей доступа).

2.9.1. При компрометации ключевой информации (пароля доступа) администратором безопасности проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба.

2.9.2. О произошедшем инциденте администратор безопасности сообщает руководителю подразделения ИБ для принятия решения по существу.

2.10. Физическое повреждение или хищение оборудования технических средств ИСПДн.

2.10.1. Работником, обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность: непосредственный руководитель, руководители подразделений ИБ и ИТ.

2.10.2. Уполномоченным работником подразделения ИТ совместно с администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности.

2.10.3. О факте повреждения элементов ИСПДн работник подразделения ИТ докладывает руководителю подразделения ИТ.

2.10.4. В случае возникновения подозрения на целенаправленный вывод оборудования из строя Группой реагирования на инциденты ИБ проводится

служебное расследование.

2.10.5. Уполномоченным работником подразделения ИТ проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.10.6. При необходимости уполномоченным работником подразделений ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.11. Невыполнение установленных правил ИБ (правил работы в ИСПДн), использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации.

2.11.1. Работником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность: непосредственный руководитель и руководитель подразделения ИБ.

2.11.2. Администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента.

2.11.3. Об обнаруженном факте администратор безопасности докладывает руководителю подразделения ИБ.

2.11.4. При необходимости по решению руководителя подразделения ИБ по фактам выявленных нарушений Группой реагирования на инциденты ИБ проводится служебное расследование.

2.12. Ошибки работников.

2.12.1. В случае возникновения сбоя, связанного с ошибками работников, руководитель подразделения _____ (территориального органа _____), в котором произошел инцидент, ставит в известность уполномоченного работника подразделения ИТ и руководителя подразделения ИБ.

2.12.2. Администратором безопасности и уполномоченным работником подразделения ИТ проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных.

2.12.3. При необходимости уполномоченным работником подразделения ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.12.4. В случае нанесения _____ (территориальному органу _____) значительного ущерба вследствие ошибок работников Группой реагирования на инциденты ИБ проводится служебное расследование.

2.13. Отказ в обслуживании.

2.13.1. Работником, обнаружившим отказ в обслуживании, ставятся в известность: непосредственный руководитель и руководители подразделений

ИТ и ИБ.

2.13.2. Уполномоченным работником подразделения ИТ и администратором безопасности проводится анализ с целью определения причин, вызвавших отказ в обслуживании.

2.13.3. Уполномоченным работником подразделения ИТ проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов.

2.13.4. При необходимости, уполномоченным работником подразделения ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

2.13.5. О причинах инцидента и принятых мерах уполномоченный работник подразделения ИТ информирует руководителя подразделения ИБ.

2.14. Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн.

2.14.1. В случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором безопасности проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента.

2.14.2. Уполномоченным работником подразделения ИТ проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП.

2.14.3. Об инциденте администратор безопасности докладывает руководителю подразделения ИБ.

2.15. Техногенные и природные проявления нештатных ситуаций.

2.15.1. При стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), работнику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других работников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему непосредственному руководителю и администратору безопасности.

2.15.2. После оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента.

2.15.3. Комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

46. Руководство администратора по обеспечению безопасности информационной системы персональных данных.

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201_ г.

Типовая форма
руководства администратора по обеспечению безопасности информационной системы персональных данных.

Санкт-Петербург 201__

СОДЕРЖАНИЕ

Общие положения

1.1. Администратор безопасности ИСПДн (далее – Администратор) назначается приказом.

1.2. Администратор подчиняется _____.

1.3. Администратор в своей работе руководствуется настоящей инструкцией, государственной политикой Санкт-Петербурга в сфере информатизации и связи, руководящими и нормативными документами ФСТЭК России и регламентирующими документами органа исполнительной власти _____ (наименование).

1.4. Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн и средств защиты, при обработке персональных данных.

1.5. Методическое руководство работой Администратора осуществляется ответственным за обеспечение защиты персональных данных.

Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);

- аппаратных средств;

- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защиты, в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля Оператором ИСПДн.

2.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий безопасности информации.

2.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

2.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.15. Не допускать к работе на рабочих станциях и серверах структурного подразделения посторонних лиц;

2.16. Осуществлять контроль монтажа оборудования структурного подразделения специалистами сторонних организаций;

2.17. Участвовать в приемке для нужд структурного подразделения новых программных средств;

2.18. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию;

2.19. При изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС, обрабатывающей информацию ограниченного доступа;

Инструкция
администратору по обеспечению безопасности информационных систем персональных данных *(наименование оператора)*

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет основные обязанности, права и ответственность администратора безопасности ИСПДн *(наименование оператора).*

1.2. Администратор безопасности назначается руководителем оператора или начальником подразделения, ответственного за обеспечение безопасности ПДн.

1.3. Администратор безопасности в своей работе руководствуется настоящей инструкцией и *(указываются действующие внутренние организационно-распорядительные документы, регламентирующие обработку ПДн у оператора).*

1.4. Администратор безопасности является ответственным должностным лицом, уполномоченным на проведение работ по поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.

1.5. Администратор безопасности осуществляет методическое руководство операторов, системных администраторов и других лиц, допущенных к работе в ИСПДн, в вопросах обеспечения защиты ПДн.

1.6. Требования администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.

1.7. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Администратор безопасности обязан:

2.2.1. Знать перечень и состав ИСПДн, перечень задач, решаемых их использованием.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий защиты ПДн.

2.2.3. Осуществлять установку, настройку и сопровождение СЗИ.

2.2.4. Осуществлять учет применяемых СЗИ, эксплуатационной и технической документации к ним.

2.2.5. Участвовать в контрольных и тестовых испытаниях и проверках элементов ИСПДн.

2.2.6. Участвовать в приемке новых программных средств.

2.2.7. Обеспечить доступ к защищаемой информации пользователям ИСПДн согласно Разрешительной системы доступа к информационным ресурсам, программным и техническим средствам ИСПДн.

2.2.8. Уточнять в установленном порядке обязанности пользователей ИСПДн.

2.2.9. Проводить резервирование ПДн.

2.2.10. Вести учет носителей ПДн.

2.2.11. Выдавать пользователям личные пароли доступа к средствам ИСПДн.

2.2.12. Анализировать состояние защиты ИСПДн и ее отдельных подсистем.

2.2.13. Контролировать неизменность состояния СЗИ их параметров и режимов защиты.

2.2.14. Контролировать физическую сохранность средств и оборудования ИСПДн.

2.2.15. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также правильность работы с элементами ИСПДн и СЗИ.

2.2.16. Контролировать исполнение пользователями парольной защиты.

2.2.17. Контролировать работу пользователей в сетях общего пользования и международного обмена.

2.2.18. Своевременно анализировать журналы учета событий, с целью выявления возможных нарушений.

2.2.19. Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.2.20. Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования СЗИ ИСПДн.

2.2.21. Оказывать помощь пользователям ИСПДн в части применения СЗИ и консультировать по вопросам введенного режима защиты.

2.2.22. Периодически представлять руководству отчет о состоянии защиты ИСПДн, о нештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.2.23. В случае отказа работоспособности СЗИ ИСПДн принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.2.24. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью ликвидации их последствий, участвовать в расследовании причин их возникновения.

3. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Личные пароли доступа к средствам ИСПДн выдаются пользователям администратором безопасности, ответственным за обеспечение безопасности ПДн или другим уполномоченным лицом.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- запрещается выбирать пароли, которые уже использовались ранее.

4. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

4.1. Администратор безопасности имеет право:

4.1.1. Отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке.

4.1.2. В установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн.

4.1.3. Требовать от сотрудников соблюдения правил работы в ИСПДн, приведенных в должностных инструкциях.

4.1.4. Требовать от пользователей безусловного соблюдения установленной технологии обработки ПДн и выполнения требований локальных документов, регламентирующих вопросы обеспечения защиты ПДн.

4.1.5. Требовать прекращения обработки информации в случае нарушения установленной технологии обработки ПДн или нарушения функционирования СЗИ.

4.1.6. Вносить свои предложения по совершенствованию СЗПДн.

4.1.7. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты ПДн в ИСПДн.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

5.1. Администратор безопасности несет ответственность:

5.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими локальными организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.

5.1.2. За правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.1.3. За разглашение сведений конфиденциального характера и другой защищаемой информации в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5.1.4. На администратора безопасности возлагается персональная ответственность за работоспособность и надлежащее функционирование СЗИ ИСПДН.

47. Типовая форма журнала учета средств криптографической защиты информации

Журнал поэкземплярного учета средств криптографической защиты информации

Журнал начат “ _____ ’ _____ 201 ___ г.

_____
(должность)

_____ / /
(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201 ____

_____
(должность)

_____ / /
(Ф.И.О. должностного лица)

На _____ листах

№ п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДН			Примечание
			От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, Произведших подключение (установку)	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата Подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14

48. Типовая форма журнала ключевой информации

ЖУРНАЛ
учета носителей ключевой информации
в _____
(наименование органа)

Журнал начат “ _____ ’ _____ 201___ г.

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201 _

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

На _____ листах

№	Тип носителя	Учетный номер	Назначение (система использования)	Дата	Кол-во	НКИ получил (ФИО, должность, подпись)	С правилами пользования ознакомлен (дата, подпись)	НКИ сдал (ФИО, дата, подпись принявшего)	Примечание

*если один и тот же ключевой носитель многократно используется для записи криптографических ключей, то его каждый раз регистрировать отдельно.

49. Типовая форма журнала выдачи носителей ключевой информации

ЖУРНАЛ
учета выдачи носителей ключевой информации
в _____
(наименование органа)

Журнал начат “ _____ ’ _____ 201___ г.

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201 _

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

На _____ листах

№	Дата	Место хранения	Назначение	НКИ получил (ФИО, должность, подпись)	НКИ сдал (ФИО, дата, подпись принявшего)	Причина сдачи/получения	Примечание

50. Типовая форма

журнала учета сертифицированных средств защиты информации,
эксплуатационной и технической документации к ним

Журнал начат “ _____ ’ _____ 201 ___ г.

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201 _

_____
(должность)

_____ / _____ /
(Ф.И.О. должностного лица)

На _____ листах

Номер п/п	**Индекс и наименование средства защиты информации, эксплуатационной и технической документации**	**Серийный (заводской) номер**	**Номер специального защитного знака**	**Наименование организации, установившей СЗИ**	**Место установки**	**Примечание**
1	СЗИ1	EAV-03569286	А 479355		ИСПДн «_____»	Сертификат ФСТЭК России № ____, действителен до _____
2	СЗИ2	455355	В 455355		ИСПДн «_____»	Сертификат ФСТЭК России № ____, действителен до _____
3	Инструкция по эксплуатации СЗИ1				Выдана ответственному _____	ФИО Подпись

51. Список лиц, допущенных к работе на автоматизированных системах или информационных системах персональных данных.

Типовая форма
списка лиц, допущенных к работе на АС (ИСПДн) _____

№ п/п	№ отдела	Должность	Фамилия и инициалы
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

Руководитель _____

“____” _____ 201__ г.

52. Акт определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)

(для каждой ИСПДн)

АКТ № 1
определения уровня защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн)

«Название ИСПДн»

В соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом _____ от «___» _____ № ____ комиссия в составе:
председатель комиссии: должность Фамилия И. О.,
члены комиссии: должность Фамилия И. О.,
должность Фамилия И. О.,
произвела сбор данных об информационной системе персональных данных и установила нижеследующее:
1) в информационной системе персональных данных (ИСПДн) обрабатываются персональные данные иных категорий персональных данных сотрудников оператора;
2) в ИСПДн одновременно обрабатываются персональные данные менее чем 100 000 субъектов персональных данных;
3) по структуре ИСПДн относится к локальной информационной системе, состоящей из нескольких из нескольких АРМ и серверов;
4) по наличию подключений к сетям международного информационного обмена (Интернет) информационная система относится к системам, не имеющим подключения;
5) по режиму обработки персональных данных в информационной системе ИСПДн относится к многопользовательским;
6) по разграничению прав доступа пользователей ИСПДн относится к системам с разграничением прав доступа;
7) в зависимости от местонахождения технических средств ИСПДн относится к системам, технические средства которых размещены в Российской Федерации;
8) речевая обработка сведений составляющих ПДн в информационной системе не осуществляется.
9) условие обработки персональных данных — для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории

персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками оператора.

В соответствии с Постановлением Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных информационной системе персональных данных «Название ИСПДн» установить уровень защищенности **4.**

Председатель комиссии:
Фамилия И. О. _____"___"_____ 201_
члены комиссии:
Фамилия И. О. _____"___"_____ 201_
Фамилия И. О. _____"___"_____ 201_

53. Акт установки средств защиты информации на объекте вычислительной техники - автоматизированное рабочее место

Типовая форма акта
установки средств защиты информации
на объекте вычислительной техники - автоматизированное рабочее место
на базе автономной ПЭВМ (инв. № _____)

«____» _____ 201_ года произведена установка следующих средств защиты информации:

№ п/п	Наименование и тип технического средства	Заводской (серийный) номер	Сведения о сертификате	Место и дата установки
1	Система защиты информации от НСД «ViP№et SafeDisk»		Сертификат ФСТЭК России № 1812 от 31.03.2019 Сертификат ФСБ России № СФ/144-1184 от 16.09.2008	В ПЭВМ АРМ Инв. № _____
2	Межсетевой экран «ViP№et Perso№al Firewall»		Сертификат ФСБ России № СФ/115-1285 от 27.02.2019	В ПЭВМ АРМ Инв. №

Монтаж средств защиты информации выполнен в соответствии с требованиями технической документации. В ходе инструментальной проверки установлено, что средства защиты информации работоспособны и обеспечивают защищенность информации.

После установки комплекса СЗИ от НСД «ViP№et SafeDisk» «ViP№et Perso№al Firewall» системный блок инв. № _____ опломбирован пломбой органа исполнительной власти или организации чей печатью опломбирован системный блок.

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

54. Акт об уничтожении материальных(машинных, бумажных носителей) конфиденциальной информации, персональных данных

Типовая форма акта
об уничтожении материальных (машинных, бумажных носителей)
конфиденциальной информации, персональных данных

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор материальных (машинных, бумажных носителей) носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации
_____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего материальных (машинных) носителей
_____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)
Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/

Примечание:

1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

55. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

и

МОДЕЛЬ НАРУШИТЕЛЯ

(примерная форма)

автоматизированной системы в защищенном исполнении

Санкт-Петербург

201_

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
АСЗИ	Автоматизированная система в защищенном исполнении
ДСП	Для служебного пользования
ЕМТС	Единая мультисервисная телекоммуникационная сеть
ЗАГС	Запись актов гражданского состояния
ИОГВ	Исполнительные органы государственной власти
ИР	Информационные ресурсы
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
РД	Руководящий документ
СЗИ	Система защиты информации
СрЗИ	Средство защиты информации
УЗ	Уровень защищенности

ОПРЕДЕЛЕНИЯ

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Государственный стандарт Российской Федерации «Комплекс стандартов на автоматизированные системы. Автоматизированные системы», (далее - ГОСТ 34.003 – 90).

Защита информации (далее – ЗИ) от НСД - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации (Государственный стандарт Российской Федерации «Защита информации. Основные термины и определения», (далее- ГОСТ Р 50922 – 2006).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922 – 2006).

Информационная система персональных данных - совокупность содержащихся в базах данных (далее – БД) ПДн и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных", (далее 152-ФЗ).

Контролируемая зона - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. («Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее - СТР – К).

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не

передавать такую информацию третьим лицам без согласия ее обладателя (Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", (далее 149-ФЗ).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (152-ФЗ).

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (149-ФЗ).

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 (152-ФЗ).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (152-ФЗ).

Персональные данные – персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (152-ФЗ).

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (152-ФЗ).

Поставщик информации – специализированная компания, предоставляющая разнообразные сведения для анализа и принятия инвестиционных решений (149-ФЗ).

Потребитель информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею (149-ФЗ).

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (152-ФЗ).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (Государственный стандарт Российской Федерации «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования», далее ГОСТ Р 51624 – 2000).

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 (152-ФЗ).

ВВЕДЕНИЕ

В настоящем документе представлена Модель угроз безопасности персональных данных (далее – Модель угроз) и модель нарушителя информационной системы персональных данных (далее – ИСПДн) автоматизированной системы в защищенном исполнении _____Санкт-Петербурга (далее – АСЗИ_____).

Модель угроз разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152–ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 № 17 «О защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер безопасности персональных данных при их обработке в информационных системах персональных данных».

Модель угроз предназначена для определения требований по защите персональных данных (далее – ПДн) в ИСПДн АСЗИ _____и обоснования выбора организационно–технических мер и технических средств защиты информации (далее – СрЗИ) в системе защиты ПДн АСЗИ _____.

Представленная ниже Модель угроз включает общее описание особенностей ИСПДн АСЗИ _____, определяющих выбор актуальных угроз безопасности ПДн и самих актуальных угроз. На основе этого материала делается вывод об актуальности для ИСПДн АСЗИ _____каждого из видов угроз.

Актуальность угроз безопасности ПДн определяется на основе оценки уровня исходной защищенности ИСПДн АСЗИ _____и вероятности реализации угроз.

Полученные данные дополняются данными о принятых мерах защиты, которые делают экспертные оценки более прозрачными и обоснованными.

Общие положения

1.1 Общие сведения о работе

Модель угроз, представленная в настоящем документе, разработана в рамках работ по развитию АСЗИ _____и представляет один из отчетных документов по этой работе.

При разработке Модели угроз использованы материалы:

- «Отчета об обследовании АСЗИ _____»;
- «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008;
- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008

Включенный в Модель перечень угроз соответствует «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной заместителем директора ФСТЭК России 15.02.2008 и Приказу ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2 Основания для выполнения работы

Работа выполнена на основании следующих документов:

1. Государственный контракт № от 00.00.201__ по развитию АСЗИ _____Санкт-Петербурга для государственных нужд Санкт-Петербурга в 201_ году, заключенного между _____ и_____.
2. Техническое задание к Государственному контракту № 00 от 00.00.201_ на проведение работ по развитию АСЗИ _____Санкт-Петербурга.

1.3 Перечень организаций, участвующих в работе

Заказчик:	
Исполнитель работ:	
Получатель услуг:	

1.4 Сроки выполнения работы

Начало выполнения работ – с момента подписания Государственного контракта.

Срок завершения выполнения работ – 00.00.201_ г.

1.5 Общие сведения об АСЗИ _____

АСЗИ _____– автоматизированная система в защищенном исполнении, предназначенная для комплексной автоматизации работы _____и его территориально-удаленных структурных подразделений, а также для обеспечения взаимодействия с другими ведомствами в случаях, предусмотренных законодательством РФ.

Защищаемой информацией являются ПДн по личному составу _____а, а также технологическая и общедоступная информация, в соответствии с Перечнем сведений конфиденциального характера, утвержденным приказом «О мерах по защите персональных данных» от 00.00.201_г. № 0).

1.6 Перечень законодательных, руководящих и нормативных документов, использованных при разработке Модели угроз

1. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ.
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149 – ФЗ.
3. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ;
4. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
5. Постановление Правительства РФ от 24.11.2009 № 953 "Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти";
6. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер безопасности персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15.02.2008;
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14.02.2008.
11. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997 г.).
12. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», Утверждены Руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-662.
13. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Гостехкомиссия России, 2002 г.).
14. Методические рекомендации с помощью криптосредств безопасности персональных данных при их обработке в информационных системах

персональных данных с использованием средств автоматизации. Утверждены Руководством 8 Центра ФСБ России 21.02.2008 №149/54-144.
15. ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
16. ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем.
17. ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
18. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
19. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
20. ГОСТ Р 51583-2000 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
21. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении.
22. РД 50-682-89 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения.
23. РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения.
24. РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

1. Общая характеристика ИСПДн АСЗИ

АСЗИ _____– автоматизированная система в защищенном исполнении, *предназначенная* для автоматизированной обработки информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также обеспечения ее конфиденциальности на всех этапах обработки в АСЗИ _____в соответствии с классом защищенности АСЗИ _____, классом ИСПДн и установленными правами и правилами доступа.

Обладателем информации, обрабатываемой в АСЗИ _____, является _____

Оператором АСЗИ _____является АСЗИ _____.

На основании Федеральных законов «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ и

«О персональных данных» от 27.07.2006 №152-ФЗ АСЗИ _____относится к информационной системе персональных данных.

В соответствии с Перечнем сведений конфиденциального характера, утвержденным председателем _____а, в АСЗИ _____обрабатываются следующие виды информации, относящиеся к информации ограниченного доступа:персональные данные кадрового состава _____а и лиц, включенных в кадровый резерв _____а;технологическая информация (совокупность документов, содержащих технологическую информацию, и сведения, раскрывающие систему защиты информации);сведения, раскрывающие организацию, содержание планируемых и (или) проводимых мероприятий в области технической защиты информации _____а, носящие конфиденциальный характер;сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с действующим законодательством Российской Федерации, Санкт-Петербурга и приказами _____ (информация для служебного пользования, обрабатываемая на выделенном АРМ и на учтенных машинных носителях).Основные характеристики ИСПДн АСЗИ _____, необходимые для разработки Модели угроз, приведены в таблице 1.

Таблица 1 - Основные характеристики ИСПДн АСЗИ _____

Характеристики ИСПДн	**Характеристики ИСПДн АСЗИ _____**
Категории ПДн	Иные
Уровень значимости информации	Четвертый уровень значимости информации (УЗ 4)
Масштаб	Объектовый
Актуальность угроз	Угрозы 3-го типа
Количество субъектов, ПДн которых обрабатываются в ИСПДн	Около 500 субъектов ПДн, являющихся сотрудниками оператора
Уровень защищенности ИСПДн	Четвертый уровень защищенности

2. Описание модели угроз

В Модели угроз представлено описание структуры АСЗИ _____, состава ПДн и режима их обработки, проведена классификация потенциальных нарушителей и дана оценка исходного уровня защищенности (далее – УЗ), проведен анализ угроз безопасности ПДн.

Анализ угроз безопасности ПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности ПДн с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИС.

Учитывая многообразие потенциальных угроз безопасности государственных ИР Санкт-Петербурга, а также участие человека в технологическом процессе сбора, обработки и передачи данных, гарантированное обеспечение защиты информации может быть достигнуто только путем постоянного поддержания АСЗИ _____в актуальном состоянии с учетом требований действующего законодательства. Развитие АСЗИ _____необходимо начинать с оценки угроз в деятельности объекта защиты, на основе которой в дальнейшем должны приниматься решения по доработке АСЗИ _____.

3. Модель нарушителя безопасности информации в АСЗИ _____

4.1 Нарушитель

Нарушитель безопасности ПДн - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн. Все физические лица, имеющие доступ к программным и техническим средствам АСЗИ _____, разделяются на следующие категории:

- категория 1 – лица, не имеющие права доступа в контролируемую зону (далее - КЗ) АСЗИ _____;
- категория 2 – лица, имеющие право постоянного или разового доступа в КЗ АСЗИ _____.

Потенциальные нарушители в свою очередь подразделяются на внешних и внутренних:

– *внешний* нарушитель осуществляет атаки из-за пределов КЗ АСЗИ _____(могут быть лица 1 и 2 категории);
– *внутренний* нарушитель осуществляет атаки, находясь в пределах КЗ АСЗИ _____(могут быть лица только 2 категории).

Целями вероятного нарушителя, реализующего субъективные угрозы в своих интересах, являются:

– возможность внесения изменений в ПДн сотрудников _____а, обрабатываемые в Отделе по вопросам государственной службы и кадров и Финансово-бухгалтерском отделе и их уничтожения, а также нарушение возможности доступа к информационным ресурсам;
– доступ к сведениям, раскрывающим систему защиты информации, организацию, содержание планируемых и (или) проводимых мероприятий в области технической защиты информации _____а, и информации, связанной с профессиональной деятельностью, доступ к которой ограничен в соответствии с действующим законодательством Российской Федерации, Санкт-Петербурга и приказами _____.

4.1.1 Внешний нарушитель

Внешний нарушитель может быть источником угроз утечки информации по техническим каналам, а также угроз НСД в АСЗИ _____.

Внешний нарушитель может воздействовать на:

– ресурс (на операционную систему, на сетевые службы, на информацию, обрабатываемую сетевыми службами);
– канал связи (на сетевое оборудование или на протоколы связи);
– персонал АСЗИ _____. Воздействие на персонал может быть как физическое, так и психологическое (с целью получения информации или с целью нарушения непрерывности функционирования АСЗИ _____).

Внешний нарушитель имеет следующие возможности:

– осуществлять несанкционированный доступ (далее - НСД) к каналам связи, выходящим за пределы КЗ АСЗИ _____;
– осуществлять НСД к защищаемым ИР АСЗИ _____с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок;
– осуществлять НСД через элементы информационной инфраструктуры АСЗИ _____, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами КЗ;
– осуществлять НСД через взаимодействующие ИС при их подключении к АСЗИ _____.

НСД к каналам связи, выходящим за пределы КЗ АСЗИ _____, исключен из-за того, что для

передачи данных используется защищенный сегмент единой мультисервисной телекоммуникационной сети (далее – ЕМТС).

Описание каждой категории внешних нарушителей приведено в таблице 2.

Таблица 2 - Классификация внешних нарушителей

Категория (вид) нарушителя, обозначение	**Квалификация**	**Канал атаки**	**Техническая оснащенность**	**Степень опасности**
Посетители организаций, являющихся объектами информатизации АСЗИ _____ _____, имеющие право постоянного или разового доступа в КЗ АСЗИ _____ _____	Может быть высокой. При этом опыт мошенничества выше, чем опыт владения информационными технологиями	Машинные носители информации	Программные средства для взлома компьютера, являющегося целью преступления	Средняя
Лица, не имеющие права доступа в КЗ АСЗИ _____ _____ и использующие технические средства ведения разведки или закладочные устройства	Высокая. Опыт получен в процессе профессиональной деятельности	Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический)	Технические средства перехвата без модификации компонентов системы	Низкая

4.1.2.Внутренний нарушитель

Внутренний нарушитель является источником угроз НСД к информации. Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах КЗ АСЗИ _____организационно-технических мер защиты, в том числе по допуску физических лиц к ПДн и контролю порядка проведения работ.

Внутренний нарушитель АСЗИ _____имеет следующие возможности:

- осуществлять НСД к каналам связи в пределах контролируемой зоны;
- осуществлять НСД к защищаемым информационным ресурсам через АРМ пользователей и обслуживающего персонала;
- осуществлять НСД к техническим средствам обработки защищаемых информационных ресурсов АСЗИ _____;
- осуществлять НСД к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, программных закладок.

Внутренние нарушители подразделяются на категории в зависимости от способа доступа и полномочий доступа к АСЗИ _____.

Внутренним нарушителем может быть лицо из следующих категорий персонала:

- лица, имеющие санкционированный доступ в КЗ, но не имеющие доступа к ИР АСЗИ _____;
- пользователи программно-технических средств АСЗИ _____(в т.ч. осуществляющие удаленный доступ к информационным ресурсам по защищенному сегменту ЕМТС);
- обслуживающий персонал АСЗИ _____.

Более подробно описание внутренних нарушителей АСЗИ _____приведено в таблице 3.

Таблица 3 - Классификация внутренних нарушителей

Категория (вид) нарушителя, обозначение	**Квалификация**	**Канал атаки**	**Техническая оснащенность**	**Степень опасности**
Сотрудники, имеющие санкционированный доступ в КЗ, но не имеющие доступа к информационным ресурсам АСЗИ _____ _____ ____	Низкая. Обладает знаниями в рамках должностных обязательств	Машинные носители информации; носители информации, выведенные из употребления; каналы связи внутри КЗ	Основное компьютерное оборудование. В некоторых случаях может использоваться более сложная аппаратура	Низкая

Категория (вид) нарушителя, обозначение	Квалификация	Канал атаки	Техническая оснащенность	Степень опасности
Пользователь, имеющий ограниченные права доступа к информационным ресурсам АСЗИ _____ _____ ____со своего рабочего места	Низкая. Обладает знаниями в рамках должностных обязательств	Машинные носители информации; каналы связи внутри КЗ	Основное компьютерное оборудование. В некоторых случаях может использоваться более сложная аппаратура	Средняя
Пользователь, имеющий ограниченные права доступа к информационным ресурсам АСЗИ _____ _____ ____со своего рабочего места	Низкая. Обладает знаниями в рамках должностных обязательств	Машинные носители информации; каналы связи внутри КЗ	Основное компьютерное оборудование. В некоторых случаях может использоваться более сложная аппаратура	Средняя
Пользователь с полномочиями системного администратора	Высокая. Опыт получен в процессе профессиональной деятельности	Машинные носители информации; каналы связи внутри КЗ	Технические средства обработки данных и системное ПО	Высокая
Пользователь с полномочиями администратора безопасности	Высокая. Опыт получен в процессе профессиональной деятельности	Программно-технические средства обработки информации; каналы связи внутри КЗ	Прикладное ПО	Высокая
Представители организаций, осуществляющих разработку и сопровождение прикладного ПО объектов информатизации	Высокая. Знает функциональные особенности, основные закономерности формирования массивов данных и потоков запросов к ним, а также умеет пользоваться основными техническими средствами и системами	Программные средства обработки информации	Модернизированные программные средства Штатные средства и недостатки СЗИ для ее преодоления	Средняя
Лица, обеспечивающие поставку, сопровождение и ремонт технических средств	Обладает высоким уровнем знаний и опытом работы с программно-техническими средствами, и их обслуживанием	Машинные носители информации; носители информации, выведенные из употребления	Основные технические средства и системы	Средняя

Каждый из перечисленных внутренних пользователей в соответствии с соответствующей степенью опасности (низкая опасность – средняя опасность

– высокая опасность) может нанести больший или меньший ущерб системе и реализовать ту или иную угрозу безопасности информации АСЗИ _____.

Наибольшую вероятность реализовать угрозы безопасности информации и нанести ущерб АСЗИ _____имеют пользователи с полномочиями системного администратора и администратора безопасности АСЗИ _____, а также представители организаций, осуществляющих разработку прикладного программного обеспечения (далее – ПО) объектов информатизации АСЗИ _____и сотрудники организации, обеспечивающей функционирование, сопровождение, настройку и ремонт системы.

Совмещение полномочий одним лицом рассматривается как совмещение полномочий внутренних потенциальных нарушителей. Вероятность реализации угроз возрастает также при усилении функций (увеличение полномочий) внутренних потенциальных нарушителей при уменьшении количества лиц, наделенных указанными полномочиями (например, выполнение функций по системному администрированию, администрированию баз данных, администрированию систем защиты информации (далее – СЗИ) и выполнение контроля одним лицом).

4. Оценка уровня исходной защищенности

5.1 Методика оценки исходной защищенности

Исходная защищенность ИСПДн оценивается по «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ФСТЭК России, 2008 г.). Согласно Методике уровень исходной защищенности определяется по показателям, приведенным в таблице 3.

Таблица 3 -Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики	**Уровень защищенности**
По территориальному размещению – *корпоративная, распределенная* информационная система – состоит из комплексов автоматизированных рабочих мест и локальных информационных систем, расположенных в различных подразделениях Санкт-Петербурга	средний
По наличию соединения с сетями общего пользования – *имеет одноточечный выход в сеть общего пользования*	средний
По встроенным (легальным) операциям с записями баз ПДн – *модификация, передача*	низкий
По разграничению доступа к ПДн – *к АСЗИ имеет доступ пределенный перечень сотрудников*	средний
По наличию соединений с другими базами ПДн иных информационных систем ПДн – *все базы ПДн принадлежат у по делам ЗАГС (организации – оператору АСЗИ)*	высокий
По уровню обобщения (обезличивания) ПДн – *предоставляемые пользователю данные не являются обезличенными (присутствует информация, позволяющая идентифицировать субъекта ПДн)*	низкий
По объему ПДн, которые предоставляются сторонним пользователям без предварительной обработки – *предоставляет часть ПДн*	средний

ИСПДн имеет высокий исходный уровень защищенности, если не менее 70% показателей соответствуют уровню «высокий», а остальные «средний». В этом случае Y_1=0.

ИСПДн имеет средний исходный уровень защищенности, если «высоких» и «средних» оценок не менее 70% («низких» оценок не более 30%). В этом случае Y_1=5.

Во всех остальных случаях ИСПДн имеет низкий исходный уровень защищенности, Y_1=10.

Таким образом, ИСПДн имеет средний исходный уровень защищенности => $\mathbf{Y_1 = 5}$

5.2 Вероятность реализации угроз информационной безопасности ПДн

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

- ***маловероятно*** – отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);
- ***низкая вероятность*** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);
- ***средняя вероятность*** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);
- ***высокая вероятность*** – объективные предпосылки для реализации угрозы существуют и меры безопасности ПДн не приняты ($Y_2 = 10$).

5.3 Угрозы информационной безопасности

Угрозы утечки информации по техническим каналам

Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн при обработке ПДн в ИСПДн возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн АСЗИ _____функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – ***маловероятна.***

Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико–электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно–вычислительных комплексов, технических средств обработки графической, видео и буквенно–цифровой информации, входящих в состав ИСПДн.

На объектах _____реализован комплекс организационно–технических мероприятий по контролю доступа в контролируемую зону (внутриобъектовый режим). АРМ ИСПДн расположены внутри контролируемой зоны. Размещение ОТСС ИСПДн фактически исключает возможность визуального просмотра посторонними лицами информации на мониторе.

Вероятность реализации угрозы – ***маловероятна.***

Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН возможны из–за наличия паразитных электромагнитных излучений у элементов ИСПДн.

Угроза утечки информации, содержащей ПДн, по каналу ПЭМИН возможна за счет перехвата техническими средствами разведки за пределами контролируемой зоны ПЭМИН, возникающих при обработке ПДн средствами вычислительной техники ИСПДн. Наиболее опасным режимом работы средств вычислительной техники является вывод информации на экран монитора автоматизированного рабочего места оператора (пользователя) ИСПДн.

В качестве наиболее вероятного нарушителя, ведущего разведку ПЭМИН, необходимо рассматривать внешнего нарушителя, действующего за пределами контролируемой зоны.

Угрозы данного класса являются ***маловероятными***, что обусловлено достаточным размером контролируемой зоны и размещением элементов ИСПДн, находящихся на удаленном расстоянии от ее границы. Комплекс реализованных организационных мероприятий, в том числе реализованный объектовый (пропускной) режим, существенно снижают вероятность реализации угроз данного класса.

Угрозы несанкционированной идентификации и аутентификации

Угроза осуществляется за счет действия пользователей ИСПДн, которые нарушают положения парольной политики в части создания паролей (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.), их хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них, вследствие чего становится возможен несанкционированный доступ к ПДн посредством подмены, подбора, расшифровки идентификационной и аутентификационной информации.

В _____е введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, осуществляется контроль за ее выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей.

Оценки вероятности реализации угроз (Y_2) безопасности данного типа приведены в таблице 4.

Угрозы среды виртуализации

Угрозы данного типа реализуются за счёт НСД как к компонентам виртуальной инфраструктуры, так и к средствам управления данной виртуальной инфраструктурой.

Угрозы среды виртуализации возникают вследствие следующих особенностей виртуальной среды:

– информация обрабатывается в гостевых машинах, которые находятся под полным контролем гипервизора, способного абсолютно незаметно для традиционных средств защиты информации перехватывать все данные, идущие через устройства (см. рисунок 1);

– администратор виртуальной инфраструктуры, имеющий права доступа к гипервизору может получить доступ к информационным ресурсам в обход существующей политики информационной безопасности.

Средства управления виртуальной инфраструктурой представляют собой самостоятельный объект атаки, проникновение в который дает возможность нарушителю получить доступ к гипервизорам серверов виртуализации, а затем к ПДн, обрабатываемым на гостевых машинах.

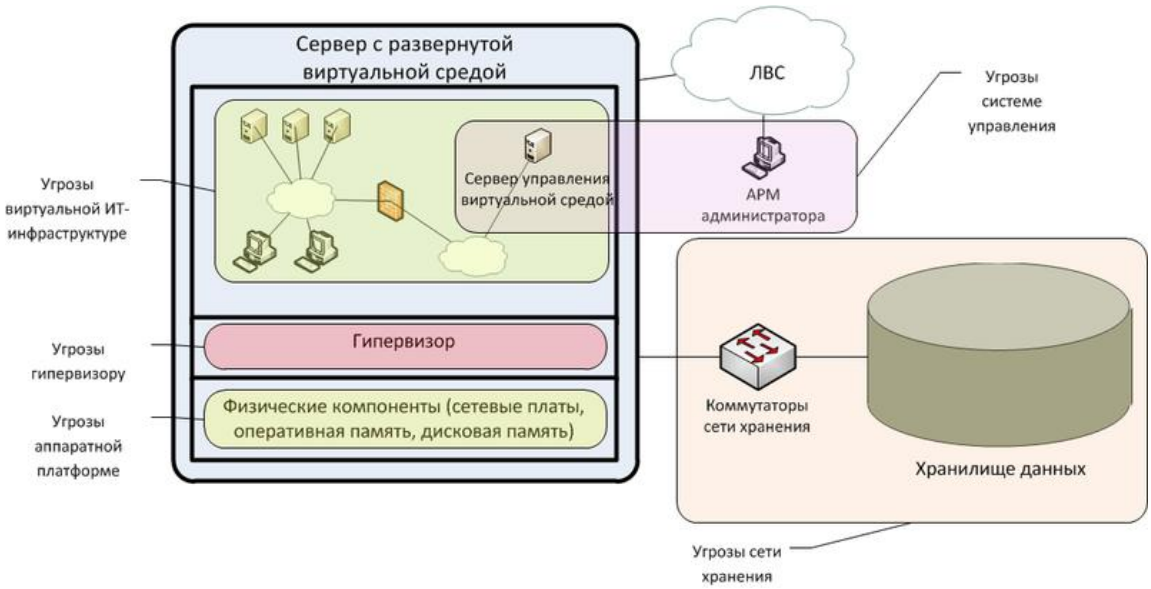


Рисунок 1 – Защита в виртуальной среде

Т.к. среда виртуализации в ИСПДн отсутствует, вероятность реализации угрозы – ***маловероятна.***

Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

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

Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

Вследствие реализации внутриобъектового и пропускного режимов, распределения персональных обязанностей, вынос компьютерной техники за пределы контролируемой зоны возможен только по предварительному согласованию, под контролем администраторов АСЗИ _____.

Вероятность реализации угрозы – ***маловероятна.***

Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

Введен контроль доступа в КЗ, двери закрываются на замок, доступ в функциональные зоны безопасности имеют исключительно авторизованные сотрудники.

Вероятность реализации угрозы – ***маловероятна.***

Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

Введен контроль доступа в КЗ, двери закрываются на замок, доступ в функциональные зоны безопасности имеют исключительно авторизованные сотрудники, ведется учет и хранение носителей в специально отведенных местах, реализована политика «чистого стола». Уборка и регламентные работы в помещениях, где расположены основные технические средства и системы ИСПДн, осуществляется под контролем Руководителя _____ либо лиц, ответственных за информационную безопасность в структурных подразделениях _____а, назначенных приказом _____.

Вероятность реализации угрозы – ***маловероятна.***

Кражи, модификации, уничтожения информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

Введен контроль доступа в КЗ, двери закрываются на замок, доступ в функциональные зоны безопасности имеют исключительно авторизованные сотрудники, ведется учет и хранение носителей в специально отведенных местах, реализована политика «чистого стола». Уборка и регламентные работы в помещениях, где расположены основные технические средства и системы ИСПДн, осуществляется под контролем _____ либо лиц, ответственных за информационную безопасность в структурных подразделениях _____, назначенных приказом _____.

Прием посетителей в помещениях, где расположены основные технические средства и системы ИСПДн, не осуществляется, либо регламентирован.

Вероятность реализации угрозы – ***маловероятна.***

Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

Введен контроль доступа в КЗ, в нерабочее время двери закрываются на замок, доступ в функциональные зоны безопасности имеют исключительно авторизованные сотрудники. Уборка и регламентные работы в помещениях, где расположены основные технические средства и системы ИСПДн, осуществляется под контролем администраторов ИСПДн либо старшего, назначенного из числа сотрудников, допущенных к обработке ПДн в ИСПДн. Прием посетителей в помещениях, где расположены основные технические средства и системы ИСПДн, не осуществляется, либо регламентирован.

Вероятность реализации угрозы – ***маловероятна.***

Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ

Уборка и регламентные работы в помещениях, где расположены основные технические средства и системы ИСПДн, осуществляется под контролем администраторов ИСПДн либо старшего, назначенного из числа сотрудников, допущенных к обработке ПДн в ИСПДн. К проведению

регламентных работ по обслуживанию технических средств из состава ИСПДн допускаются сотрудники сторонних организаций с подписанием соответствующего соглашения о конфиденциальности. Подписываемое соглашение о конфиденциальности выступает в качестве меры доверия к данным сотрудникам.

Вероятность реализации угрозы – ***маловероятна***.

Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

Доступ в функциональные зоны безопасности (помещения, где расположены основные технические средства и системы ИСПДн) регламентирован и ограничен введенным внутриобъектовым режимом. Пользователи ИСПДн проинструктированы о порядке и правилах работы с ПДн с использованием ИСПДн, и осуществляют автоматизированную обработку ПДн под контролем администратора ИСПДн и руководителей соответствующих отделов.

Вероятность реализации угрозы – ***низкая вероятность***.

Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно–аппаратных и программных средств (в том числе программно–математических воздействий)

Действия вредоносных программ

Программно–математическое воздействие – это воздействие с помощью вредоносных программ (вирусы и др.). Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На всех элементах ИСПДн (кроме серверов с ОС Li№ux) установлена антивирусная защита. Реализована регламентированная система обновления

сигнатур вирусных баз. Пользователи проинструктированы о мерах предотвращения вирусного заражения. Кроме того, в программной среде ИСПДн отсутствуют средства модификации и отладки программного кода.

Вероятность реализации угрозы – ***низкая вероятность.***

Ндекларированные возможности системного ПО и ПО для обработки ПДн

Недекларированные возможности – функциональные возможности программных средств и средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

В качестве общесистемного и специального ПО используются программные средства, приобретаемые централизованно у доверенного вендора, с соблюдением авторских прав и лицензионности. Доработку и сопровождение программного обеспечения ИСПДн (БД ПДн) осуществляет доверенная организация. Соглашение о конфиденциальности, заключаемое с сотрудниками, реализующими данные функции, и, реализованная СЗИ, позволяют судить о вероятности наличия НДВ в системном и прикладном ПО АСЗИ _____. В качестве системного ПО в АСЗИ _____на серверах установлена несертифицированная операционная система ОС Windows Server 2008.

Вероятность реализации угрозы – ***средняя.***

Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все пользователи проинструктированы о политике установки ПО. Ведется контроль со стороны администраторов. На АРМ присутствуют сертифицированные средства защиты от НСД.

Вероятность реализации угрозы – ***низкая вероятность.***

Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн в ее составе из–за сбоев в программном обеспечении, 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

Угроза осуществляется за счет действия пользователей ИСПДн, которые нарушают положения парольной политики в части создания паролей (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.), их хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

Введена парольная политика, предусматривающая требуемую сложность пароля, введена политика «чистого стола», осуществляется контроль ее выполнения.

Вероятность реализации угрозы – ***средняя вероятность***.

Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

Осуществляется резервное копирование обрабатываемых ПДн. Работа в ИСПДн осуществляется под контролем администраторов.

Вероятность реализации угрозы – ***средняя вероятность***.

Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

Введен контроль доступа в КЗ, осуществляется разграничение доступа к настройкам режимов СрЗИ, пользователи проинструктированы о работе с ИСПДн. Введена многоуровневая система администрирования ИСПДн. Работы пользователей в ИСПДн осуществляются под контролем администраторов ИСПДн.

Вероятность реализации угрозы – ***низкая вероятность***.

Выход из строя аппаратно–программных средств

Угроза осуществляется вследствие несовершенства аппаратно–программных средств, из–за которых может происходить нарушение целостности и доступности защищаемой информации.

Организационно–техническими методами осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – ***низкая вероятность***.

Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из–за чего может происходить нарушение целостности и доступности защищаемой информации.

Ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – ***маловероятна***.

Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности, а также мер по предотвращению воздействия прочих техногенных факторов.

Реализованы мероприятия по действиям в условиях внештатных ситуациях и обеспечению безопасной жизнедеятельности сотрудников в процессе выполнения ими служебных обязанностей. Установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций. Серверные помещения оборудованы системой газопожаротушения.

Вероятность реализации угрозы – ***маловероятна***.

Угрозы преднамеренных действий внутренних нарушителей

Доступ к информации (модификация, уничтожение) лиц, не допущенных к ее обработке

Угроза осуществляется путем НСД внутренних нарушителей в помещения, где расположены элементы ИСПДн и СрЗИ, а также происходит работа пользователей ИСПДн.

Введен контроль доступа в КЗ, в нерабочее время двери закрываются на замок и осуществляется видеонаблюдение, доступ в функциональные зоны безопасности имеют исключительно авторизованные сотрудники. Уборка и регламентные работы в помещениях, где расположены основные технические средства и системы ИСПДн, осуществляется под контролем администраторов ИСПДн либо старшего, назначенного из числа сотрудников, допущенных к обработке ПДн в ИСПДн. Прием посетителей в помещениях, где расположены основные технические средства и системы ИСПДн, не осуществляется, либо регламентирован.

Вероятность реализации угрозы – ***маловероятна.***

Разглашение информации сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия пользователей ИСПДн, которые нарушают положения о конфиденциальности обрабатываемой информации или не осведомлены о них.

Пользователи осведомлены о порядке работы с ПДн, а также подписали Соглашение о конфиденциальности.

Вероятность реализации угрозы –***средняя.***

Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6.Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- 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 навязывания ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;

– угрозы внедрения по сети вредоносных программ.

Угроза «Анализ сетевого трафика»

Эта угроза реализуется с помощью специальной программы–анализатора пакетов (s№iffer), перехватывающей пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль. В ходе реализации угрозы нарушитель:

– изучает логику работы ИСПДн – то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

– перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TEL№ET, не предусматривающих шифрование), ее подмены, модификации и т.п.

В ИСПДн АСЗИ _____Организации используется программный комплекс «Застава-офис» версии 5.3.

С учетом архитектуры и топологии ИСПДн возможна реализация следующих угроз:

1. Перехват за переделами контролируемой зоны.

Вероятность реализации угрозы – ***маловероятна.***

2. Перехват в пределах контролируемой зоны внешними нарушителями

Вероятность реализации угрозы – ***маловероятна.***

3. Перехват в пределах контролируемой зоны внутренними нарушителями.

Вероятность реализации угрозы – ***средняя вероятность.***

Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

Вероятность реализации угрозы – ***средняя вероятность.***

Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP–spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последователь-

ного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В ИСПДн применяются стойкие пароли.

В ИСПДн АСЗИ _____Санкт-Петербурга используется, МЭ WatchGuard XTM 23-W.

Вероятность реализации угрозы – ***средняя вероятность***.

Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из–за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе АСЗИ _____. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно–адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

В ИСПДн АСЗИ _____на канальном уровне используется программный комплекс «Застава-офис» версии 5.3, что делает угрозу маловероятной.

Вероятность реализации угрозы – ***маловероятна***.

Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh–службы UNIX–хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно–адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству АСЗИ _____.

В ИСПДн АСЗИ _____используется программный комплекс «Застава-офис» версии 5.3, что делает угрозу маловероятной.

Вероятность реализации угрозы – ***маловероятна.***

Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell Net Ware; ARP, D№S, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно–адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом–жертвой, будет проходить через ложный объект сети.

В ИСПДн АСЗИ _____на канальном уровне используется программный комплекс «Застава-офис» версии 5.3, что делает невозможным внедрение ложного объекта сети.

Вероятность реализации угрозы – ***маловероятна.***

Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо–запросов по протоколу ICMP (Pingflooding), шторм запросов на установление TCP–соединений (SYN–flooding), шторм запросов к FTP–серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из–за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP–эхо–запросов (Smurf), направленный шторм (SYN–flooding), шторм сообщений почтовому серверу (Spam);
- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем

управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно–адресных данных (например, ICMP Redirect Host, D№S–flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа «Land», «TearDrop», «Bonk», «nuke», «UDP–bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа «PingDeath»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в АСЗИ _____, передача с одного адреса такого количества запросов на подключение к техническому средству в составе АСЗИ _____, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка АСЗИ _____из–за невозможности системы заниматься ничем другим, кроме обработки запросов.

На границе выхода объектов информатизации _____в ЕМТС установлены программные комплексы криптографической защиты информации «Застава» и межсетевые экраны серии Cisco ASA 5520.

Вероятность реализации угрозы – ***средняя***.

Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте АСЗИ _____различные предварительно внедренные вредоносные программы: программы–закладки, вирусы, «сетевые шпионы», основная цель которых – нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;
- удаленный запуск приложения путем переполнения буфера приложений–серверов;
- удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый

код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java–апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного «вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, «троянскими» программами типа Back.Orifice, netBus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, BackOrifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

На границе выхода объектов АСЗИ _____в ЕМТС установлены программные комплексы криптографической защиты информации «Застава» и межсетевые экраны Cisco.

Вероятность реализации угрозы – ***средняя***.

Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование не декларированных возможностей программного и программно–аппаратного обеспечения ИСПДн;
- программы–генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

На границе выхода объектов АСЗИ _____в ЕМТС установлены программные комплексы криптографической защиты информации «Застава-офис» версии 5.3 и межсетевые экраны Cisco.

Вероятность реализации угрозы – ***средняя***.

5.2 Реализуемость угроз

По итогам оценки уровня защищенности (Y_1=5) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.

Показатель Y_2 равен:

0 – для маловероятной угрозы;

2 – для низкой вероятности угрозы;

5 – для средней вероятности угрозы;

10 – для высокой вероятности угрозы.

Возможность реализации угрозы считается:

«низкой» при $0 \leq Y \leq 0,3$;

«средней» при $0,3 < Y \leq 0,6$;

«высокой» при $0,6 < Y \leq 0,8$;

«очень высокой» при $0,8 < Y$.

Оценка реализуемости УБПДн представлена в таблице 4.

Таблица 4 – Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,25	низкая
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,35	средняя
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированныевозможности системного ПО и ПО для обработки	0,5	средняя

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
персональных данных		
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,35	средняя
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.		
2.3.1. Утрата ключей и атрибутов доступа	0,5	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,5	средняя
2.3.3. Непреднамеренное отключение средств защиты	0,35	средняя
2.3.4. Выход из строя аппаратно-программных средств	0,35	средняя
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	0,25	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,5	средняя
2.5.Угрозы несанкционированного доступа по каналам связи.		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:		
2.5.1.1. Перехват за переделами с контролируемой зоны	0,25	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,5	средняя
2.5.2.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.	0,5	средняя
2.5.3.Угрозы выявления паролей по сети	0,5	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,25	низкая
2.5.5.Угрозы подмены доверенного объекта в сети	0,25	низкая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,25	низкая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,5	средняя
2.5.8.Угрозы удаленного запуска приложений	0,5	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,5	средняя

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
3. Угрозы идентификации и аутентификации		
3.1.Попытка использовать простой пароль к защищаемому ресурсу	0,25	низкая
3.2.Попытки подобрать частично известный пароль	0,25	низкая
3.3.Вход на чужой компьютер с использованием чужого пароля	0,25	низкая
4. Угрозы среды виртуализации	0,25	низкая

5.3 Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по ЗИ и определяется вербальным показателем опасности, который имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов ПДн;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

Оценка опасности угроз безопасности ПДн представлена в таблице 5.

Таблица 5 – Опасность угроз безопасности ПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	Низкая
1.2. Угрозы утечки видовой информации	Низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	Низкая
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	Средняя
2.1.2. Кража носителей информации	Высокая
2.1.3. Кража ключей и атрибутов доступа	Высокая
2.1.4. Кражи, модификации, уничтожения информации	Высокая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Средняя
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Высокая
2.1.7. Несанкционированное отключение средств защиты	Высокая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	Средняя
2.2.2. Не декларированные возможности системного ПО и ПО для обработки персональных данных	Высокая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Средняя
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и системы защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	

Тип угроз безопасности ПДн	Опасность угрозы
2.3.1. Утрата ключей и атрибутов доступа	Средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Высокая
2.3.3. Непреднамеренное отключение средств защиты	Высокая
2.3.4. Выход из строя аппаратно-программных средств	Низкая
2.3.5. Сбой системы электроснабжения	Низкая
2.3.6. Стихийное бедствие	Низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации (модификация, уничтожение) лицами, не допущенными к ее обработке	Высокая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокая
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	Средняя
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Средняя
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	Высокая
2.5.2.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.	Низкая
2.5.3.Угрозы выявления паролей по сети	Высокая
2.5.4.Угрозы навязывание ложного маршрута сети	Средняя
2.5.5.Угрозы подмены доверенного объекта в сети	Высокая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Высокая
2.5.7.Угрозы типа «Отказ в обслуживании»	Низкая
2.5.8.Угрозы удаленного запуска приложений	Средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	Низкая
3. Угрозы идентификации и аутентификации	
3.1.Попытка использовать простой пароль к защищаемому ресурсу	Низкая
3.2.Попытки подобрать частично известный пароль	Низкая
3.3.Вход на чужой компьютер с использованием чужого пароля	Средняя
4. Угрозы среды виртуализации	Низкая

5. Определение актуальности угроз в ИСПДн

В соответствии с правилами отнесения угрозы безопасности к актуальной для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6 – Правила определения актуальности угроз безопасности ПДн

Возможность реализации угрозы	**Показатель опасности угрозы**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Оценка актуальности угроз безопасности представлена в таблице 7.

Таблица 7 – Актуальность угроз безопасности ПДн

Тип угроз безопасности ПДн	**Актуальность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	Неактуальная
1.2. Угрозы утечки видовой информации	Неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	Неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	Неактуальная
2.1.2. Кража носителей информации	**Актуальная**
2.1.3. Кража ключей и атрибутов доступа	**Актуальная**
2.1.4. Кражи, модификации, уничтожения информации	**Актуальная**
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	**Актуальная**
2.1.7. Несанкционированное отключение средств защиты	**Актуальная**
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).	
2.2.1. Действия вредоносных программ (вирусов)	**Актуальная**
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	**Актуальная**
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	**Актуальная**
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и система защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.	
2.3.1. Утрата ключей и атрибутов доступа	**Актуальная**
2.3.2. Непреднамеренная модификация (уничтожение) информации	**Актуальная**

сотрудниками	
2.3.3. Непреднамеренное отключение средств защиты	**Актуальная**
2.3.4. Выход из строя аппаратно-программных средств	Неактуальная
2.3.5. Сбой системы электроснабжения	Неактуальная
2.3.6. Стихийное бедствие	Неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	**Актуальная**
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	**Актуальная**
2.5.Угрозы несанкционированного доступа по каналам связи.	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	Неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	Неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	**Актуальная**
2.5.2.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.	Неактуальная
2.5.3.Угрозы выявления паролей по сети	**Актуальная**
2.5.4.Угрозы навязывания ложного маршрута сети	Неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	**Актуальная**
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	**Актуальная**
2.5.7.Угрозы типа «Отказ в обслуживании»	Неактуальная
2.5.8.Угрозы удаленного запуска приложений	**Актуальная**
2.5.9.Угрозы внедрения по сети вредоносных программ	Неактуальная
3. Угрозы идентификации и аутентификации	
3.1.Попытка использовать простой пароль к защищаемому ресурсу	Неактуальная
3.2.Попытки подобрать частично известный пароль	Неактуальная
3.3.Вход на чужой компьютер с использованием чужого пароля	Неактуальная
4. Угрозы среды виртуализации	Неактуальная

Были выявлены следующие актуальные угрозы:

1) 2.1.2. Кража носителей информации
2) 2.1.3. Кража ключей и атрибутов доступа
3) 2.1.4. Кражи, модификации, уничтожения информации
4) 2.1.5. Вывод из строя узлов ПЭВМ, каналов связи
5) 2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ
6) 2.1.7. Несанкционированное отключение средств защиты
7) 2.2.1. Действия вредоносных программ (вирусов)
8) 2.2.2. Не декларированные возможности системного ПО и ПО для обработки персональных данных
9) 2.2.3. Установка ПО не связанного с исполнением служебных обязанностей
10) 2.3.1. Утрата ключей и атрибутов доступа
11) 2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

12) 2.3.3. Непреднамеренное отключение средств защиты

13) 2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

14) 2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

15) 2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.

16) 2.5.3.Угрозы выявления паролей по сети

17) 2.5.5.Угрозы подмены доверенного объекта в сети

18) 2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях

19) 2.5.8.Угрозы удаленного запуска приложений

В таблице 8 приведена Модель угроз безопасности ПДн ИСПДн _____.

Таблица 8 – Модель угроз безопасности ПДн ИСПДн _____.

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
1. Угрозы от утечки по техническим каналам				
1.1. Угрозы утечки акустической информации	Маловероятно	Низкая	Низкая	Неактуальная
1.2. Угрозы утечки видовой информации	Маловероятно	Низкая	Низкая	Неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	Маловероятно	Низкая	Низкая	Неактуальная
2. Угрозы несанкционированного доступа к информации				
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
2.1.1. Кража ПЭВМ	Маловероятно	Низкая	Средняя	Неактуальная
2.1.2. Кража носителей информации	Маловероятно	Низкая	Высокая	Актуальная
2.1.3. Кража ключей доступа	Маловероятно	Низкая	Высокая	Актуальная
2.1.4. Кражи, модификации, уничтожения информации.	Маловероятно	Низкая	Высокая	Актуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	Маловероятно	Низкая	Средняя	Неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Маловероятно	Низкая	Высокая	Актуальная
2.1.7. Несанкционированное отключение средств защиты	Низкая	Средняя	Высокая	Актуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);				
2.2.1. Действия вредоносных программ (вирусов)	Низкая	Средняя	Средняя	Актуальная

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	Маловероятно	Низкая	Высокая	Актуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	Низкая	Средняя	Средняя	Актуальная
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и средства защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.				
2.3.1. Утрата ключей и атрибутов доступа	Средняя	Средняя	Средняя	Актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	Средняя	Средняя	Высокая	Актуальная
2.3.3. Непреднамеренное отключение средств защиты	Низкая	Средняя	Высокая	Актуальная
2.3.4. Выход из строя аппаратно-программных средств	Низкая	Средняя	Низкая	Неактуальная
2.3.5. Сбой системы электроснабжения	Маловероятно	Низкая	Низкая	Неактуальная
2.3.6. Стихийное бедствие	Маловероятно	Низкая	Низкая	Неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	Маловероятно	Низкая	Высокая	Актуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Средняя	Средняя	Высокая	Актуальная
2.5. Угрозы несанкционированного доступа по каналам связи				
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:				
2.5.1.1. Перехват за переделами с контролируемой зоны;	Маловероятно	Низкая	Средняя	Неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	Маловероятно	Низкая	Средняя	Неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	Средняя	Средняя	Высокая	Актуальная

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы
2.5.2.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.	Средняя	Средняя	Низкая	Неактуальная
2.5.3. Угрозы выявления паролей по сети.	Средняя	Средняя	Высокая	Актуальная
2.5.4. Угрозы навязывание ложного маршрута сети.	Низкая	Низкая	Средняя	Неактуальная
2.5.5. Угрозы подмены доверенного объекта в сети.	Низкая	Низкая	Высокая	Актуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.	Низкая	Низкая	Высокая	Актуальная
2.5.7. Угрозы типа «Отказ в обслуживании».	Средняя	Средняя	Низкая	Неатуальная
2.5.8. Угрозы удаленного запуска приложений.	Средняя	Средняя	Средняя	Актуальная
2.5.9. Угрозы внедрения по сети вредоносных программ.	Средняя	Средняя	Низкая	Неактуальная
3. Угрозы идентификации и аутентификации				
3.1.Попытка использовать простой пароль к защищаемому ресурсу	Низкая	Низкая	Низкая	Неактуальная
3.2.Попытки подобрать частично известный пароль	Низкая	Низкая	Низкая	Неактуальная
3.3.Вход на чужой компьютер с использованием чужого пароля	Низкая	Низкая	Средняя	Неактуальная
4. Угрозы среды виртуализации	Низкая	Низкая	Низкая	Неактуальная

ЗАКЛЮЧЕНИЕ

_____ имеет обозначенный набор угроз, которые должны быть снижены путём модернизации АСЗИ _____и принятия особых организационно-режимных мер в организациях, обеспечивающих функционирование АСЗИ _____.

Рассмотренная Модель угроз ПДн в ИСПДн позволяет сделать следующие выводы:

1. Полученные характеристики вероятности и опасности угроз безопасности ПДн разработанной Модели угроз следует использовать для обоснования выбора СрЗИ ПДн в ИСПДн.
2. Угрозы утечки информации по техническим каналам следует признать неактуальными для АСЗИ _____.
3. Угрозы НСД, идентификации и аутентификации, угрозы программной среды, незарегистрированных действий нарушителей являются наиболее актуальными для АСЗИ _____. Для нейтрализации актуальных угроз этого вида целесообразно использовать встроенные возможности ОС, СУБД, приложений и сертифицированные СрЗИ от НСД, прошедшие в установленном порядке процедуру оценки соответствия.
4. Угрозы среды виртуализации являются неактуальными, поскольку в АСЗИ _____отсутствуют платформы виртуализации.
5. Угрозы нарушения целостности являются в основном неактуальными для АСЗИ ___. Угрозы воздействия вредоносного ПО нейтрализуются механизмами имеющегося антивирусного решения «Dr.Web Enterprise Security Suite версии 6.0», Anti-X, Cisco 5520, 5510. Оставшиеся актуальные угрозы могут быть нейтрализованы настойками имеющихся встроенных в ОС механизмов защиты, а также применением СрЗИ, прошедших в установленном порядке процедуру оценки соответствия.
6. Угрозы межсетевого взаимодействия, являются в основном неактуальными для АСЗИ _____, т.к. нет прямого подключения к сетям общего пользования.
7. В соответствии с постановлением Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», исходя из анализа угроз безопасности ПДн, а также, учитывая параметры АСЗИ _____, можно рекомендовать установить следующие значение УЗ ПДн для АСЗИ _____- УЗ.4.
8. Наиболее вероятными нарушителями из числа внутренних нарушителей являются пользователи без прав администратора АСЗИ _____(в соответствии с «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённой ФСТЭК России 15.02.2008). Поскольку АСЗИ

_____является локальной и не подключена напрямую к сетям общего пользования, возможности реализация угроз со стороны внешнего нарушителя минимальны.

9.Наиболее вероятными типом нарушителя является тип Н1 (в соответствии с "Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных"(утв. ФСБ России 21.02.2008 № 149/6/6-622)

56. План мероприятий по технической защите конфиденциальной информации и персональных данных в органах исполнительной власти и их подведомственных учреждениях

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 20__ г.

Типовая форма
плана мероприятий по технической защите
конфиденциальной информации и персональных данных

Санкт-Петербург 201__

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
Мероприятия по плану вышестоящего руководства																			
1	Участие в заседании Межведомственного совета по защите информации при полномочном представителе Президента Российской Федерации в Северо-Западном федеральном округе:																		
2	Мероприятия для выполнения решений Межведомственного совета по защите информации при полномочном представителе Президента Российской Федерации в Северо-Западном федеральном округе:																		
	Мероприятие…																		
	Мероприятие…																		
3	Плановая проверка Роскомнадзора по вопросам обеспечения защиты персональных данных																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
4	Совместная проверка Комитета по информатизации и связи по вопросам состояния технической защиты конфиденциальной информации																		
6	Мероприятие…																		
7	Мероприятие…																		
8	Мероприятие…																		
Мероприятия по плану органа исполнительной власти																			
Организационные мероприятия по защите конфиденциальной информации																			
1	Проведение заседания Комиссии по информационной безопасности при руководителе органа исполнительной власти				10														
2	Подготовка и представление руководителю органа исполнительной власти доклада о состоянии дел в органе исполнительной власти по вопросам защиты конфиденциальной информации															30			
3	Разработка или уточнение приказа о назначении работника																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	(структурного подразделения), ответственного за обеспечение безопасности конфиденциальной информации, в том числе ПДн																		
4	Разработка или уточнение приказа о составе комиссии по классификации или переклассификации автоматизированных систем.																		
5	Разработка или уточнение приказа о составе комиссии по классификации информационных систем персональных данных.																		
6	Разработка или уточнение приказа о выделении помещения (помещений) в котором производится обработка конфиденциальной информации, в том числе ПДн																		
7	Разработка или уточнение приказа об утверждении списка лиц, допущенных к работе на автоматизированных системах																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	(АС), также в ИСПДн																		
8	Разработка или уточнение приказа об утверждении списка лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей																		
9	Разработка или доработка приказа о назначении администраторов безопасности СЗ конфиденциальной информации, в том числе ПДн в целом и прикладных администраторов																		
10	Разработка или доработка инструкции по порядку учета и хранению машинных носителей конфиденциальной информации																		
11	Разработка или доработка инструкции, определяющей порядок охраны, внутри объектовый режим и порядок																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	допуска лиц в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональные данные																		
12	Разработка или доработка положения о порядке организации и проведения работ по защите конфиденциальной информации																		
13	Разработка или доработка положения о порядке обработки и обеспечении безопасности персональных данных																		
14	Разработка или доработка инструкции о порядке резервирования и восстановления работоспособности ТС и ПО, баз данных и средств СЗПДн																		
15	Разработка или уточнение руководства пользователя безопасности ИСПДн																		
16	Разработка или уточнение руководства администратора безопасности ИСПДн																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
17	Разработка или уточнение перечня используемых сертифицированных технических средств защиты информации																		
18	Разработка или уточнение перечня сведений конфиденциального характера, подлежащих защите, в том числе ПДн																		
19	Разработка или уточнение перечня АС и ИС, обрабатывающих конфиденциальную информацию и персональные данные																		
20	Разработка акта классификации АС или переклассификации АС.																		
21	Разработка акта классификации ИСПДн или переклассификации ИСПДн.																		
22	Разработка или уточнение модели угроз безопасности информации и модели нарушителя																		
23	Разработка или уточнение частной модели угроз безопасности ПДн																		
24	Разработка или уточнение матрицы																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	доступа персонала к сведениям конфиденциального характера																		
25	Разработка или уточнение схемы расположения объекта информатизации относительно границы КЗ																		
26	Разработка плана внутренних проверок состояния защиты конфиденциальной информации		15																
27	Мероприятие…																		
27	Мероприятие…																		
29	Подготовка и проведение аттестации АС и ЗП																		
30	Подготовка и проведение переаттестации АС и ЗП																		
31	Разработка и подача предложений (расчет-обоснование) по необходимому объему финансирования для проведения работ по защите информации на следующий финансовый год																		
32	Разработка и подача заявки в Комитет по информатизации и																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	связи на закупку технических средств защиты																		
33	Подготовка и проведения конкурсных процедур, заключение государственного контракта на создание подсистемы информационной безопасности																		
34	Мероприятие…																		
35	Ввод в промышленную эксплуатацию подсистемы информационной безопасности																		
36	Мероприятие…																		
Технические мероприятия по защите конфиденциальной информации																			
1	Установка на автоматизированные рабочие места АИС «____» СЗИ Secret №et 5.0																		
2	Настройка Active Directory в соответствии с политикой разграничения прав доступа пользователей к информационным ресурсам																		
3	Мероприятие…																		
			Внутренние проверки и контроль																

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
1	Проведение внутренней проверки состояния защиты конфиденциальной информации			10–12															
2	Мероприятие…																		
3	Мероприятие…																		
Организационные мероприятия по защите персональных данных																			
1	Создание Комиссии по инвентаризации ИСиР и классификации ИСПД .																		
2	Проведение анализа ИСПДн на соответствие с присвоенным ранее классом																		
3	Назначение ответственных сотрудников за проведение мероприятий безопасности ПДн и распределение зон ответственности																		
4	Проведение классификации ИС с оформлением соответствующего акта.																		
5	Урегулирование правовых вопросов обработки (использования) ПДн (уточнение правовых оснований обработки																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
	ПДн, получение согласия субъектов на обработку, пересмотр (при необходимости) договоров с субъектами, установка сроков обработки ПДн и др.)																		
6	Оформление и направление в территориальный орган уполномоченного органа по защите прав субъектов ПДн уведомления об обработке ПДн																		
7	Разработка модели угроз (на основании результатов обследования ИС)																		
8	Определение требований по защите ПДн при их обработке в ИСПДн в соответствии с присвоенным классом																		
9	Разработка ЧТЗ (требований) по созданию (модернизации) подсистемы информационной безопасности																		
10	Проектирование подсистемы информационной безопасности.																		

№ п/п	Наименование мероприятий	Сроки исполнения мероприятий															Ответственный сотрудник	Отметка о выполнении	Примечание
		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15			
		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30			
1	2	3															4	5	6
11	Разработка и реализация комплекса организационных мероприятий защиты ПДн (данный комплекс мероприятий приведен в настоящих рекомендациях и аналогичен вышеприведенному)																		
12	Реализация проекта по созданию (модернизации) подсистемы информационной безопасности																		
13	Аттестация или декларирование ИСПДн на соответствие требованиям по защите ПДн																		
14	Мероприятие…																		
15	Мероприятие…																		

57. План внутренних проверок состояния защиты конфиденциальной информации

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
плана внутренних проверок состояния защиты конфиденциальной информации

Санкт-Петербург 201__

Общие положения

План внутренних проверок состояния защиты конфиденциальной информации, содержит перечень внутренних проверок.

План внутренней проверки содержит следующую информацию:

- Название проверяемого мероприятия.
- Период проведения проверки.
- Исполнитель мероприятия.

Внутренняя проверка проводится в подразделениях органа исполнительной власти, обрабатывающих конфиденциальную информацию.

План внутренней проверки состояния защиты конфиденциальной информации

	Мероприятие	Период проверки	Исполнитель
1	Проверка полноты и качества разработанных распорядительных и нормативно-методических документов, регламентирующих обеспечение безопасности КИ	15-17.03.2014	Рабочая группа
2	Контроль выполнения требований по режиму доступа в здание органа исполнительной власти, защищаемые помещения и на автоматизированные рабочие места, обрабатывающие КИ	18-19 03.2014	Рабочая группа
3	Проверка порядка использования технических средств защиты конфиденциальной информации	с 20 по 21 03.2014	Рабочая группа
4	Проверка выполнения требований СТР-К по защите конфиденциальной информации	с 22 по 23 03.2014	Рабочая группа
5	Подведение итогов	с 24 по 25 03.2014	Рабочая группа
6	Составление акта проверки	с 25 по 26 03.2014	Рабочая группа
7	Доклад руководителю органа исполнительной власти по результатам проверки	27.03.2014	Руководитель рабочей группы

ПРИЛОЖЕНИЕ №
к приказу от «___»_____ 201_ г.
№____

58. Схема расположения объекта информатизации относительно границы КЗ, размещения АС и ЗП относительно контролируемой зоны, топологической схемы АС, схем коммуникаций, электропитания и заземления объекта

_____
(_____)

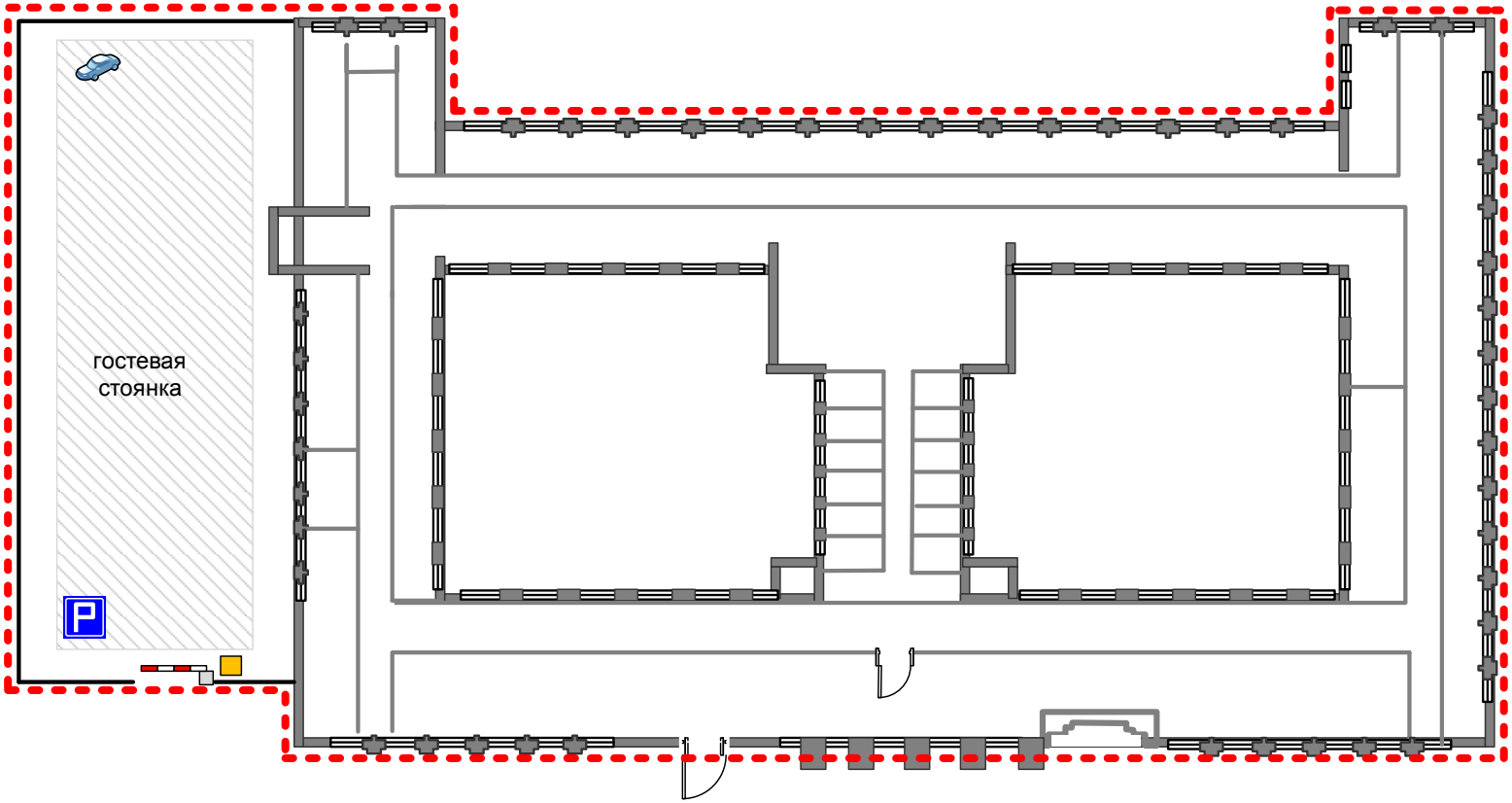
УТВЕРЖДАЮ

_____
«__» _____ 201__ г.

Типовая форма
схем расположения объекта информатизации относительно границы КЗ, размещения АС и ЗП относительно контролируемой зоны, топологической схемы АС, схем коммуникаций, электропитания и заземления объекта

Санкт-Петербург 201__

СХЕМА
контролируемой зоны здания
_____ по адресу _____



Условные обозначения:

- граница контролируемой зоны
- забор
- въезд с автоматическим шлагбаумом
- центральный вход

СХЕМА
размещения АС и ЗП относительно контролируемой зоны,
схем коммуникаций и электропитания объекта

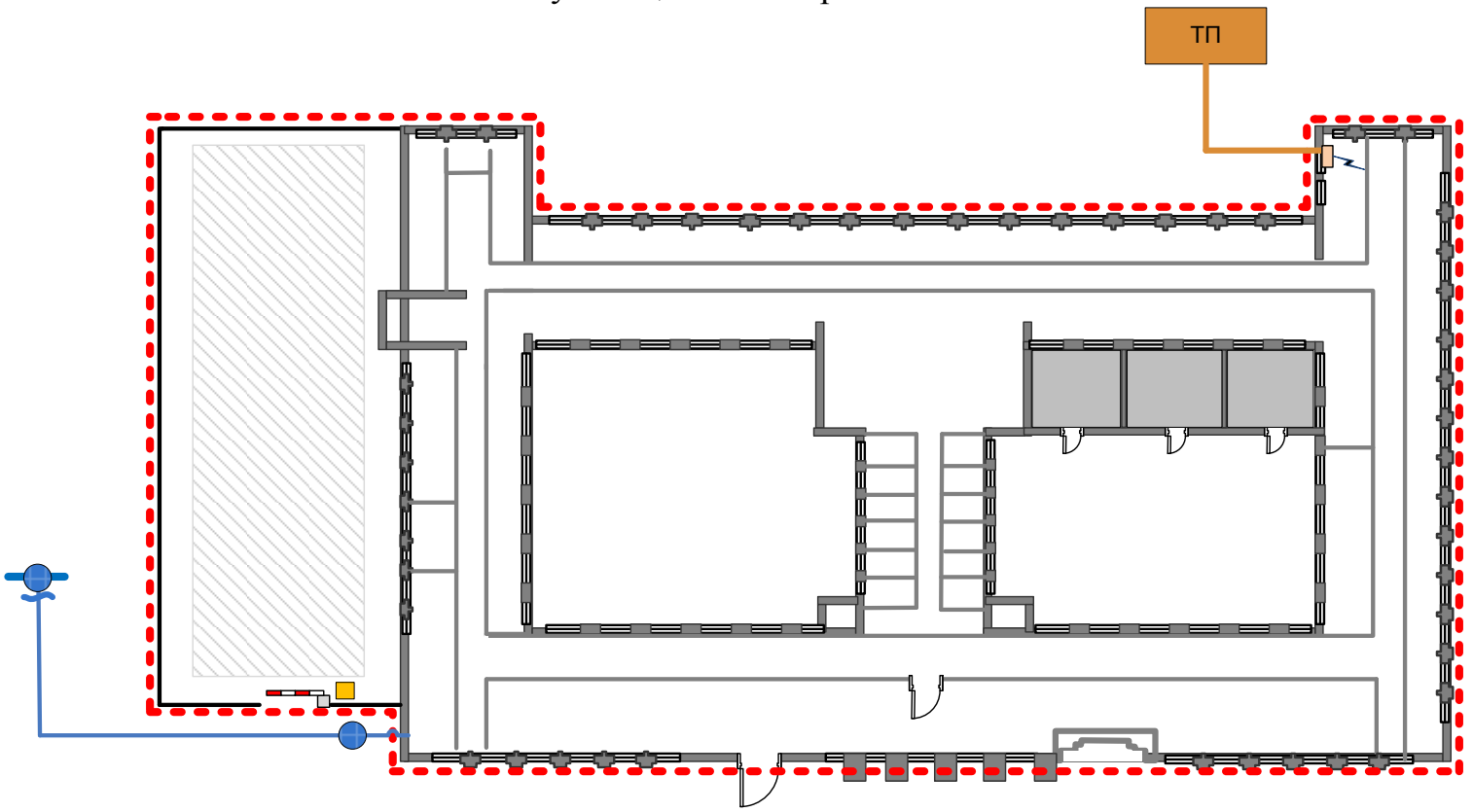
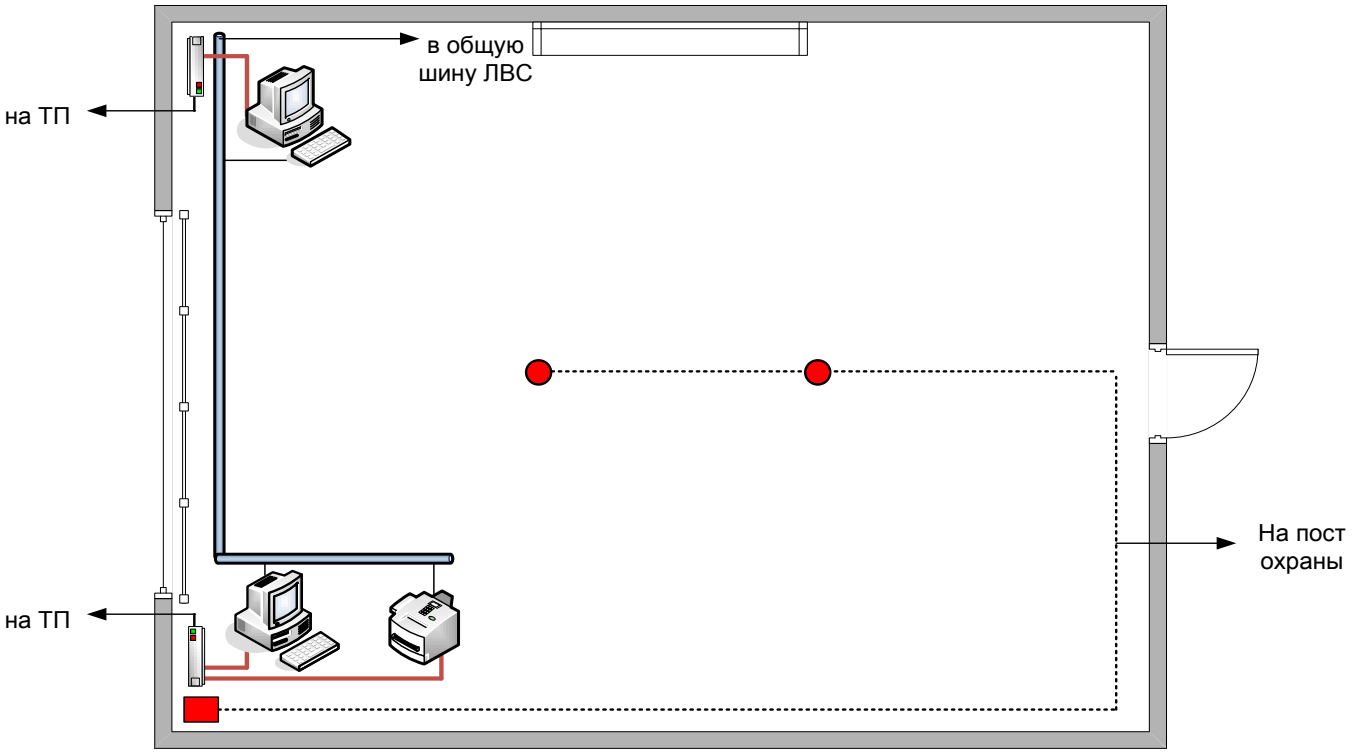


СХЕМА
размещения автоматизированных рабочих мест
в помещении № _____



Условные обозначения:

- АРМ
- принтер
- кондиционер
- пожарный извещатель ИП-122
- охранный извещатель SWAN PGP
- батарея системы отопления
- система электропитания
- соната рк-1

СХЕМА
размещения технических средств в защищаемом помещении
№ _____

Условные обозначения:

C
F
- генератор Соната АВ 3М

- батарея системы отопления

- извещатель охранной сигнализации

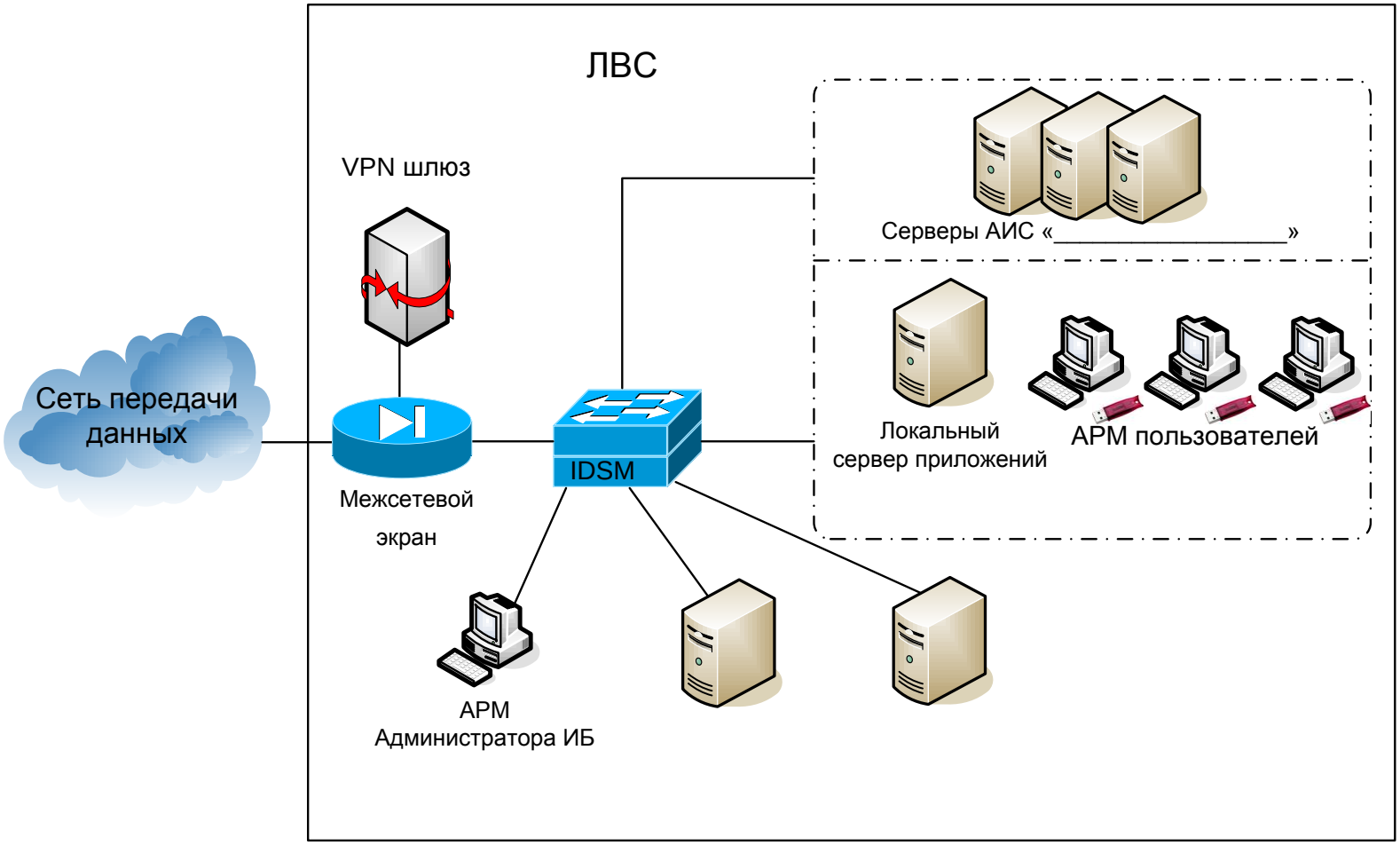
- виброакустический излучатель

- акустическая колонка

- телефонный аппарат

- СЗИ МП-1А

СХЕМА
топологической структуры АС _____



59. Заключение о готовности средств защиты информации к использованию и возможности их эксплуатации в информационной системе персональных данных

УТВЕРЖДАЮ

_____

(руководитель)

_____

(подпись)

«__» _____ 201__г.

ЗАКЛЮЧЕНИЕ

о готовности средств защиты информации к использованию и возможности их эксплуатации в информационной системе персональных данных

В соответствии с Приказом №_____ от «____»_____201__ г. комиссией в составе:

Председатель комиссии:*(ФИО, должность)*_____

Члены комиссии:*(ФИО, должность)*_____

_____

_____

_____

проведена проверка готовности и возможности ввода в эксплуатацию средств защиты информации:

- межсетевой экран WatchGuard XTM 2 series;
- межсетевой экран и VPN шлюз «ЗАСТАВА-Офис»;
- средство антивирусной защиты Kaspersky 6.0;
- встроенные механизмы защиты сертифицированной ОС Windows 7.

на автоматизированных рабочих местах _____*(Название организации)*_____, (далее - Организации) сертифицированных ФСТЭК России.

В ходе проверки установлено:

1. На автоматизированных рабочих местах организации установлено следующее системное и прикладное программное обеспечение:

Производитель	**Используемое ПО**
ЗАО **«Лаборатория Касперского»**	Kaspersky 6.0
Microsoft Corporation	Windows 7

2. Настройка средств защиты информации, обрабатываемой в организации соответствует требованиям эксплуатационной документации на указанные средства.
3. Средства защиты информации, используемые в СЗИ ИСПДн сертифицированы по требованиям ФСТЭК России и могут

использоваться для защиты информации в информационной системе персональных данных 3 класса.

4. Средства защиты информации:
   - межсетевой экран WatchGuard XTM 2 series;
   - межсетевой экран и VPN шлюз «ЗАСТАВА-Офис»;
   - средство антивирусной защиты Kaspersky 6.0;
   - встроенные механизмы защиты сертифицированной ОС Windows 7.

   готовы к эксплуатации в ИСПДн организации

Председатель комиссии _____ _____
(подпись) *(ФИО)*

Члены комиссии: _____ _____
(подпись) *(ФИО)*

_____ _____
(подпись) *(ФИО)*

60. Приказ об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

ПРОЕКТ ПРИКАЗА

**Об утверждении Правил
осуществления внутреннего
контроля соответствия
обработки персональных
данных требованиям
к защите персональных данных**

На основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»", Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления 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», **приказываю:**

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____ (приложение № 1).

2. Контроль по исполнению настоящего постановления возложить _____

Приложение №1

**Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в_____**

1.Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____ (далее – Правила) определяются процедуры, направленные на выявление и предотвращение нарушений

законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2.Настоящие Правила разработаны в соответствии Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», 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 другими нормативными правовыми актами.

3.В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организовывается проведение периодических проверок условий обработки персональных данных.

5.Проверки осуществляются ответственными за организацию обработки персональных данных в _____ либо комиссией, образуемой распоряжением _____.

6.Проверки соответствия обработки персональных данных установленным _____ ежегодного требованиям проводятся на основании утвержденного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

7.При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий целостности персональных данных.

8.Ответственный за организацию обработки персональных данных (комиссия) имеет право:

- запрашивать у сотрудников информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить _____ предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить _____ предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, _____ докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

11. _____ контролирует своевременность и правильность проведения проверки.

Акт осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в

_____

название ИСПДн

(примерная форма)

1.1 Структура ИСПДн

Таблица 1 – Параметры ИСПДн

Заданные характеристики безопасности персональных данных	Типовая информационная система / специальная информационная система
Структура информационной системы	Автоматизированное рабочее место/ Локальная информационная система / Распределенная информационная система
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется / не имеется
Режим обработки персональных данных	Однопользовательская / многопользовательская система
Режим разграничения прав доступа пользователей	Система с разграничение доступа / без разграничения доступа
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах Российской Федерации / технические средства частично или целиком находятся за пределами Российской Федерации
Дополнительная информация	К персональным данным предъявляется требование целостности и (или) доступности

1.1 Состав и структура персональных данных

В ИСПДн обрабатываются следующие персональные данные:

20) персональные данные субъектов ПДн:

- ФИО;
- Дата рождения;

- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;
- Паспортные данные;

21) персональные данные сотрудников:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Адрес проживания (реальный);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся к **категории персональных данных**.

Объем обрабатываемых персональных данных, **не превышает _____ записей** субъектов персональных данных, не являющихся сотрудниками оператора.

В соответствии с Постановлением Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных информационной системе персональных данных «Название ИСПДн» установить уровень защищенности 4.

Так же в ИСПДн существуют следующие объекты защиты:

22) Технологическая информация:

- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию об информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

23) Программно-технические средства обработки:

- общесистемное и специальное программное обеспечение, участвующее в обработке ПДн (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

24) Средства защиты ПДн:

- средства управления и разграничения доступа пользователей;

- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

25) Каналы информационного обмена и телекоммуникации.
26) Объекты и помещения, в которых размещены компоненты ИСПДн.

1.2 Конфигурация ИСПДн

На рисунке 1 представлена конфигурация элементов ИСПДн.

На рисунке 2 представлено территориальное расположение ИСПДн относительно контролируемой зоны.

1.3 Структура обработки ПДн

В ИСПДн _____ обработка персональных данных происходит следующим образом:
27) _____
28) _____
29) _____

1.4 Режим обработки ПДн

В ИСПДн _____ обработка персональных данных осуществляется в однопользовательском/многопользовательском режиме с разграничением/без разграничения прав доступа.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2 и иллюстрирован на примере таблицы 3.

Таблица 2 – Матрица доступа

Группа	Уровень доступа к ПДн	Разрешенные действия	Сотрудники отдела
Администраторы ИСПДн	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Отдел информационных технологий
Администратор безопасности	Обладает правами Администратора ИСПДн. Обладает полной информацией об ИСПДн. Имеет доступ к средствам защиты информации и	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Петров П.П.

	протоколирования и к части ключевых элементов ИСПДн. Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).		
Операторы ИСПДн с правами записи	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем ПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение	Отдел регистратуры
Операторы ИСПДн с правами чтения	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к подмножеству ПДн.	- использование	Сотрудники call-центра

В ИСПДн осуществляют работу следующие сотрудники:

Таблица 3 – Перечень сотрудников

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИСПДн	Иванов И.И.	
	Администратор ИСПДн	Петров П.П.	
	Оператор	Сидорова А.А.	

1.5 Угрозы безопасности ПДн

При обработке персональных данных в ИСПДн можно выделить следующие угрозы:

30) Угрозы от утечки по техническим каналам.

а) Угрозы утечки акустической информации.

б) Угрозы утечки видовой информации.

в) Угрозы утечки информации по каналам ПЭМИН.

31) Угрозы несанкционированного доступа к информации.

а) Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

1) Кража ПЭВМ;

2) Кража носителей информации;

3) Кража ключей и атрибутов доступа;

4) Кражи, модификации, уничтожения информации;

5) Вывод из строя узлов ПЭВМ, каналов связи;

6) Несанкционированное отключение средств защиты.

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

1) Действия вредоносных программ (вирусов);

2) Недекларированные возможности системного ПО и ПО для обработки персональных данных;

3) Установка ПО не связанного с исполнением служебных обязанностей.

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

1) Утрата ключей и атрибутов доступа;

2) Непреднамеренная модификация (уничтожение) информации сотрудниками;

3) Непреднамеренное отключение средств защиты;

4) Выход из строя аппаратно-программных средств;

5) Сбой системы электроснабжения;

6) Стихийное бедствие.

г) Угрозы преднамеренных действий внутренних нарушителей.

1) Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке;

2) Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

д) Угрозы несанкционированного доступа по каналам связи.

1) Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:

- Перехват за переделами с контролируемой зоны;
- Перехват в пределах контролируемой зоны внешними нарушителями;
- Перехват в пределах контролируемой зоны внутренними нарушителями.

2) 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.

3) Угрозы выявления паролей по сети.

4) Угрозы навязывание ложного маршрута сети.

5) Угрозы подмены доверенного объекта в сети.

6) Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях.

7) Угрозы типа «Отказ в обслуживании».

8) Угрозы удаленного запуска приложений.

9) Угрозы внедрения по сети вредоносных программ.

1.6 Существующие меры защиты

Существующие в ИСПДн технические меры защиты представлены в таблице ниже.

Таблица 4 – Меры защиты

Элемент ИСПДн	Программное средство обработки ПДн	Установленные средства защиты
АРМ пользователя	ОС Windows XP Браузер	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией. Антивирус *НАЗВАНИЕ* - регистрацию и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружений вторжений.
АРМ администратора	ОС Windows XP Клиент	Средства ОС: - управление и разграничение доступа пользователей;

	приложения	- регистрацию и учет действий с информацией. Антивирус *НАЗВАНИЕ* - регистрацию и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружений вторжений.
Сервер приложений	OS Windows Server 2007	Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечивать целостность данных. Антивирус *НАЗВАНИЕ* - регистрацию и учет действий с информацией; - обеспечивать целостность данных; - производить обнаружений вторжений.
СУБД	БД ORACLE	Средства БД Средства ОС: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечивать целостность данных. - производить обнаружений вторжений.
Граница ЛВС		Межсетевой экран: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечивать целостность данных. - производить обнаружений вторжений.

Каналы передачи		СКЗИ *НАЗВАНИЕ* Средства СКЗИ: - управление и разграничение доступа пользователей; - регистрацию и учет действий с информацией; - обеспечивать целостность данных.

В ИСПДн введены следующие организационные меры защиты:

- В Учреждении осуществляется контроль доступа в контролируемую зону, установлена охранная сигнализация, двери закрываются на замок, установлены решетки на первых и последних этажах здания
- Ведется учет носителей информации.
- Носители информации хранятся в сейфе.
- В Учреждении существует отдел/ответственный сотрудник за обеспечение безопасности ПДн.
- В учреждение проводятся периодические режима безопасности ПДн.
- Введена парольная политика, устанавливающая сложность ключей и атрибутов доступа (паролей), а также их периодическую смену.
- Пользователи осведомлены и проинструктированы о порядке работы и защиты персональных данных.
- Осуществляется резервное копирование защищаемой информации.
- В помещениях, где расположены элементы ИСПДн, установлена пожарная сигнализация.

1.7 Необходимые меры защиты

На основании анализа актуальности выявленных угроз безопасности, для достижения требуемого уровня защиты рекомендуется осуществить следующие мероприятия:

1._____
2._____
3._____

(Типовая форма)

61. Журнал
учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля

_____

(дата начала ведения Журнала)

_____

_____

_____

(наименование юридического лица/фамилия, имя, отчество (в случае, если имеется) индивидуального предпринимателя)

_____

_____

_____

(адрес (место нахождения) постоянно действующего исполнительного органа юридического лица/место жительства (место осуществления деятельности (если не совпадает с местом жительства) индивидуального предпринимателя)

_____

_____

(государственный регистрационный номер записи о государственной регистрации юридического лица/индивидуального предпринимателя, идентификационный номер налогоплательщика (для индивидуального предпринимателя); номер реестровой записи и дата включения сведений в реестр субъектов малого или среднего предпринимательства (для субъектов малого и среднего предпринимательства))

Ответственное лицо: _____

_____

(фамилия, имя, отчество (в случае, если имеется), должность лица (лиц), ответственного
за ведение журнала учета проверок)

_____

_____

(фамилия, имя, отчество (в случае, если имеется) руководителя юридического лица, индивидуального предпринимателя)

Подпись: _____

М.П.

Сведения о проводимых проверках

1	Дата начала и окончания проверки	

2	Общее время проведения проверки (в отношении субъектов малого предпринимательства и микропредприятий указывается 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): в отношении плановой проверки: – со ссылкой на ежегодный план проведения проверок; в отношении внеплановой выездной проверки: – с указанием на дату и номер решения прокурора о согласовании проведения проверки (в случае, если такое согласование необходимо)	
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 нарушенное требование, допустившее его лицо)	
9	Дата, номер и содержание выданного предписания об устранении выявленных нарушений	
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	

62. Положение о порядке обработки и обеспечении безопасности персональных данных

_____

(_____)

УТВЕРЖДАЮ

_____

«__» _____ 201__ г.

Типовая форма
положения о порядке обработки и обеспечении безопасности персональных данных

Санкт-Петербург 201__

1. Общие положения

Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №152–ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и устанавливает единый порядок обработки персональных данных в _____Санкт-Петербурга и их подведомственных учреждениях.

1.1. В целях настоящего Положения используются следующие термины и понятия:

- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 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;
- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Основные условия проведения обработки персональных данных

2.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно приложению №1 к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;
- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по городу Санкт-Петербургу, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;
- после принятия необходимых мер по защите персональных данных.

2.2. В органе исполнительной власти и подведомственных им учреждениях приказом руководителя назначается сотрудник, ответственный за организацию обработки персональных данных и определяется перечень лиц, допущенных к обработке персональных данных.

2.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные, по форме согласно приложению №2 к настоящему Положению.

2.4. Запрещается:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод персональных данных под диктовку.

3. Порядок определения защищаемой информации

В органе исполнительной власти на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации от 6.03.1997 № 188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - конфиденциальной информации) и перечень информационных систем персональных данных.

3.1. На стадии проектирования каждой ИСПДн определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных

4.Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

4.1 Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2 Оператором осуществляется определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) в соответствии с требованиями постановления Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" в зависимости от типа и объема обрабатываемых персональных данных, а также типа угроз.

4.3 Мероприятия безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с требованиями постановления Правительства РФ от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

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

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПДн, инструкции пользователя, администратора по организации антивирусной защиты, и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других

программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных;

5 Порядок обработки персональных данных без использования средств автоматизации

5.1 Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) в соответствии с постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

5.2 При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.3 При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

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

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

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

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

а) 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;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

в) 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;

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

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

5.6 При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

5.7 Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению №3 к настоящему Положению.

К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.

5.8 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 раздельной обработки персональных данных, в частности:

а) 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;

б) 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.

5.9 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.

5.10 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 (удаление, вымарывание).

6. Ответственность должностных лиц

Гражданские государственные служащие (работники), допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

***Лист ознакомления работников**
с положением о порядке обработки и обеспечении безопасности персональных данных
(утв. Приказом от _____№),

№ п/п	Ф.И.О. работника	Дата ознакомления	Подпись
1	Иванов Иван Иванович	10.10.201__	Иванов
2			
3			
4			
5			
6			
7			

подписывается до подписания трудового договора

63. Типовая форма журнала учета обращений и запросов субъектов персональных данных (или их представителей) по вопросам обработки персональных данных

Журнал учета обращений и запросов граждан по вопросам обработки персональных данных

_____

(наименование организации)

Журнал начат “ _____ ’ _____ 201___ г.

_____

(должность)

_____ / /

(Ф.И.О. должностного лица)

Журнал завершен “ _____ ” _____ 201 _

_____

(должность)

_____ / /

(Ф.И.О. должностного лица)

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предостав-лении информации или отказе в ее предоставлении	Дата передачи/отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение
к Положению о порядке обработки
персональных данных в _____

64. ОБЯЗАТЕЛЬСТВО
о неразглашении информации, содержащей персональные данные

Я,_____
(Ф.И.О.)
исполняющий (ая) должностные обязанности по замещаемой должности

_____

_____
(должность, наименование структурного подразделения)

предупрежден (а) о том, что на период исполнения должностных обязанностей в соответствии с должностным регламентом мне будет предоставлен допуск к информации, содержащей персональные данные. Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному Руководителю.

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

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

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

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

_____ ___
(фамилия, инициалы) (подпись)

«_____»_____ ____г.

65. ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ РЕЗЕРВНОГО КОПИРОВАНИЯ
(ПРОЕКТ)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция устанавливает основные требования к организации резервного копирования (восстановления) программ и данных, хранящихся в базах данных на серверах территориального органа _____, а также к резервированию аппаратных средств.

1.2. Настоящая Инструкция разработана с целью:

- определения категории информации, подлежащей обязательному резервному копированию;
- определения процедуры резервирования данных для последующего восстановления работоспособности информационных систем при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы и определения ответственности должностных лиц, связанной с резервным копированием и восстановлением информации.

1.3. Под резервным копированием информации понимается создание избыточных копий защищаемой информации в электронном виде для быстрого восстановления работоспособности информационных систем персональных данных (ИСПДн) в случае возникновения аварийной ситуации, повлекшей за собой повреждение или утрату данных.

1.4. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги подразделений) на файловых серверах;
- информация, обрабатываемая пользователями в ИСПДн, а также информация, необходимая для восстановления работоспособности ИСПДн, в т.ч. систем управления базами данных (СУБД) общего пользования и справочно-информационные системы общего использования;
- рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн, СУБД, серверов и рабочих станций;
- информация, необходимая для восстановления серверов и систем управления базами данных ИСПДн, локальной вычислительной сети, системы электронного документооборота;

- регистрационная информация системы информационной безопасности ИСПДн;

- другая информация ИСПДн, по мнению пользователей и администратора безопасности, являющаяся критичной для работоспособности ИСПДн.

1.5. Для каждой ИСПДн разрабатывается отдельный Регламент резервного копирования в зависимости от следующих требований:

- состав и объем копируемых данных, необходимая периодичность проведения резервного копирования (по форме, приведенной в Приложении №1);

- максимальный срок хранения резервных копий;

- требований к надежности и защищенности хранения резервных копий;

- требований к резервируемым аппаратным средствам ИСПДн (при необходимости, в случае предъявления высоких требований к обеспечению доступности данных, обрабатываемых в ИСПДн, и значительного ущерба _____ при нарушении заданных характеристик безопасности ПДн).

Допускается составление одного Регламента для нескольких ИСПДн в случае идентичности требований к их резервированию.

1.6. Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений.

1.7. Резервные копии хранятся вне пределов серверного помещения, доступ к резервным копиям ограничен. К носителям информации, содержащим резервные копии, а также к резервируемым программным и аппаратным средствам допускаются только работники _____, указанные в Списке лиц, имеющих доступ к резервируемым программным и аппаратным средствам ИСПДн. Изменение прав доступа к резервируемым техническим средствам, массивам и носителям информации производится на основании Заявки руководителя подразделения. О выявленных попытках несанкционированного доступа к резервируемой информации и аппаратным средствам, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается в ответственному_____ служебной запиской в течение рабочего дня после обнаружения указанного события.

2. ОБЩИЕ ТРЕБОВАНИЯ К РЕЗЕРВНОМУ КОПИРОВАНИЮ

2.1. В Регламенте резервного копирования описываются действия при выполнении следующих мероприятий:

- резервное копирование с указанием конкретных резервируемых данных и аппаратных средств (в случае необходимости);

- контроль резервного копирования:

- хранение резервных копий;

- полное или частичное восстановление данных.

2.2. Архивное копирование резервируемой информации производится при помощи специализированных программно-аппаратных систем резервного копирования, программный и аппаратный состав которых обеспечивает выполнение требования к резервному копированию, приведенные в п. 1.5. Система резервного копирования обеспечивает производительность, достаточную для сохранения информации, указанной в п. 1.4, в установленные сроки и с заданной периодичностью.

2.3. Требования к техническому обеспечению систем резервного копирования:

- это комплекс взаимосвязанных технических средств, обеспечивающих процессы сбора, передачи, обработки и хранения информации, основывающийся на единой технологической платформе;

- имеет возможность расширения (замены) состава технических средств, входящих в комплекс, для улучшения их эксплуатационно-технических характеристик по мере возрастания объемов обрабатываемой информации:

- обеспечивает выполнение функций, перечисленных в п. 2.1;

- средства вычислительной техники отвечают действующим на момент сертификации российским и международным стандартам и рекомендациям.

2.4. Требования к программному обеспечению систем резервного копирования:

- лицензионное системное программное обеспечение и программное обеспечение резервного копирования;

- программное обеспечение резервного копирования обеспечивает простоту процесса инсталляции, конфигурирования и сопровождения.

2.5. Сопровождение системы резервного копирования возлагается на уполномоченных работников подразделения _____, которые обязаны следить за работоспособностью программных и аппаратных средств, осуществляющих архивное копирование, в соответствии с их инструкциями по эксплуатации.

2.6. Предварительный учет магнитных носителей архивных копий производится в отдельном журнале учета магнитных носителей для архивного копирования, который находится в подразделении _____(форма журнала приведена в Приложении №3). Все магнитные носители с архивными копиями маркируются, на них указывается предназначение носителя.

В случае неотделимости носителей архивной информации от системы резервного копирования допускается их не маркировать и учитывать всю систему как одно целое.

2.7. Хранение отдельных магнитных носителей архивных копий организуется в отдельном от используемых данных помещении. Физический доступ к архивным копиям строго ограничен. Контроль за физическим доступом возлагается на администратора безопасности.

2.8. Доступ к носителям архивных копий имеют только уполномоченные работники подразделений _____, которые несут персональную ответственность за сохранность архивных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

2.9. Магнитные носители для архивных копий изымаются для работы только работником, непосредственно осуществляющим резервное копирование, под роспись в журнале учета магнитных носителей архивных копий. Передача магнитных носителей с архивными копиями кому бы то ни было без документального оформления не допускается.

2.10. Уничтожение отделяемых магнитных носителей архивных копий производится установленным порядком в случае прихода их в негодность или замены типа носителя с обязательной записью в журнале их учета.

3. ОТВЕТСТВЕННОСТЬ ЗА СОСТОЯНИЕ РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1. Ответственность за периодичность и полноту резервного копирования, а также состояние системы резервного копирования возлагается на уполномоченных работников подразделения _____, осуществляющих резервное копирование.

3.2. Ответственность за контроль над своевременным осуществлением резервного копирования и соблюдением соответствующего Регламента, а также за выполнением требований по хранению архивных копий и предотвращению несанкционированного доступа к ним возлагается на администратора безопасности.

3.3. В случае обнаружения попыток несанкционированного доступа к носителям архивной информации, а также иных нарушениях ИБ, произошедших в процессе резервного копирования, сообщается в подразделение _____служебной запиской в течение рабочего дня после обнаружения указанного события.

4. ПЕРИОДИЧНОСТЬ РЕЗЕРВНОГО КОПИРОВАНИЯ

4.1. Резервное копирование специализированного программного обеспечения производится при его получении (если это предусмотрено инструкцией по его применению и не противоречит условиям его распространения), а также при его обновлении и получении исправленных и обновленных версий.

4.2. Резервное копирование открытой информации делается не позднее чем через сутки после ее изменения, но не реже одного раза в месяц.

4.3. Информация (ПДн), содержащаяся в постоянно изменяемых базах данных _____, сохраняется в соответствии со следующим графиком:

- ежедневно проводится копирование измененной и дополненной информации. Носители с ежедневной информацией должны храниться в течение недели;

- еженедельно проводится резервное копирование всей базы данных. Носители с еженедельными копиями хранятся в течение месяца;

- ежемесячно производится резервное копирование на специально выделенный носитель длительного хранения, информация на котором хранится постоянно.

4.4. Не реже одного раза в год на носители длительного хранения записывается информация, не относящаяся к постоянно изменяемым базам данных (приказы, распоряжения, открытые издания и т.д.).

5. КОНТРОЛЬ РЕЗУЛЬТАТОВ РЕЗЕРВНОГО КОПИРОВАНИЯ

5.1. Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, указанными в _____, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур. В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает руководителю подразделения _____ до 18 часов текущего рабочего дня.

5.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, осуществляется ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

6. РОТАЦИЯ НОСИТЕЛЕЙ РЕЗЕРВНОЙ КОПИИ

6.1. Система резервного копирования обеспечивает возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивает восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования.

6.2. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования осуществляются ответственным работником подразделения _____. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек. Информация ограниченного доступа с носителей, которые перестают использоваться в системе резервного копирования, уничтожается.

7. ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ ИЗ РЕЗЕРВНЫХ КОПИЙ

7.1. В случае необходимости восстановление данных из резервных копий производится ответственным работником _____.

7.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в систему, воздействия вирусов, программных ошибок, ошибок работников и аппаратных сбоев.

7.3. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

7.4. Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

7.5. Восстановление информации, не относящейся к постоянно изменяемым базам данных, производится с резервных носителей. При этом используется последняя копия информации.

7.6. При частичном нарушении или исчезновении записей баз данных восстановление производится с последней ненарушенной ежедневной копии. Полностью информация восстанавливается с последней еженедельной копии, которая затем дополняется ежедневными частичными резервными копиями.

66. ИНСТРУКЦИЯ
по организации антивирусной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных _____.

1.2. Настоящая Инструкция предназначена для уполномоченных работников территориального органа _____), а также должностного лица, выполняющего функции администратора безопасности информации (далее - администратор безопасности), и пользователей, осуществляющих обработку персональных данных в _____.

1.3. Действие настоящей Инструкции распространяется на структурные подразделения _____.

1.4. В целях обеспечения защиты от деструктивных воздействий компьютерных вредоносных программ производится антивирусный контроль. Обязательному антивирусному контролю подлежит любая информация, поступающая на средства вычислительной техники, в том числе получаемая на внешних носителях из сторонних организаций.

1.5. Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ресурсы информационных систем.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции (сервера);
- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

1.6. Основными задачами системы обеспечения антивирусной защиты являются:

- исключение или существенное затруднение противоправных действий в отношении ИСПДн _____ как носителей защищаемой информации;

- обеспечение условий для устойчивой бесперебойной работы объектов, сетей передачи данных.

1.7. Объектом защиты от воздействия вредоносных программ являются вычислительные структуры и транспортная среда передачи данных ИСПДн _____.

1.8. Обеспечение антивирусной защиты включает:

- регулярные профилактические работы;

- анализ ситуации проявления вредоносных программ и причины их появления;

- уничтожение вредоносных программ на автоматизированных рабочих местах (АРМ) (серверах);

- принятие мер по предотвращению причин появления вредоносных программ.

1.9. Для выполнения требований по антивирусной защите информационных структур ИСПДн _____ используется специализированное программное обеспечение (ПО), обеспечивающее надежную ежедневную автоматическую антивирусную защиту и контроль чистоты информационных массивов данных от вредоносных программ.

1.10. Организация работ по антивирусной защите и ответственность за сопровождение системы антивирусной защиты возлагается на подразделение ИТ.

1.11. Ответственность за контроль установленного порядка антивирусной защиты возлагается на администратора безопасности.

1.12. Периодический контроль состояния антивирусной защиты ИСПДн _____ возлагается на работников подразделения ИТ и администратора безопасности.

1.13. Работники, на которых возлагается ответственность по антивирусной защите, имеют полноправный доступ ко всем АРМ, серверам и другому оборудованию ИСПДн _____.

1.14. Все процессы производятся в автоматическом режиме без участия пользователей и без помех для работы основного и специального ПО.

Процесс плановой полной проверки файловой системы рабочих станций пользователей и серверов ИСПДн _____ проводится во время наименьшей нагрузки оборудования пользовательскими задачами.

1.15. Работник, отвечающий за ежедневное сопровождение антивирусной защиты, обладает необходимыми практическими навыками и теоретическими знаниями по данному вопросу. В основные обязанности по антивирусной защите входит:

- проведение периодического анализа и оценки ситуации антивирусной безопасности для контроля степени защищенности ИСПДн _____ и выработки предложений по изменению и улучшению состояния дел;

- проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;

- осуществление контроля за состоянием средств антивирусной защиты на серверах, рабочих станциях пользователей;

- осуществление контроля за соблюдением работниками требований антивирусной защиты;

- обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также за характером и объемом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;

- передача еженедельного отчета по состоянию антивирусной защиты администратору безопасности.

Администратор безопасности осуществляют следующие действия:

- контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;

- проведение служебных расследований по фактам обнаружения вредоносных программ, повлекших неустойчивую работу и (или) разрушение технологического оборудования, локально-вычислительной сети и информационных массивов _____;

- организацию мероприятий по улучшению антивирусной защиты _____.

1.16. Устанавливаемое (изменяемое) ПО в ИСПДн _____ предварительно проверяется представителем эксплуатирующего подразделения на отсутствие вредоносных программ. Непосредственно после установки (изменения) ПО администратор безопасности выполняет антивирусную проверку на рабочих станциях и серверах ИСПДн _____.

1.17. При возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) администратор безопасности проводит внеочередной антивирусный контроль рабочих станций (серверов) ИСПДн _____.

1.18. Для пользователей рабочих станций ИСПДн _____ запрещена возможность изменения настроек и параметров защиты антивирусных средств на своей рабочей станции, эти действия производит администратор безопасности с помощью средств централизованного управления или вручную.

1.19. По факту появления и проникновения вредоносных программ, повлекших неустойчивую работу и (или) вывод из строя технологического оборудования, локально-вычислительной сети и информационных массивов

_____, проводится служебное расследование Группой реагирования на инциденты информационной безопасности.

1.20. Результаты расследования причин появления и последствий воздействия вредоносных программ на рабочую станцию (сервер) докладываются руководителю Отдела информационной безопасности территориального органа _____ с предложениями по принятию мер, предотвращающих в будущем повторение подобных фактов.

2. ТРЕБОВАНИЯ К АНТИВИРУСНОМУ ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

2.1. Применение только лицензионного антивирусного ПО.

2.2. Возможность обнаружения как можно большего числа известных вредоносных программ, в том числе вирусов, деструктивного кода (макро-вирусы, объектов ActiveX, апплетов языка Java и т.п.), а также максимальная готовность быстрого реагирования на появление новых видов вирусных угроз.

2.3. Исчерпывающий список защищаемых точек (почтовые серверы, файловые серверы, автоматизированные рабочие места и т.д.) возможного проникновения вредоносных программ.

2.4. Обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО.

2.5. Возможность автоматического распространения обновлений антивирусных баз на каждую рабочую станцию (сервер) в ИСПДн _____.

2.6. Соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники.

2.7. Надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде.

2.8. Наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

3. МЕРОПРИЯТИЯ ПО ШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

3.1. В штатном режиме работы системы антивирусной администратор безопасности выполняет:

- установку средств антивирусной защиты на все объекты антивирусной защиты, добавляемые в средства защиты ИСПДн _____, в порядке, описанном в эксплуатационной документации;

- контроль наличия связи между сервером администрирования и защищаемыми объектами;

- необходимые обновления версий средств антивирусной защиты на объектах антивирусной защиты;

- контроль над выполнением задач постоянной защиты;

- настройку автоматических проверок объектов антивирусной защиты не реже одного раза в неделю с целью профилактики;

- контроль актуальности версий антивирусных баз и модулей сканирования ПО сервера администрирования;

- непрерывный мониторинг информационного обмена в средствах защиты ИСПДн _____ с целью выявления проявлений программно-математических воздействий;

- обработку сведений, поступающих от средств антивирусной защиты;

- формирование сводных отчетов о работе средств антивирусной защиты, инцидентах и проч.;

- обработку отчетов о состоянии логических сетей;

- формирование отчетов о работе средств антивирусной защиты логической сети.

3.2. Процесс управления системой антивирусной защиты включает в себя следующие действия администратора безопасности:

- внесение изменений в политику антивирусной защиты;

- управление средствами антивирусной защиты, входящими в состав системы антивирусной защиты;

- мониторинг событий, информация о которых поступает от средств антивирусной защиты с объектов защиты.

3.3. В обязанности администратора безопасности входит проведение мероприятий, обеспечивающих возможность анализа результатов работы средств системы антивирусной защиты:

- разработка отчетов о работе средств антивирусной защиты;

- разработка сводных отчетов о работе средств антивирусной защиты, инцидентах и пр. за месяц.

В отчетах о состоянии системы антивирусной защиты отражается следующая информация:

- количество обнаруженных вредоносных программ за данный период;

- наиболее активные обнаруженные вредоносные программы;

- объекты, где наблюдается наибольшая частота обнаружения вредоносных программ;

- список зараженных объектов.

4. МЕРОПРИЯТИЯ ПО НЕШТАТНОМУ УПРАВЛЕНИЮ СРЕДСТВАМИ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. В случае заражения рабочих станций (серверов) вредоносными программами администратор безопасности выполняет следующие действия:

- централизованно обновляет антивирусные базы сервера администрирования и всех объектов антивирусной защиты;

- проверяет состояние всех объектов антивирусной защиты, наличие зараженных рабочих станций в случае обнаружения пораженных узлов;

- оперативно принимает меры по предотвращению распространения заражения вредоносными программами и при необходимости отключает от сети зараженную рабочую станцию (сервер);

- проводит действия, направленные на устранение вредоносной программы на всех пораженных узлах ИСПДн _____;

- по завершении мероприятий по устранению последствий заражения восстанавливает работоспособность рабочей станции и передает ее ответственному пользователю.

5. УНИЧТОЖЕНИЕ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. Уничтожение вредоносных программ выполняется администратором безопасности.

5.2. Если вредоносная программа поразила какие-либо программы, то уничтожение вредоносной программы выполняется путем уничтожения программы на жестком диске либо на ином магнитном носителе. После уничтожения зараженной программы восстанавливают программу, используя ее резервную копию.

5.3. Если вредоносная программа поразила файлы, то вредоносная программа уничтожается либо путем стирания этих файлов, либо путем использования специального "лечащего" режима антивирусного ПО. Использование "лечащего" режима не дает полной гарантии восстановления файла, поэтому после "лечения" необходима проверка восстановления данного файла. "Лечащие" программы используются лишь в тех случаях, когда отсутствует резервная копия зараженной программы или файла с данными либо восстановление уничтоженного файла с помощью резервной копии очень трудоемко.

5.4. В любом случае после уничтожения вредоносных программ и восстановления зараженных программ и файлов с данными еще раз выполняется проверка наличия вредоносных программ, используя антивирусную программу с установленными последними обновлениями. Перед повторной проверкой производится перезагрузка сервера или рабочей станции через выключение и последующее их включение. Если повторная проверка не выявила вредоносных программ, то можно быть уверенным в их отсутствии.

6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

6.1. Организация мероприятий по централизованной антивирусной защите ИСПДн _____ возлагается на администратора безопасности.

6.2. Администратор безопасности несет ответственность за формирование политики антивирусной защиты, организацию своевременной инсталляции средств антивирусной защиты информации и централизованное обновление баз данных вирусных описаний на комплексе программно-технических средств ИСПДн _____.

6.3. Выполнение технических мероприятий по централизованной антивирусной защите в ИСПДн _____ производится непосредственно администратором безопасности.

6.4. Непосредственную ответственность за соблюдение в повседневной деятельности установленных норм обеспечения антивирусной защиты информации и требований настоящей Инструкции в части защиты ИСПДн _____ несут пользователи, за которыми закреплены соответствующие рабочие станции ИСПДн _____.

67. Уведомление о получении персональных данных не от субъекта персональных данных

Уважаемый Иван Иванович!

Сообщаем Вам, что в связи с _____

(необходимость получения персональных данных)

в соответствии с п. 3 ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" уведомляем субъекта персональных данных _____о том, что оператором

_____

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

получены персональные данные от

_____

_____

(источник получения персональных данных)

с целью:

_____

(цель обработки персональных данных)

предполагаемые пользователи персональных данных:

_____

Оператор обязуется обеспечить права субъекта персональных данных, установленные Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных"

_____

_____ _____ _____

(должность) (подпись) (расшифровка подписи)

“___” _____ 20___ г.

68. Типовая форма уведомления субъекта персональных данных о необходимости дать согласие на предоставление персональных данных третьим лицам

Наименование (Ф.И.О.) оператора

_____

Адрес оператора

_____

Ф.И.О, должность субъекта персональных данных

Уведомление

от 00.00.201___ №00

О необходимости дать согласие на предоставление персональных данных

Уважаемый Иван Иванович!

Сообщаем Вам, что в _____ поступил запрос из _____ от 00.00.201_ исх. №00 о необходимости предоставления Ваших персональных данных для рассмотрения вопроса о выдаче Вам кредита.

В связи с получением данного запроса просим Вас дать согласие на предоставление _____ следующий персональных данных:

1. дата приема на работу в _____;
2. занимаемая должность;
3. размер заработной платы.

Должность оператора

С уведомлением ознакомлен:

00.00.201___

69. Примерная форма ответа работодателя на запрос третьей стороны о передаче персональных данных работника, с требованием соблюдения режима секретности (конфиденциальности) переданных персональных данных работника.

Руководителю

Ф.И.О. руководителя
«____» _____ 201_ г.

Уважаемый Петр Петрович!

В ответ на Ваше письмо от 00.00.201_ исх. №00, сообщаю, что Иванов Иван Иванович работает в _____с 00.00.201__ в должности _____ с ежемесячной заработной платой в размере 00000 (_____ тысяч) рублей.

Сообщаю, что предоставленная Вам информация относится к персональным данным работника и является конфиденциальной.

Предупреждаю Вас о том, что указанные персональные данные могут быть использованы Вами исключительно в целях, для которых они сообщены.

В соответствии со статьей 88 Трудового кодекса Российской Федерации прошу предоставить письменное подтверждение того, что предоставленная Вам информация была использована только в указанных целях.

Должность оператора

70. План мероприятий по организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

№ п/п	Наименование этапа	Содержание работ	Форма завершения работ	Ориентировочные сроки выполнения	Отметка о выполнении
1	Уточнение классификации ИСПДн	Разработка и утверждение приказа о созыве комиссии и классификации ИСПДн	Приказ о создании комиссии по проведению классификации ИСПДн. Акты классификации ИСПДн	1 неделя	
2	Проведение организационных мероприятий	Доработка, разработка новых и утверждение организационно-распорядительных документов	Утвержденные приказы, положения, инструкции, модели угроз, техническое задание на создание СЗИ ИСПДн и т.д.	2 недели	
3	Разработка технического проекта создания СЗПДн	Разработка технического проекта	Технический проект в составе: – ведомость Технического проекта; – пояснительную записку к Техническому проекту;	4 недели	

№ п/п	Наименование этапа	Содержание работ	Форма завершения работ	Ориентировочные сроки выполнения	Отметка о выполнении
			– ведомость покупных изделий; – описание организационной структуры; – схему организационной структуры; – схему структурную комплекса технических средств; – схему функциональной структуры.		
4	Поставка и установка необходимого оборудования.	Поставка необходимого комплекта средств защиты информации, Установка и настройка поставляемого оборудования и программного обеспечения.	– Товарные накладные на поставку аппаратных, аппаратно-программных СЗИ; – Акты передачи неисключительных прав на программные средства защиты информации; – Акты выполненных работ на установку и настройку средств защиты информации.	4 недели	
5	Ввод СЗИ ИСПДн в опытную эксплуатацию.	Разработка программы ввода подсистемы в опытную эксплуатацию. Проведение работ согласно программе ввода	- Программа ввода в опытную эксплуатацию; - Акт сдачи СЗПДн в опытную эксплуатацию.	1 неделя	

№ п/п	Наименование этапа	Содержание работ	Форма завершения работ	Ориентировочные сроки выполнения	Отметка о выполнении
		подсистемы в опытную эксплуатацию.			
6	Приёмо-сдаточные испытания и ввод СЗПДн в промышленную эксплуатацию.	Разработка программы проведения приёмо-сдаточных испытаний. Проведение работ согласно программе приёмо-сдаточных испытаний.	- Программа приёмо-сдаточных испытаний; - Акт ввода СЗПДн в промышленную эксплуатацию; - Протокол проведения приёмо-сдаточных испытаний; - Комплект эксплуатационной (исполнительной) документации на СЗПДн;	1 неделя	

71.Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных

УТВЕРЖДАЮ
_____
_____
«__» _____ 201__ г.

Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных

СОГЛАСОВАНО

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

_____ _____ _____
подпись, дата

ОБЩИЕ ПОЛОЖЕНИЯ

В данном документе представлен список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа к обрабатываемым персональным данным.

Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а так же исходя из характера и режима обработки персональных данных в ИСПДн.

Список лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа для каждой ИСПДн представлен в Приложении №№____.

Приложение 1

ИСПДн _____

УТВЕРЖДАЮ

_____(_____)

"_____" _____201_ г

Перечень групп, участвующих в обработке персональных данных в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
		использование блокировка
		сбор систематизация накопление копирование хранение уточнение использование блокировка уничтожение

Перечень лиц, получивших доступ к персональным данным

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИСПДн	Иванов И.И.	
	Администратор ИСПДн	Петров П.П.	
	Оператор	Сидорова А.А.	

Приложение 2

ИСПДн _____

УТВЕРЖДАЮ

_____(_____)

"_____" _____201_ г

Перечень групп, участвующих в обработке персональных данных в ИСПДн

Группа	Уровень доступа к ПДн	Разрешенные действия
		использование блокировка
		сбор систематизация накопление копирование хранение уточнение использование блокировка уничтожение
		систематизация использование

Перечень лиц, получивших доступ к персональным данным

№	Роль	ФИО сотрудника	Подразделение
	Администратор ИСПДн	Иванов И.И.	
	Администратор ИСПДн	Петров П.П.	
	Оператор	Сидорова А.А.	

72. Журнал
учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств _____

Начат: «____» _____ 201___г.
Окончен:«____» ___ _____ ___ 201___г.

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации, профилактической работы, установка, модификация)	ФИО исполнителей и их подписи	ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)

73. ПОЛОЖЕНИЕ
о разрешительной системе доступа сотрудников к защищаемым информационным ресурсам

Типовое
Положение о разрешительной системе доступа сотрудников к защищаемым информационным ресурсам _____

Сфера действий настоящего Положения

Настоящее Положение устанавливает правила предоставления и разграничения доступа сотрудников к защищаемым информационным ресурсам _____(далее – _____), не содержащим сведений, составляющих государственную тайну. Доступ к информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Положение предназначено для руководителей структурных подразделений, лиц, ответственных за подключение сотрудников к информационным системам Комитета, других лиц, участвующих в процедурах предоставления и прекращения доступа сотрудников к информационным ресурсам.

Положение распространяется на информационные ресурсы, накапливаемые и обрабатываемые в электронном виде на персональных компьютерах сотрудников, в вычислительной сети исполнительных органов государственной власти Санкт-Петербурга, в базах данных информационных систем, а также на отчуждаемых (съемных) электронных носителях информации.

Положение не распространяется на информационные ресурсы на бумажных носителях, кино- и фотоматериалы.

Основные понятия, используемые в Положении

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные ресурсы _____- документы, массивы документов, накапливаемые и обрабатываемые в централизованных системах хранения данных _____.

Общедоступные информационные ресурсы - информационные ресурсы, содержащие информацию, доступ к которой не ограничен. Общедоступными

информационными ресурсами могут пользоваться все сотрудники Комитета по их усмотрению.

Защищаемые информационные ресурсы - объекты файловых систем, содержащие информацию, нарушение целостности, доступности и (или) конфиденциальности которой может нанести ущерб _____ и ИОГВ СПб.

Ответственный за информационный ресурс - лицо, которому предоставлено право разрешать или ограничивать доступ к информационному ресурсу.

Перечень защищаемых информационных ресурсов, с указанием лиц ответственных за них, утверждается _____. Перечень пересматривается при изменении состава ресурсов и условий их обработки, а также при инвентаризации информационных ресурсов.

Предоставление доступа сотрудникам к защищаемым информационным ресурсам, не содержащим персональных данных

Правом предоставления доступа к защищаемым информационным ресурсам, не содержащим персональных данных, обладает ответственный за информационные ресурсы - начальник структурного подразделения, где создается и поддерживается в актуальном состоянии информационный ресурс.

Допуск сотрудника к защищаемым информационным ресурсам или изменение прав доступа осуществляется на основании служебной записки начальника структурного подразделения допускаемого сотрудника на имя _____ с приложением заявки.

Начальник _____ проверяет обоснованность поступившей служебной записки, принимает решение о предоставлении доступа пользователя к информационному ресурсу и накладывает соответствующую резолюцию в служебной записке и заявке. В случае положительного решения, информационный ресурс будет предоставлен сотруднику в объеме указанном в заявке на подключение.

_____ оценивает техническую возможность предоставления доступа к запрашиваемому информационному ресурсу и в случае наличия технической возможности дает указание службе технической поддержки по настройке доступа к информационному ресурсу (при необходимости на создание учетной записи или на внесение изменений в существующую учетную запись).

Сотрудники службы технической поддержки выполняют работы по предоставлению доступа пользователя к защищаемому информационному ресурсу, инструктируют пользователя об особенностях работы с вновь установленными прикладными программами, а также (при необходимости) сообщают пользователю

регистрационное имя и пароль способом, исключающим возможность ознакомления с этими данными посторонних лиц.

Предоставление доступа сотрудникам к защищаемым информационным ресурсам, содержащим персональные данные

Перечень информационных систем, в которых разрешено обрабатывать персональные данные, и список лиц ответственных за каждый информационный ресурс, содержащий персональные данные, утверждаются приказом _____.

Сотрудники, доступ которых к персональным данным, обрабатываемым в информационных системах _____, необходим для выполнения ими служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного _____.

Состав персональных данных, права при обработке персональных данных (чтение, запись, удаление и т.д.), необходимые сотруднику для выполнения служебных обязанностей определяются начальником структурного подразделения, допускаемого сотрудника на имя _____ с приложением заявки.

В служебной записке обосновывается необходимость допуска сотрудника к персональным данным, состав персональных данных, необходимые права по обработке персональных данных, срок, на который предоставляется допуск сотрудника к обработке персональных данных.

_____ проверяет обоснованность поступившей служебной записки, накладывает соответствующую резолюцию и, в случае положительного решения, информационный ресурс будет предоставлен сотруднику в объеме указанном в заявке на подключение.

_____ дает указания сотрудникам службы технической поддержки по настройке доступа сотрудника к обработке персональных данных с соответствующими правами (при необходимости на создание учетной записи или на внесение изменений в существующую учетную запись).

Порядок прекращения доступа сотрудника к защищаемым информационным ресурсам

Прекращение прав доступа сотрудника к защищаемым информационным ресурсам, содержащим персональные данные, а также не содержащим персональные данные, осуществляется на основании служебной записки непосредственного начальника сотрудника _____.

При увольнении сотрудника непосредственный начальник отправляет уведомление по электронной почте начальнику _____ для

прекращения действия прав, уволенного сотрудника, по доступу к информационным ресурсам и удаления учетных записей сотрудника.

В случае нарушения сотрудником требований, установленных правил безопасности персональных данных в _____, права доступа сотрудника к защищаемым информационным ресурсам временно приостанавливаются по решению начальника _____. Восстановление или прекращение прав доступа сотрудника к защищаемым информационным ресурсам в этом случае осуществляется после проведения служебного расследования.

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам в сторону их расширения аналогичен порядку их предоставления.

Порядок изменения прав доступа сотрудника к защищаемым информационным ресурсам в сторону их уменьшения аналогичен порядку их прекращения.

Ответственность

Начальник структурного подразделения несет ответственность за обоснованность запроса на предоставление доступа сотруднику к защищаемым информационным ресурсам и контроль выполнения сотрудником установленных требований безопасности информации.

Начальник _____ несет ответственность за принятие обоснованного решения по предоставлению прав доступа сотруднику к защищаемым информационным ресурсам.

_____, несут ответственность за правильность настроек программных и технических средств разграничения доступа к защищаемым информационным ресурсам в соответствии с правами, необходимыми сотрудникам для выполнения функциональных обязанностей.

Сотрудники, допущенные к защищаемым информационным ресурсам, несут ответственность за нарушение конфиденциальности информации, доступ к которой ограничен федеральным законом или обладателем информации, в соответствии с действующим законодательством.

74. Приказ о внесении изменений в документы, содержащие персональные данные работника (образец заполнения)

ПРИКАЗ

О внесении изменений в документы,
содержащие персональные данные работника

В связи с изменением фамилии _____Иванова И.И. на Петрова И.И.

ПРИКАЗЫВАЮ:

1. Внести соответствующие изменения в документы, содержащие персональные данные работника, а именно изменить в данных документах фамилию и паспортные данные. Ответственный специалист по кадрам_____.

2. Контроль исполнения приказа возложить на начальника отдела кадров _____.

Основание: свидетельство о заключении брака I-РН № 637962, паспорт серии 0503 № 456575 выдан 09.01.2014 ОВД "Пушкин" г. Санкт-Петербург.

Руководитель

С приказом ознакомлены:

начальник отдела кадров

специалист по кадрам

75. Оформление дополнительного соглашения к трудовому договору, в связи с назначением ответственным за организацию обработки персональных данных

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № 1
к трудовому договору от _____№ _____

«____» _____201__

_____, именуемое в дальнейшем «Работодатель», в лице _____, действующего на основании_____, с одной стороны, и _____, именуемая в дальнейшем «Работник», с другой стороны, заключили настоящее соглашение о нижеследующем:

1. Дополнить часть 4 трудового договора от _____. № ___ пунктом ___: «Работник назначается ответственным за организацию обработки персональных данных:

- осуществляет внутренний контроль за соблюдением требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводит до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов».

2. Настоящее дополнительное соглашение составлено в двух экземплярах, по одному для каждой из сторон, и вступает в силу с _____. Оба экземпляра соглашения имеют равную юридическую силу.

3. Реквизиты сторон:

Работодатель:	**Работник:**
Адрес:	Адрес:
ИНН:	Паспорт:

4. Подписи сторон:

Руководитель:	**Работник:**

Работник получил один экземпляр настоящего соглашения:

(подпись, дата)

76. Перечень персональных данных, подлежащих защите в информационных системах персональных данных

Введение

Настоящий Перечень персональных данных, подлежащих защите в информационных системах персональных данных (ИСПДн) (далее – Перечень) *(полное наименование оператора)* (далее – *(краткое наименование оператора)*), разработан

_____.

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться системой защиты персональных данных (СЗПДн).

1.Общие положения

Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты.

Объекты защиты каждой ИСПДн включают:

Обрабатываемая информация:

- персональные данные субъектов ПДн (раздел 2.1.1);
- персональные данные сотрудников (раздел 2.1.2);

Технологическая информация (раздел 2.2).

Программно-технические средства обработки (раздел 2.3).

Средства защиты ПДн (раздел 2.4).

Каналы информационного обмена и телекоммуникации (раздел 2.5).

Объекты и помещения, в которых размещены компоненты ИСПДн (раздел 2.6).

2. ИСПДн _____

2.1. Обрабатываемая информация

2.1.1 Перечень персональных данных субъектов ПДн

Персональные данные субъектов ПДн включают:

- ФИО;
- Дата рождения;
- Контактный телефон;
- Адрес проживания;
- Прочие данные.

2.1.2 Перечень персональных данных сотрудников Учреждения

Персональные данные сотрудников Учреждения включают:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке;
- Адрес проживания (реальный);
- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);

- Информация о трудовой деятельности до приема на работу;
- Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения);
- Телефонный номер (домашний, рабочий, мобильный);
- Семейное положение и состав семьи (муж/жена, дети);
- Информация о знании иностранных языков;
- Форма допуска;
- Оклад;
- Данные о трудовом договоре (номер трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, номер и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- ИНН;
- Данные об аттестации работников;
- Данные о повышении квалификации;
- Данные о наградах, медалях, поощрениях, почетных званиях;
- Информация о приеме на работу, перемещении по должности, увольнении;
- Информация об отпусках;
- Информация о командировках;
- Информация о болезнях;
- Информация о негосударственном пенсионном обеспечении.

2.2 Технологическая информация

Технологическая информация, подлежащая защите, включает:

- управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическую информацию средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информацию на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащих защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информацию о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

- служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

2.3 Программно-технические средства обработки

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (АРМ и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4 Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

2.5 Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6 Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

77. ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. ОБЩИЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных _____(далее - _____), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с "Перечнем защищаемых информационных ресурсов _____".

1.2. Действие настоящей Инструкции распространяется на _____.

1.3. Обработка защищаемой информации в _____ разрешается на основании приказа руководителя _____.

1.4. Ответственность за организацию защиты информации в _____ и выполнение установленных условий ее функционирования возлагается на администратора безопасности информации _____. Ответственность за выполнение мероприятий безопасности информации возлагается на лицо, производящее ее обработку (пользователя _____).

1.5. Допуск пользователей к работе в _____ осуществляется в соответствии с "Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей", утверждаемом руководителем _____.

1.6. К самостоятельной работе на автоматизированных рабочих местах (АРМ), входящих в состав _____, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.7. Помещения, в которых размещены технические средства _____, отвечают режимным требованиям и в нерабочее время сдаются под охрану установленным порядком.

1.8. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении работников _____.

1.9. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица _____. При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

1.10. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. При первичном допуске к работе в _____ пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у должностного лица, выполняющего функции администратора безопасности информации в _____ (далее - администратор безопасности).

2.2. Каждый работник _____, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным _____, несет персональную ответственность <1> за свои действия и обязан:

<1> Работники, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность.

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами _____.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в _____.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только администратору безопасности _____.

2.2.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.6. Немедленно ставить в известность администратора безопасности в следующих случаях:

- при подозрении компрометации личного пароля;

- обнаружения нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам _____;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств _____;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию _____, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных средств защиты;

- обнаружения непредусмотренных отводов кабелей и подключенных устройств;

- обнаружения фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения _____ в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств _____ или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД.

2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.

2.3.8. Производить перемещения технических средств АРМ без согласования с администратором безопасности.

2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего Акта.

2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.

Кому_____
_____
Адрес: _____
От: _____ (Фамилия, имя, отчество)
Адрес: _____
Паспортные данные: Паспорт № _____
Выдан (кем и когда): _____

78. ЗАЯВЛЕНИЕ (ОТЗЫВ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ)

Я, _____(ФИО полностью), проживающий по адресу _____, паспорт № _____ выдан (кем и когда) _____ _____, Настоящим, во исполнение требований Федерального закона «О персональных данных», на основании ст. 9 п. 1 указанного федерального закона отзываю у _____ ранее данное мной согласие на обработку персональных данных. В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной _____ согласия на обработку персональных данных.

Напоминаю, что, в соответствии со ст. 21 п. 5 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ, в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.
Указанное уведомление прошу предоставить в письменной форме.

Дата: __.__._____ .

Подпись: _____ (____)

79. Уведомление об уточнении персональных данных

Уважаемый(ая)_____(Ф.И.О.), в связи с _____сообщаем Вам, что Ваши персональные данные уточнены в соответствии со сведениями: _____.

_____	_____	_____
(должность)	(подпись)	(ФИО)

«___»_____201__г.

80. Уведомление об уничтожении персональных данных

Уважаемый(ая)_____(Ф.И.О.), в связи с _____сообщаем Вам, что Ваши персональные данные уничтожены в соответствии со сведениями: _____.

_____	_____	_____
(должность)	(подпись)	(ФИО)

«___»_____201__г.

81. Информационное письмо о внесении изменений в сведения об операторе в реестре операторов, осуществляющих обработку персональных данных

_____

(полное и сокращенное наименование, фамилия, имя, отчество оператора)

_____

(адрес местонахождения и почтовый адрес оператора)

_____

_____

(регистрационный номер записи в реестре)

Основания изменений: _____

_____

_____

руководствуясь: _____

(правовое основание обработки персональных данных)

_____

с целью: _____

(цель обработки персональных данных)

_____

осуществляет обработку: _____

(категории персональных данных)

_____

принадлежащих: _____

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

(перечень действий с персональными данными, общее описание используемых оператором способов

обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

(описание мер, предусмотренных ст. ст. 18.1 и 19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ

“О персональных данных”, в т.ч. сведения о наличии шифровальных (криптографических)

средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование

юридического лица, ответственных за организацию обработки персональных данных,

и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных

(при наличии трансграничной передачи персональных данных в процессе их обработки, с указанием перечня

иностранных государств, на территорию которых осуществляется трансграничная передача персональных данных)

Сведения об обеспечении безопасности персональных данных

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных

_____

(число, месяц, год)

Срок или условие прекращения обработки персональных данных

_____ _____ _____

(должность) (подпись) (расшифровка подписи)

“___” _____ 201___

82. Инструкция о порядке использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты

1. Общие положения

Инструкция разработана на основании Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 09.09.2000 № Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30.08.2002 № 282, Указа Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 № 351 и других нормативных правовых документов в области защиты информации.

Настоящая инструкция определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании информационно-телекоммуникационных сетей международного информационного обмена и электронной почты, в _____.

Интернет - всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (on-line). Существует ряд протоколов и служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

SMTP - протокол приема - передачи электронной почты.

TELNET - протокол для подключения к удаленным системам, присоединенным к МИС общего пользования в режиме удаленного терминала.

FTP - протокол предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.

DNS - служба сетевых имен используемых для протоколов TELNET, FTP и т.д.

WWW - служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи тестовой,

графической, аудио и видео информации, а также ссылок на другие документы (гипертекстовые ссылки - выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

Помимо перечисленных, существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах

2. Источники угроз информационной безопасности

Подключение средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).

Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;

перенос в АС разрушающего программного обеспечения (внедрение программных закладок, вирусов);

выбор и использование законным пользователем системы неудачных паролей;

несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.

При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

получить информацию об адресной структуре сети;

установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);

получить информацию о пользователях сети;

попытаться подключиться к информационным ресурсам сети;

вызвать отказ в обслуживании легальных пользователей.

Кроме явных, то есть непосредственно направленных на сеть органа, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими сотрудниками органа. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться

для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам, например домашним).

3. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся: системы разграничения прав доступа, межсетевые экраны, системы построения защищенных виртуальных сетей (Virtual Private Network – VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.

3.1. Системы разграничения доступа

Система разграничения доступа запрещает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных, удаленных и терминальных пользователей.

3.2 Межсетевые экраны (МСЭ)

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить: контроль доступа на межсетевом уровне, протоколирование информационных потоков, сокрытие топологии защищаемой сети, реагирование на несанкционированные действия.

Средствами МСЭ могут быть выявлены следующие виды атак: сканирование сетевых портов, атаки на отказ в обслуживании, изучение топологии внутренней сети, использование слабостей протоколов прикладного уровня, распространение вирусов и спама.

К дополнительным службам МСЭ относятся: средства резервного копирования и восстановления, средства обеспечения высокой доступности, сетевая служба имен (split D№S).

Основные показатели защищенности МСЭ: управление доступом, идентификация и аутентификация, регистрация событий и оповещение, контроль целостности, восстановление работоспособности.

Межсетевые экраны делятся на пять классов в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защите от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссиия России, 1997 г.

3.3. Системы построения защищенных виртуальных сетей

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

3.4. Системы обнаружения атак

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

- системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);
- системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).

5.5. Системы анализа защищенности

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак;

4. Организация работы с международными информационными сетями

4.1 Общие требования

АС МИС общего пользования должны быть автономны, не иметь логических и физических каналов (линий) связи с объектами вычислительной техники, на которых ведется обработка информации ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам.

На технических средствах абонентского пункта должно находиться только программное обеспечение, необходимое для его функционирования системы. Владельцам открытых и общедоступных государственных информационных ресурсов необходимо осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов необходимо осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть "Интернет", вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

4.2 Резервное копирование

При размещении информации в сетях общего пользования, необходимо иметь копию такой информации, для ее восстановления в случае разрушения, изменения или блокирования по причине несанкционированного доступа либо неисправности

оборудования. Также необходимо иметь резервную копию системы для восстановления информации в случае ее разрушения.

4.3 Аппаратно - программная защита

Для фильтрации входящих и исходящих сообщений, а также обнаружения атак, рекомендуется использовать межсетевые экраны.

Для работы с открытыми информационными ресурсами в режиме реального времени (on-line) как правило, используют технологию VPN. Для передачи информации конфиденциального характера по открытым каналам связи необходимо использовать сертифицированные средства криптографической защиты.

Программное обеспечение, устанавливаемое на АС МИС общего пользования, должно быть сертифицировано и иметь все последние обновления.

4.4 Организационные меры

Приказом по предприятию, подразделению, учреждению, организации назначаются должностные лица, ответственные за эксплуатацию АС МИС, допущенные к работам в МИС общего пользования (в том числе администратор АС МИС, должностные лица, имеющие право подписи документов для отправки по МИС общего пользования, должностные лица, ответственные за прием/отправку электронных сообщений и т.д.).

Пользователь АС МИС обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты установленной на АС;

Администратор АС МИС обязан:

перед работой пользователей в МИС обеспечить обновление антивирусных баз;

после окончания работы проверить технические средства на наличие/отсутствие вредоносного кода и целостность АС (запрещается использование АС при отключенных или неисправных средствах защиты информации).

Администратор обеспечивает выдачу аутентификаторов (имя пользователя/электронный адрес) и идентификаторов (пароль) пользователя, а также регулярную смену идентификаторов. В случае прекращения полномочий пользователя по работе с МИС (перевод на другую должность, не предусматривающую работу с МИС или увольнение), администратор удаляет учетную запись пользователя из АС МИС.

Администратор обеспечивает ведение журнала приема-передачи информации средствами МИС на бумажных или электронных носителях, который должен содержать следующие обязательные поля: дата работы в сети, ФИО пользователя,

время (продолжительность) работы в сети, подпись (в случае ведения журнала на бумажном носителе) или аутентификатор (при ведении электронного журнала). Данная информация используется для сверки времени работы в сети со счетом предъявленным организацией предоставляющей услуги связи с МИС, и выявления злоупотреблений работы в сети, а также для обнаружения факта компрометации пароля пользователя сети.

Пользователи, работающие на АС МИС общего пользования, обязаны:
знать порядок входа в МИС общего пользования и регистрации в сети;
знать данную инструкцию;
знать правила работы со средствами защиты информации установленными на АС;

передачу документированной информации, производить только по письменному разрешению должностного лица, имеющего право подписи документов для отправки по МИС общего пользования, и после учета в несекретном делопроизводстве;

материальные носители информации с записанной на них входящей документированной информации полученной в процессе работы с информационными ресурсами МИС общего пользования передавать для учета в несекретное делопроизводство;

при пользовании электронной почтой запрещается передача сведений, содержащих конфиденциальную информацию без применения специальных мер защиты (сертифицированных средств криптографической защиты информации);

- запрещается копирование или распространение информации с нарушением авторских прав или условий программных лицензий;
- запрещается распространение противозаконных материалов;

С целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией - спамом не рекомендуется размещать адрес своего электронного ящика на досках (доски объявлений или BBS) объявлений. Для фильтрации данных сообщений необходимо использование белого и черного списка для настройки почтовой службы, а также сообщить о наличии спама администратору сети, провайдеру.

Ежемесячно необходимо проверять фактически отработанное время работы в сети Интернет со счетом, представленным провайдером.

4.5 Антивирусная защита

АС МИС общего пользователя оснащаются, в обязательном порядке, антивирусным программным обеспечением, обновление антивирусной базы которого производится непосредственно перед каждым началом работы. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения. АС МИС общего пользования регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.

При отправке электронных сообщений необходимо заполнять поле тема. Не рекомендуется открывать для чтения почтовые сообщения, адресат которых неизвестен или почтовое отправление носит подозрительный характер (реклама или запрос информации неизвестной фирмы, спам, и т.д.)

Если обнаружено, что почтовое отправление, пришедшее от адресата, заражено вредоносным кодом, администратору необходимо:

срочно принять все меры по предотвращению дальнейшего распространения заражения путем прекращения приема передачи сообщений данной АС МИС;

провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);

отметить данный факт в журнале учета с указанием названия вредоносного программного обеспечения и адресата, от которого оно получено;

поставить в известность руководителя подразделения Правительства области, а также абонента с которыми осуществлялась связь в период заражения для проверки АС антивирусными средствами.

сообщить адресату о наличии у него заражения, для последующего принятия адресатом срочных мер.

Запрещается хранение вредоносного кода, на каких-либо носителях информации.

При обнаружении вредоносного кода необходимо произвести его удаление антивирусными средствами. Удаление зараженных файлов средствами операционной системы может привести к безвозвратному разрушению информации.

5.Работа в сети Интернет

5.1.Доступ к сети Интернет для сотрудников _____предоставляется по служебной записке руководителя соответствующего структурного подразделения Комитета и только на выделенных для работы с Интернет ресурсом персональных компьютерах.

5.2.Пользователи используют поиск информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

5.3.По использованию Интернет ведется статистика, которая хранится на электронных носителях на Узле телематических служб Смольного.

5.4.Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.

5.5.Сотрудникам, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

5.6.Программное обеспечение, используемые для работы в сети Интернет, должно быть согласовано с _____.

5.7.При необходимости переноса рабочих материалов, полученных из сети Интернет, на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции по организации

антивирусной защиты в _____.
5.8.Сотрудники, должны соблюдать эту политику после предоставления им доступа к сети Интернет.

6. Порядок осуществления доступа и обмена данными с внешними информационными ресурсами и по электронной почте

6.1.Установка и настройка программного обеспечения для работы с электронной почтой или ресурсами сети Интернет осуществляется администратором _____. Пользователям запрещается изменение любых параметров, касающихся способов подключения и используемых протоколов.
6.2. При работе с электронной почтой или ресурсами сети Интернет пользователям запрещается:

1) обмен информацией для служебного пользования, а также информацией ограниченного доступа, по электронной почте или с использованием ресурсов сети Интернет;

2) использование ресурсов сети Интернет для развлечения и получения информации, не относящейся к функциональным обязанностям пользователя;

3) предоставление доступа к электронной почте или к ресурсам сети Интернет с использованием данных своей учетной записи другим лицам;

4) публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;

5) подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей;

6) открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением
6.3.Электронная почта предоставляется сотрудникам только для выполнения своих прямых служебных обязанностей по служебной записке руководителя соответствующего структурного подразделения _____. Использование ее в личных целях запрещено. Создание почтового ящика проводится службой технической поддержки по заявке, согласованной с _____.
6.4._____ оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.
6.5.Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.
6.6.Пользователи не должны позволять кому-либо посылать письма от чужого имени.

6.7.В качестве клиентов электронной почты могут использоваться только согласованные с _____ почтовые программы.

7.Ответственность

7.1.Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.
7.2.Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.
7.3.Узел телематических служб Смольного отвечает за бесперебойное функционирование вверенной ему сети, качество предоставляемых пользователям сервисов.
7.4.За нарушение настоящей инструкции пользователь может быть отстранен от работы в сети.

83. ПРИМЕРНЫЙ ПРОЕКТ ДОГОВОРА О ПОРУЧЕНИИ ОБРАБОТКИ ПДН ТРЕТЬИМ ЛИЦАМ

ПРИМЕРНЫЙ ПРОЕКТ СОГЛАШЕНИЯ О КОНФИДЕНЦИАЛЬНОСТИ

Санкт-Петербург, 201___

Договор №_____
на поручение обработки персональных данных
третьим лицам

г. Санкт-Петербург «____» _____201__г.

Администрация _____, именуемое в дальнейшем «**Оператор**», в лице _____,
должность и Ф.И.О
действующего на основании Положения (или доверенности от «__» _____ 201__ года), с одной стороны, и _____ именуемый в
полное наименование организации
дальнейшем «**Уполномоченная сторона**», в лице _____,
должность и Ф.И.О.
действующий на основании Устава с другой стороны, вместе именуемые **Стороны,** с соблюдением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также другими нормативными правовыми актами Российской Федерации и города Санкт-Петербурга в области защиты персональных данных и безопасности информации, заключили настоящий договор (далее - Договор) о нижеследующем:

1. Термины и определения

1.1. Термины и определения, используемые в настоящем Договоре, применяются в том значении, в котором они установлены в законодательстве Российской Федерации о персональных данных.

2. Предмет договора

2.1. Уполномоченная сторона обязуется по заданию Оператора оказывать услуги в виде обработки персональных данных (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение) в соответствии с перечнем, приведенным в п.5 настоящего Договора

2.2. Уполномоченная сторона обязуется принять меры к обеспечению конфиденциальности и безопасности персональных данных представляемых ей Оператором для обработки, и выполнять иные обязательства в соответствии с настоящим Договором.

3. Обязанности, связанные с безопасностью

3.1 Уполномоченная сторона обязана совершать какие-либо действия в отношении персональных данных, которые она обрабатывает от имени Оператора, исключительно в соответствии с указаниями Оператора.

3.2 Уполномоченная сторона обязана принимать надлежащие технические и организационные меры по обеспечению безопасности в соответствии с требованиями законодательства в части защиты персональных данных.

3.3 В случае реорганизации или ликвидации одной из Сторон, Уполномоченная Сторона обязуется незамедлительно уничтожить или, по просьбе Оператора, вернуть все полученные Уполномоченной Стороной персональные данные.

4. Конфиденциальность

4.1. Уполномоченная сторона соглашается с тем, что она обязана обрабатывать персональные данные от имени Оператора, соблюдая конфиденциальность обработки. В частности, если Уполномоченная сторона не получила письменного согласия от Оператора, она не будет раскрывать персональные данные, переданные ей Оператором/для Оператора/от имени Оператора посторонним лицам.

4.2. Если Уполномоченная сторона обязана в силу закона раскрыть персональные данные третьей стороне, она раскрывает эту информацию только этой стороне и только в той степени, насколько этого требует закон.

4.3. Если произойдут события или действия, в результате которых Уполномоченная сторона будет вынуждена разгласить персональные данные, она немедленно оповещает Оператора, субъекта персональных данных в случае получения запроса, уполномоченный орган по защите прав субъектов персональных данных об этих событиях или действиях в письменной форме, и предпринимает все возможные действия, чтобы избежать дальнейшего разглашения персональных данных.

4.4. Уполномоченная сторона не вправе использовать персональные данные, переданные ей Оператором, иначе, чем соответствующие полномочия определены настоящим договором, и с соблюдением требований, установленных федеральным законом к обработке и защите персональных данных.

4.5. Требования сохранять конфиденциальность информации распространяются на весь срок действия Договора и сохраняют свою силу в течение _____ лет с момента прекращения действия Договора.

4.6. Вышеуказанные обязательства конфиденциальности не распространяются на обезличенную и общедоступную информацию.

4.7. Никакие положения настоящего Договора не освобождают Стороны от соблюдения правовых требований, предъявляемых уполномоченным органом по защите прав субъектов персональных данных или судом. Стороны должны, по мере возможности обсуждать друг с другом ответы на запросы на получение информации со стороны уполномоченного органа по защите прав субъектов персональных данных или судов.

5. Перечень персональных данных для обработки

5.1. Перечень персональных данных Оператора, обрабатываемых Уполномоченной стороной, включает в себя:

-
-
-

6. Обязательства Сторон

6.1. Оператор обязуется:

6.1.1. Предоставить Уполномоченной стороне все необходимые для обработки данные, определить цель их обработки и перечень действий над ними.

6.1.2. Предоставить Уполномоченной стороне достоверные персональные данные и сообщать обо всех изменениях в составе персональных данных, переданных для обработки.

6.1.3. Сообщить субъекту персональных данных или его законному представителю о заключении настоящего Договора и передаче Уполномоченной стороне его персональных данных для обработки.

6.1.4. Требовать от Уполномоченной стороны представления надлежащим образом оформленной отчетной документации и материалов, подтверждающих исполнение обязательств по настоящему Договору.

6.1.5. Своевременно принять и оплатить надлежащим образом оказанные услуги в соответствии с настоящим Договором.

6.1.6. Направлять Уполномоченной стороне уведомления об уплате в добровольном порядке сумм неустойки (пеней, штрафов), предусмотренных настоящим Договором за неисполнение (ненадлежащее исполнение) Уполномоченной стороной своих обязательств по настоящему Договору.

6.1.7.. В случае неуплаты Уполномоченной стороной в добровольном порядке предусмотренных настоящим Договором сумм неустойки (пеней, штрафов) взыскивать их в судебном порядке.

6.2. Уполномоченная сторона обязуется:

6.2.1. Обрабатывать полученные персональные данные в соответствии с законодательством и иными нормативными правовыми актами Российской Федерации и города Санкт-Петербурга.

6.2.2. При обработке персональных данных обеспечить 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.

6.2.3. Обеспечивать конфиденциальность обрабатываемых персональных данных, а также применять меры по их защите, в соответствии с категорией и объемом обрабатываемых персональных данных.

6.2.4. Не разглашать полученные от Оператора персональные данные никому, кроме следующих лиц:

- сотрудников и субподрядчиков, принадлежащих к Сторонам Договора, которые напрямую связаны с обработкой Уполномоченной стороне персональных данных;

- субъектов персональных данных или их законных представителей, которые хотят получать информацию, касающуюся своих персональных данных;

- уполномоченным органам по защите прав субъектов персональных данных.

6.2.5. Следить за тем, чтобы ее сотрудники и субподрядчики соблюдали условия конфиденциальности и требования по защите персональных данных.

6.2.6. Проследить, чтобы любая третья сторона, которой были раскрыты персональные данные, соблюдала условия конфиденциальности.

6.2.7. По письменному требованию Оператора подтвердить в письменной форме, что она соблюдает обязательства по настоящему Договору в части обработки и защиты персональных данных.

6.2.8. Требовать своевременного подписания Оператором актов приемки выполненных работ по настоящему Договору.

6.2.9. Требовать своевременной оплаты оказанных услуг.

6.2.10. Исполнять иные обязательства, предусмотренные действующим законодательством и Договором.

7. Ответственность Сторон

7.1. За неисполнение или ненадлежащее исполнение своих обязательств, установленных настоящим Договором, Оператор несет ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. В случае просрочки исполнения Оператором обязательств по оплате Цены Договора Уполномоченная сторона вправе потребовать от Оператора уплату неустойки. Неустойка начисляется за каждый день просрочки исполнения обязательства по оплате *Цены Договора* начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства по оплате Цены Договора. Размер такой неустойки устанавливается в размере одной трехсотой действующей на день уплаты неустойки ставки рефинансирования Центрального банка Российской Федерации от Цены Договора. Оператор освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине Уполномоченной стороны.

7.3 Уполномоченная сторона несет ответственность в соответствии с действующим законодательством РФ:

- за ненадлежащее проведение операций с персональными данными переданными ему Оператором;
- за разглашение персональных данных;
- за действия, которые осуществляют сотрудники и субподрядчики с персональными данными Оператора, повлекшие нарушения законодательства в области обработки и защиты персональных данных и (или) права субъектов персональных данных.

7.4. Уполномоченная сторона не несет ответственность за невыполнение условий настоящего Договора, в случае возникновения обстоятельств непреодолимой силы (форс-мажорных), повлекших за собой неисполнение Уполномоченной стороной обязательств по настоящему Договору.

7.5. В случае просрочки исполнения Уполномоченной стороной обязательств, предусмотренных настоящим Договором, Оператор вправе потребовать уплату неустойки (штрафа, пеней). Неустойка (штраф, пени) начисляется за каждый день просрочки исполнения обязательства, предусмотренных Договором, начиная со дня, следующего после дня истечения, установленного настоящим договором срока исполнения обязательства. Размер такой неустойки (штрафа, пеней) устанавливается Договором в размере не менее одной трехсотой действующей на день уплаты неустойки (штрафа, пеней) ставки рефинансирования Центрального банка Российской Федерации. Уполномоченная сторона освобождается от уплаты неустойки (штрафа, пеней), если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине Оператора.

8. Порядок расчетов

8.1. Оператор оплачивает Уполномоченной стороне услуги, предоставляемые, по настоящему Договору из расчета в месяц _____ руб. (сумма прописью) с учетом НДС.

8.2. Цена Договора составляет _____ руб. (сумма прописью) в т.ч. НДС 18%.

8.3. Оплата по Договору производится ежемесячно, путём перечисления денежных средств в российских рублях на расчётный счёт Уполномоченной стороны в следующем порядке: в течение 5 банковских дней со дня подписания Оператором актов приемки выполненных работ за фактически оказанные в предыдущем месяце услуги на основании счета и счета-фактуры.

8.4. Цена Договора включает в себя все затраты, издержки и иные расходы Уполномоченной стороны, в том числе сопутствующие, связанные с исполнением настоящего Договора.

8.5. Обязательства Оператора по оплате Цены Договора считаются исполненными с момента списания денежных средств в размере, составляющем Цены Договора, с банковского счета Оператора, указанного в статье 13 настоящего Договора.

8.6. В случае изменения расчетного счета Уполномоченной стороны последний обязан в трехдневный срок в письменной форме сообщить об этом Оператору с указанием новых реквизитов расчетного счета.

В противном случае все риски, связанные с перечислением Оператором денежных средств на указанный в настоящем Договоре счет Уполномоченного лица, несет Уполномоченное лицо.

9. Порядок разрешения споров

9.1. Все споры и разногласия, возникшие в связи с исполнением настоящего Договора, его изменением, расторжением или признанием недействительным, Стороны будут стремиться решить путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями.

9.2. В случае невозможности разрешения споров путем переговоров стороны передают их на рассмотрение в Арбитражный суд города Санкт-Петербурга и Ленинградской области.

10. Обстоятельства непреодолимой силы

10.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору в случае, если оно явилось следствием действия обстоятельств непреодолимой силы, а именно чрезвычайных и непредотвратимых при данных условиях обстоятельств: стихийных природных явлений (землетрясений, наводнений, пожара и т.д.), действий объективных внешних факторов (военные действия, акты органов государственной власти и управления и т.п.), а также других чрезвычайных обстоятельств, подтвержденных в установленном законодательством порядке, препятствующих надлежащему исполнению обязательств по настоящему Договору, которые возникли после заключения настоящего Договора, на время действия этих обстоятельств, если эти обстоятельства непосредственно повлияли на исполнение Сторонами своих обязательств, а также которые Стороны были не в состоянии предвидеть и предотвратить.

10.2. Если в результате обстоятельств непреодолимой силы оказываемым услугам нанесен значительный, по мнению одной из Сторон, ущерб, то эта Сторона обязана уведомить об этом другую Сторону в 3-дневный срок, после чего Стороны обязаны обсудить целесообразность дальнейшего оказания услуг и заключить дополнительное соглашение с обязательным указанием новых объемов, сроков и стоимости работ, которое с момента его подписания становится неотъемлемой частью Договора, либо расторгнуть настоящий Договор. Если обстоятельства, указанные в п. 10.1, будут длиться более 2 (двух) календарных месяцев с даты соответствующего уведомления, каждая из Сторон вправе расторгнуть настоящий Договор без требования возмещения убытков, понесенных в связи с наступлением таких обстоятельств.

10.3. Если, по мнению Сторон, оказание услуг может быть продолжено в порядке, действовавшем согласно настоящему Договору до начала действия обстоятельств непреодолимой силы, то срок исполнения обязательств по Договору продлевается соразмерно времени, в течение которого действовали обстоятельства непреодолимой силы и их последствия.

11. Срок действия и порядок изменения, расторжения Договора

11.1. Договора вступает в силу со дня его подписания Сторонами и действует до "__" _____ 201___ г.

11.2. Изменение и дополнение настоящего Договора возможно по соглашению Сторон. Все изменения и дополнения оформляются в письменном виде путем подписания Сторонами дополнительных соглашений к Договору. Дополнительные

соглашения к Договору являются его неотъемлемой частью и вступают в силу с момента их подписания Сторонами.

11.2. Настоящий Договор может быть расторгнут:

- по соглашению Сторон, совершенному в письменной форме за подписью уполномоченных лиц сторон;

- в судебном порядке, при существенном нарушении условий Договора Уполномоченной стороной.

11.2. Сторона, которой направлено предложение о расторжении Договора по соглашению сторон, должна дать письменный ответ по существу в срок не позднее 5 (пяти) календарных дней с даты его получения

12. Прочие условия

12.1. Все уведомления Сторон, связанные с исполнением настоящего Договора, направляются в письменной форме по почте заказным письмом по фактическому адресу Стороны, указанному в статье 13 настоящего Договора, или с использованием факсимильной связи, электронной почты с последующим представлением оригинала. В случае направления уведомлений с использованием почты уведомления считаются полученными Стороной в день фактического получения, подтвержденного отметкой почты. В случае отправления уведомлений посредством факсимильной связи и электронной почты уведомления считаются полученными Стороной в день их отправки.

12.2. Договор составлен в 2 (двух) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

12.3. Во всем, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

13. Адреса, реквизиты и подписи Сторон

Оператор:	Уполномоченная сторона:
Адрес местонахождения:	Адрес местонахождения:
Телефон _____, факс _____	Телефон _____, факс _____
Электронный адрес:	Электронный адрес:
Получатель: л/с _____	Получатель: л/с _____
ОГРН _____	ОГРН _____
ИНН _____	ИНН _____
КПП _____	КПП _____
БИК _____	БИК _____
р/с _____	р/с _____
_____	_____
(должность подписывающего и его Ф.И.О)	(должность подписывающего и его Ф.И.О)
М.П.	М.П.

СОГЛАШЕНИЕ №_____
О КОНФИДЕНЦИАЛЬНОСТИ

г. Санкт-Петербург «____» _____201__г.

Настоящее Соглашение заключено между _____ (далее «Передающая Сторона»), с местом нахождения: _____ в лице _____
(должность, Ф.И.О)
действующего на основании Устава, с одной стороны, и _____ (далее «Получающая Сторона»), с местом нахождения: _____, в лице _____, действующего на основании Устава, далее_____(должность, Ф.И.О) совместно именуемыми «Стороны», а каждый в отдельности «Сторона», договорились о нижеследующем:

1. Для целей настоящего Соглашения термин «Конфиденциальная Информация» означает любую информацию Передающей Стороны, а равно сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе персональные данные субъектов, переданную Получающей Стороне и обозначенную как конфиденциальная.

Информация не является конфиденциальной в случае, если такая информация:

(а) является или становится общеизвестной не в результате нарушения настоящего Соглашения;

(б) находилась в распоряжении Получающей Стороны до ее получения от Передающей Стороны;

(в) получена Получающей Стороной от третьих лиц, в отношении которых у Получающей Стороны не было сведений о неправомерном раскрытии такими лицами данной информации.

Термин «персональные данные» означает любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Конфиденциальная информация не может без предварительного письменного разрешения Передающей Стороны копироваться или иным образом воспроизводиться Получающей Стороной.

2. Передача Передающей Стороной Конфиденциальной Информации Получающей Стороне может осуществляться письменно, устно или путем передачи (предоставления) конфиденциальной информации на магнитных

носителях, мультимедийными средствами или в виде фотографий или другими способами.

Передача Конфиденциальной Информации по настоящему Соглашению оформляется двусторонним актом, подписываемым представителями Сторон, с указанием количества информации, ее носителя, объема, формата и других идентификационных признаков.

В случае передачи Конфиденциальной Информации устно или визуально на переговорах либо совещаниях между Сторонами настоящего Соглашения, ее передача фиксируется путем подписания представителями Сторон соответствующего протокола, с указанием характера Конфиденциальной Информации, ее объема, формата и других идентификационных признаков.

3. Настоящее Соглашение не предоставляет Получающей Стороне никаких прав в отношении Конфиденциальной Информации кроме права использования, необходимого для целей

_____

(указать в каких целях будет использоваться передаваемая информации)

4. В отношении Конфиденциальной Информации Получающая Сторона обязуется:

4.1. Не использовать Конфиденциальную Информацию в каких-либо других целях, кроме как для целей, определенных в пункте 3 Соглашения;

4.2. Принимать меры по охране Конфиденциальной Информации, находящейся на хранении или используемой ею, с такой же степенью, с какой она охраняет собственную конфиденциальную информацию;

4.3. Раскрывать полученную Конфиденциальную Информацию своим сотрудникам, которым требуется получение такой Конфиденциальной Информации только в тех пределах, которые необходимы для целей, определенных в пункте 3 Соглашения, соответственно проинформировав их о конфиденциальном характере информации и ограничениях, связанных с ее использованием, а равно иным способом обеспечив соблюдение конфиденциальности информации;

4.4. Раскрывать полученную Конфиденциальную Информацию третьим лицам только при условии получения предварительного письменного согласия Передающей Стороны на такое раскрытие. При этом Передающая Сторона вправе заключить с одобренными ею третьими лицами отдельные соглашения о конфиденциальности в отношении Конфиденциальной Информации;

4.5. По требованию Передающей Стороны возвратить ей или уничтожить Конфиденциальную Информацию, которая была получена Получающей Стороной в течение срока действия настоящего Соглашения и находится у Получающей Стороны на момент получения соответствующего требования Передающей Стороны.

5. Получающая Сторона имеет право без предварительного письменного согласия Передающей Стороны предоставлять Конфиденциальную Информацию тем лицам, раскрытие информации в пользу которых предусмотрено требованиями

действующего законодательства, включая любое предписание уполномоченного государственного или судебного органа и только в порядке, установленном таким документом. В случае раскрытия Конфиденциальной информации на основании настоящего пункта Получающая сторона ограничит передачу информации запрашиваемым объемом и проинформирует Передающую сторону о факте получения запроса о предоставлении информации в максимально короткие сроки.

6. После окончания действия настоящего Соглашения либо в случае реорганизации или ликвидации Получающей Стороны, Получающая Сторона обязуется незамедлительно уничтожить или, по просьбе Передающей Стороны, вернуть всю полученную Конфиденциальную Информацию и копии, сделанные с нее.

7. Все споры и разногласия, возникающие в связи с исполнением настоящего Соглашения, Стороны будут разрешать путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями. В случае невозможности разрешения споров путем переговоров стороны передают их на рассмотрение в Арбитражный суд города Санкт-Петербурга и Ленинградской области.

8. В случае нарушения Получающей Стороной положений настоящего Соглашения, Получающая Сторона компенсирует все убытки Передающей Стороны, вызванные таким нарушением.

9. В случае признания недействительным или невозможным исполнение любого положения настоящего Соглашения полностью или частично по любой причине остальные положения настоящего Соглашения сохраняют юридическую силу и действие в полном объеме настолько, насколько это позволяет действующее законодательство.

10. Все изменения и дополнения к настоящему Соглашению действительны лишь в случае, если они совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон.

11. Настоящее Соглашение вступает в силу с даты его подписания, действует по «____» _____ 201___ года.

12. Настоящее соглашение может быть расторгнуто по договоренности Сторон либо по инициативе одной из Сторон с предупреждением в письменной форме другой Стороны не менее чем за 30 календарных дней до расторжения настоящего соглашения.

13. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

14. Адреса, реквизиты и подписи Сторон

Передающей Стороны:	Получающая Сторона:
Адрес местонахождения	Адрес местонахождения:
Телефон _____, факс _____	Телефон _____, факс _____
Электронный адрес:	Электронный адрес:
ОГРН _____	ОГРН _____

ИНН _____ ИНН _____
КПП _____ КПП _____

_____ _____
(должность подписывающего и его Ф.И.О) (должность подписывающего и его Ф.И.О)

М.П. М.П.

84. Инструкция о порядке проведения разбирательств по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности персональных данных

1. Внутреннее расследование (разбирательство) – деятельность комиссии, направленная на сбор, анализ и оценку информации и документов в целях установления причин и виновных лиц в совершении деяния, повлекшего неблагоприятные последствия для _____, его подразделений или отдельных работников. Внутреннее расследование проводится при получении сведений о фактах нарушения режима конфиденциальности информации (персональных данных), либо о фактах приготовления или попыток к его нарушению.

2. Для проведения внутреннего расследования распоряжением Руководителя создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав работников _____, Комиссию возглавляет председатель.

3. Председатель организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений _____, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого внутреннего расследования, которое передается на рассмотрение руководителю.

4. При проведении внутреннего расследования устанавливаются:

- наличие самого факта совершения деяния, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства совершения противоправного деяния, а также оценка его последствий;
- конкретный работник, совершивший установленное деяние;
- наличие и степень вины работника в совершении деяния;
- цели и мотивы совершения деяния и их оценки, оценки обстоятельств, смягчающих или отягчающих ответственность, в том числе причин и условий, способствовавших совершению данного деяния.

5. В целях внутреннего расследования все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними

материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

6. Работник, совершивший установленное деяние, выразившееся в несоблюдении условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационной системы или делавший попытки (приготовления) к их нарушению, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений комиссией составляется акт.

Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами расследования, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании расследования работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом председателю комиссии.

8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения внутреннего расследования и ставшие известные им обстоятельства.

9. В процессе проведения внутреннего расследования комиссией выясняются:

- перечень разглашенных документов и сведений, составляющих конфиденциальную информацию (персональные данные);
- причины разглашения информации, содержащей конфиденциальную информацию (персональные данные);
- лица, виновные в разглашении;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с информацией, содержащей конфиденциальную информацию (персональные данные);
- иные обстоятельства, необходимые для определения причин разглашения конфиденциальной информации (персональных данных), степени виновности отдельных лиц, возможности применения к ним мер воздействия.

10. По завершении внутреннего расследования комиссией составляется заключение. В заключении указываются:

- основание для проведения внутреннего расследования;
- состав комиссии и время проведения внутреннего расследования;
- сведения о времени, месте и обстоятельствах совершения противоправного деяния;
- сведения о работнике, совершившем противоправное деяние (должность, фамилия, имя, отчество, год рождения, время работы в учреждении, а также в занимаемой должности);

- мотивы и цели совершения работником противоправного деяния;
- причины и условия совершения деяния;
- данные о характере и размерах причиненного в результате противоправного деяния ущерба, причинную связь деяния и причиненного ущерба;
- предложения о мере ответственности работника, совершившего противоправное деяние.

11. На основании заключения выносится решение о применении мер ответственности к работнику, виновному в несоблюдения условий использования средств защиты информации, которые могут привести к нарушению безопасности информации или другим нарушениям, снижающим уровень защищенности информационной системы, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

12. Все материалы внутренних расследований относятся к конфиденциальной информации и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам внутреннего расследования приобщаются к личному делу работника, в отношении которого оно проводилось.

85. Об электронном журнале безопасности

ПРОЕКТ ПРИКАЗА

О проведении работ по защите персональных данных при их обработке в информационных системах персональных данных
в_____

Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах и в целях исполнения постановления Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" в_____:

ПРИКАЗЫВАЮ:

1) Организовать ведение электронного журнала безопасности.

2) Обеспечить автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудников _____ по доступу к персональным данным, содержащимся в информационной системе.

3) Журнал вести в электронном виде.

4) Контроль за исполнением настоящего приказа возложить на _____.

Руководитель

86.Согласие субъекта на трансграничную передачу персональных данных

Заявление-согласие
субъекта на трансграничную передачу персональных данных на территорию иностранного государства, не обеспечивающего адекватной защиты прав субъектов персональных данных

Я, _____, проживающий (-ая) по адресу _____, паспорт серии _____, номер_____, выдан _____"___ "_____ _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" даю согласие **Наименование организации**, расположенному по адресу индекс _____, г. _____, ул. _____ д. ___, на трансграничную передачу моих персональных данных:

□ ФИО	□ Адрес	□ Образование
□ Дата рождения	□ Паспортные данные	□ Доходы
□ Место рождения	□ Семейное положение	□ Профессия

□ другие: _____
(перечислить дополнительные категории персональных данных)

на территорию иностранного государства, не обеспечивающего адекватной защиты прав субъектов ПДн:
_____
(указать страну)

В целях _____
_____
(указать цели обработки)

Перечень действий, осуществляемых с персональными данными: передача третьей стороне с существенным условием обеспечения конфиденциальности передаваемых сведений;
Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.
Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___"_____ 201__г.

(подпись)

87.Согласие субъекта персональных данных на обработку биометрических персональных данных

Заявление-согласие субъекта на обработку биометрических персональных данных

Я, _____, проживающий (-ая) по адресу _____, паспорт серии _____, номер_____, выдан _____"___"_____ _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" даю согласие **Наименование организации**, расположенному по адресу индекс _____, г. _____, ул. _____ д. ___, на обработку моих биометрических персональных данных, а именно:

_____

_____

_____

_____

(указать состав биометрических персональных данных)

В целях _____

_____

_____

(указать цели обработки)

Перечень действий, осуществляемых с персональными данными: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение;

Наименование организации осуществляет смешанную обработку персональных данных с применением ЭВМ, с передачей по внутренней сети, с передачи по сети Интернет.

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___"_____ 201__г. _____

88.ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ
к трудовому договору от _____

_____(далее-_____), именуемое в дальнейшем "Работодатель", в лице _____, действующего на основании Устава, с одной стороны, и инспектор по кадрам отдела кадров _____ (на дату заключения трудового договора _____), именуемая в дальнейшем "Работник", с другой стороны, совместно именуемые "Стороны", заключили настоящее Соглашение о нижеследующем:

1.1. В связи с изменением персональных данных работника Стороны определили, что трудовой договор заключен с _____в соответствии с паспортом серии 05 03 № 456575, выдан 29.09.2011 ОВД "Колпино" г. Санкт-Петербурга.

1.2. Изменения, вносимые в трудовой договор настоящим Соглашением, вступают в силу с 03.10.2011.

1.3. Все остальные условия трудового договора остаются прежними.

1.4. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному для каждой Стороны.

Работодатель: Работник:

Руководитель

Экземпляр дополнительного соглашения получил(а)

89. Запрос
на предоставление информации, касающейся обработки персональных данных субъекта персональных данных

(наименование или Ф.И.О. оператора)

от _____
(Ф.И.О. субъекта персональных данных)
адрес: _____,
телефон: _____, факс: _____,
электронный адрес: _____

Запрос
на предоставление информации, касающейся обработки персональных данных субъекта персональных данных

В период с "___"_____ _____ г. по "___"_____ _____ г. обрабатывались <1> следующие (вариант дополнительно: специальные <2>; биометрические <3>) персональные данные <4>: _____
_____
(перечень обрабатываемых персональных данных)
с целью _____
(цель обработки персональных данных)
в форме _____
(способы обработки персональных данных)
субъекта персональных данных - _____
_____
(Ф.И.О., паспортные данные, в т.ч. дата выдачи, выдавший орган)
оператором - _____.
(наименование или Ф.И.О. оператора, ИНН, адрес)
Обработка проводилась в рамках _____
_____,
(номер, дата договора либо сведения, иным образом подтверждающие факт обработки персональных данных оператором)
что подтверждается _____.
(сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором)

В связи с _____
(обоснование причин)
и на основании ч. ч. 3 и 7 ст. 14, ст. 18, ч. 1 ст. 20 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" прошу предоставить следующую информацию, касающуюся обработки указанных персональных данных: _____
_____,
(существо запроса с учетом ч. 7 ст. 14 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных")
в следующем порядке _____ в срок до _____.

"__"_____ ____ г.

Субъект персональных данных
_____
(подпись, Ф.И.О.)

<1> Согласно ч. 3 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" 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.

<2> Согласно ч. 1 ст. 10 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" специальные категории персональных данных касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

<3> Согласно ч. 1 ст. 11 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

<4> Согласно ч. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

90. Перечень основных действующих документов

в области защиты информации

(по состоянию на 18.03.2014)

I Перечень основных действующих документов в области технической защиты информации

	Федеральные Законы
1.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями от 28.12.2013 № 398-ФЗ)
2.	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями от 23.07.2013 № 205-ФЗ)
3.	Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (с изменениями и дополнениями от 02.07.2013 №185-ФЗ)
4.	Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (в редакции от 28.12.2013 №396-ФЗ)
5.	Закон Российской Федерации от 28.12.2010 № 390-ФЗ «О безопасности»
6.	Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (редакция, действующая с от 21.12.2013 №377-ФЗ)
7.	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (с изменениями от 11.07.2011 № 200-ФЗ)
8.	Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (с изменениями от 28.12.2013 № 396-ФЗ)
9.	Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (с изменениями и дополнениями от 02.07.2013 № 185-ФЗ)
10.	Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (выписка в части вопросов защиты информации) (с изменениями от 02.12.2013 № 341-ФЗ)
11.	Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (выписка в части вопросов защиты информации) (с изменениями и дополнениями от 25.11.2013 № 317-ФЗ)
12.	Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (глава 14) с изменениями от 28.12.2013 № 421-ФЗ)
	Указы Президента Российской Федерации

1.	Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (с изменениями от 14.01.2011 № 38)
2.	Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 23.09.2005 № 1111)
3.	Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (в ред. Указа Президента РФ от 21.12.2013 № 940)
4.	«Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895
5.	Указ Президента Российской Федерации от 12.05.2009 № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»
6.	Указ Президента Российской Федерации от 25.07.2013 № 648 «О формировании системы распределенных ситуационных центров, работающих по единому регламенту взаимодействия»
7.	Стратегия развития информационного общества в Российской Федерации, утверждённая Президентом Российской Федерации 07.02.2008 № Пр-212.
	Постановления Правительства Российской Федерации
1.	Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденное постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 № 912-51
2.	Постановление Правительства РФ от 15.05.2010 № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, предназначенной для эксплуатации в загранучреждениях Российской Федерации, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ, услуг), и о внесении изменения в Положение о сертификации средств защиты информации»
3.	Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»)

4.	Постановление Правительства РФ от 03.03.2012 № 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации»)
5.	Постановление Правительства РФ от 21.11.2011 № 957 (в ред. Постановления Правительства РФ от 28.10.2013 № 966) «Об организации лицензирования отдельных видов деятельности»
6.	Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
7.	Постановление 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»
8.	Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
9.	Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
10.	Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии» (в ред. Постановления Правительства РФ от 20.07.2012 № 740)
11.	Постановление Правительства Российской Федерации от 14.09.2012 № 928 (ред. от 22.11.2013) «О базовых государственных информационных ресурсах» (вместе с «Требованиями к порядку формирования, актуализации и использования базовых государственных информационных ресурсов», «Правилами формирования, актуализации и использования реестра базовых государственных информационных ресурсов»)
12.	Постановление Правительства Российской Федерации от 16.07.2012 № 722 «Правила предоставления документов по вопросам лицензирования в форме электронных документов»
Руководящие документы, нормативно-методические и методические документы	
1.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»)

2.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи РФ) от 14.11.2011 № 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных»
3.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязи РФ) от 21.12.2011 № 346 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных»
4.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)от 19.08.2011 №706 «Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных»
5.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 15.03.2013 № 274 «Об утверждении перечня иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»
6.	«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21.02.2008 № 149/6/6-622)
7.	Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) «О вопросах отнесения фото- и видео - изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»
8.	Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»
9.	Приказ Федеральной службы охраны Российской Федерации (ФСО РФ) от 07.08.2009 № 487 «Об утверждении Положения о сегменте информационно-телекоммуникационной сети «Интернет» для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации»

Руководящие документы ФСТЭК России (Гостехкомиссии России) **Нормативно-методические и методические документы**	
1.	Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия России. М.,1998 г. В составе: Руководящий документ. Защита от несанкционированного доступа к информации Термины и определения. Гостехкомиссия России, 1992 г. Руководящий документ. Концепция защиты средств вычислительной техники автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России,1992 г. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992 г. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992 г. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах средствах вычислительной техники. Гостехкомиссия России, 1992 г. Руководящий документ. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997 г. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России, 1997 г. Руководящий документ. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Гостехкомиссия России, 1998 г.
2.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992 г.
3.	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 № 114.
4.	Руководящий документ Гостехкомиссии России «Средства защиты информации. Специальные общие технические требования, предъявляемые к сетевым помехоподавляющим фильтрам» Гостехкомиссия России, 1999 г.

5.	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.
6.	Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25.11.1994
7.	«Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», Гостехкомиссия России, 2002 г.
8.	«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», Гостехкомиссия России, 2002 г.
9.	«Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», Гостехкомиссия России, 2002 г.
10.	«Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», Гостехкомиссия России, 2002 г.
11.	Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам в министерствах и ведомствах, в органах государственной власти субъектов Российской Федерации; Типовое положение о подразделении по защите информации от иностранных технических разведок и от ее утечки по техническим каналам на предприятии (в учреждении, организации, утверждено Решением Гостехкомиссии России от 14.03.1995 № 32
12.	Типовые требования к содержанию и порядку разработки руководств по защите информации на объектах, утверждены Решением Гостехкомиссии России от 03.10.1995 № 42
13.	Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом председателя Гостехкомиссии России от 30.08.2002 № 282 Извещение № 1 – 2008 о корректировке СТР-К.
14.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены Заместителем директора ФСТЭК России 15.02.2008
15.	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 14.02.2008
16.	Решение ФСТЭК России, утвержденное первым заместителем директора ФСТЭК России от 05.03.2010
17.	Приказ ФСТЭК России от 18.02.2013 № 21 Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

18.	Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
19.	Методический документ «Меры защиты информации в государственных информационных системах» утвержден ФСТЭК России 11.02.2014
20.	Сборник нормативно-методических документов ФСТЭК России «Базовая модель и методика определения угроз безопасности информации в ключевых системах информационной инфраструктуры» в составе: Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утверждена Заместителем директора ФСТЭК России 18.05.2008; Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры утверждена Заместителем директора ФСТЭК России 18.05.2008
21.	Методические документы. Утверждены ФСТЭК России 14.06.2012 «Профили защиты средств антивирусной защиты»
22.	Методические документы. Утверждены ФСТЭК России 06.03.2012 «Профили защиты систем обнаружения вторжений»
23.	Методические документы. Утверждены ФСТЭК России 03.02.2012 «Профили защиты систем обнаружения вторжений»
24.	Руководящий документ. «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» Гостехкомиссия России, 2003 г.
25.	Руководящий документ «Безопасность информационных технологий. Руководство по регистрации профилей защиты». Гостехкомиссия России, 2003 г.
26.	Руководящий документ. «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты» Гостехкомиссия России, 2003 г.
27.	Руководящий документ. «Руководство по разработке профилей защиты и заданий по безопасности» Гостехкомиссия России, 2003 г.
28.	Информационное сообщение ФСТЭК России от 20.11.2012 № 240/22/4669 Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных
29.	Информационное письмо ФСТЭК России от 01.03.2012 № 240 «Об утверждении требований к системам обнаружения вторжений».
30.	Информационное сообщение ФСТЭК России от 30.07.2012 № 240/24/3095 Об утверждении требований в средствам антивирусной защиты
31.	Информационное сообщение ФСТЭК России от 04.05.2012 № 240/24/1701 О работах в области оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа

32.	Информационное сообщение ФСТЭК России от 15.07.2013 № 240/22/2637 по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
33.	Информационное сообщение ФСТЭК России от 07.04.2014 № 240/24/1208 «О применении сертифицированной по требованиям безопасности информации операционной системы WINDOWS XP в условиях прекращения её поддержки разработчиком»
34.	Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам, (решение Гостехкомиссии России 2002 г.). Извещение № 1 – 2007 о корректировке Сборника временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам.
35.	Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27дсп
36.	Методические рекомендации по технической защите информации, составляющей коммерческую тайну, утверждённые заместителем директора ФСТЭК России 25.12.2006
37.	Пособие по организации технической защиты информации, составляющей коммерческую тайну, утверждённое заместителем директора ФСТЭК России 25.12.2006
38.	Решение Гостехкомиссии России от 21.12.1997 № 61 «О защите информации при вхождении России в международную информационную систему Интернет»
	Государственные стандарты в области защиты информации и смежные с ними (ГОСТы)
1.	ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения».
2.	ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
3.	ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
4.	ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»
5.	ГОСТ 12.1.050-86 «Методы измерения шума на рабочих местах».

6.	ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».
7.	ГОСТ 2.114-95 «Единая система конструкторской документации. Технические условия».
8.	ГОСТ 2.601-2006 «Единая система конструкторской документации. Эксплуатационные документы».
9.	ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
10.	ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создании автоматизированных систем».
11.	ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».
12.	ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».
13.	РД Госстандарта СССР 50-682-89 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Общие положения».
14.	РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».
15.	РД 50-680-88 «Методические указания. Автоматизированные системы. Основные положения».
16.	ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания».
17.	ГОСТ 6.10-84 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствам вычислительной техники. Основные положения».
18.	ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».
19.	ГОСТ Р ИСО /МЭК 9126- 93 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению».
20.	ГОСТ 2.111-68 «Нормоконтроль».
21.	ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».
22.	ГОСТ 13661-92 «Совместимость технических средств электромагнитная. Пассивные помехоподавляющие фильтры и элементы. Методы измерения вносимого затухания».
23.	ГОСТ 29216-91 «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний».

24.	ГОСТ 22505-97 Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний
25.	ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний»
26.	ГОСТ Р 50948-2001. «Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности».
27.	ГОСТ Р 50949-2001 «Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности».
28.	ГОСТ Р 50923-96 «Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения».
29.	ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения»
30.	ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»
	Нормативные правовые акты Санкт-Петербурга
1.	Закон Санкт-Петербурга от 07.07.2009 № 371-70 «О государственных информационных системах Санкт-Петербурга» (с изменениями от 29.11.2013 № 635-111)
2.	Постановление Правительства Санкт-Петербурга от 30.12.2013 № 1095 «О системе закупок товаров, работ, услуг для обеспечения нужд Санкт-Петербурга»
3.	Распоряжение Администрации Санкт-Петербурга от 08.08.2001 № 616-ра «О мерах, обеспечивающих отнесение сведений, содержащихся в государственных информационных ресурсах исполнительных органов государственной власти Санкт-Петербурга, к категории конфиденциальной информации» (в редакции от 06.12.2001 № 1277-ра)
4.	Распоряжение Администрации Санкт-Петербурга от 15.05.2002 № 751-ра «Об организации использования электронной цифровой подписи в электронных документах, хранимых, обрабатываемых и передаваемых в автоматизированных информационных и телекоммуникационных сетях и системах исполнительных органов государственной власти Санкт-Петербурга» (с изменениями от 07.10.2010 № 1359)
5.	Распоряжение Администрации Санкт-Петербурга от 06.12.2002 № 2532-ра «О создании Комиссии по защите информации в исполнительных органах государственной власти Санкт-Петербурга» (с изменениями от 22.06.2009 № 677)
6.	Распоряжение Администрации Санкт-Петербурга от 24.03.2003 № 525-ра «О совершенствовании обеспечения исполнительных органов государственной власти Санкт-Петербурга услугами телематических служб в защищенном варианте»

7.	Распоряжение Администрации Санкт-Петербурга от 04.02.2003 № 220-ра «Об организации контроля за состоянием технической защиты информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга» (с изменениями от 03.08.2011 № 1095)
8.	Приказ Администрации Санкт-Петербурга от 19.02.2003 № 6-пв «О создании Комиссии по контролю за состоянием работ по технической защите информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга»

II Перечень основных действующих документов в области криптографической защиты информации

	Постановления Правительства Российской Федерации
1.	Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)
	Руководящие документы ФСБ России **Нормативно-методические и методические документы**
1.	Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»
2.	Приказ ФСБ России от 27.02.2009 № 75 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»

3.	Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден руководством 8 Центра ФСБ России 08.08.2009 № 149/7/2/6-1173
4.	Приказ ФСБ России от 30.08.2012 № 440 «Об утверждении административного регламента Федеральной службы безопасности Российской Федерации по предоставлению государственной услуги по осуществлению лицензирования деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
5.	Приказ ФСБ России от 13.11.1999 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия»
6.	Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».
7.	Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении требований к средствам электронной подписи и требований к средствам удостоверяющего центра»
8.	Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144
9.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»)
10.	Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» утвержденные Руководителем Роскомнадзора 13.12.2013
11.	Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

	Нормативные правовые акты Санкт-Петербурга
1	Приказ Администрации Санкт-Петербурга от 19.02.2003 № 6-пв «О создании Комиссии по контролю за состоянием работ по технической защите информации ограниченного доступа в исполнительных органах государственной власти Санкт-Петербурга»

III Перечень основных действующих документов в области обеспечения безопасности общедоступной информации

	Федеральные Законы
1.	Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления (с изменениями от 28.12.2013 № 396-ФЗ)
	Постановления Правительства Российской Федерации
1	Постановление Правительства Российской Федерации от 18.05.2009 № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».
	Руководящие документы, нормативно-методические и методические документы
1.	Приказ Министерства экономического развития Российской Федерации от 16.11.2009 № 470 «О требованиях к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти».
2.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»
3.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 27.06.2013 № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования»
4.	Приказ Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»

5.	Приказ Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 3.07.2013 № 155 «Об утверждении Методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры»
Нормативные правовые акты Санкт-Петербурга	
1.	Закон Санкт-Петербурга от 16.07.2010 № 445-112 Об обеспечении доступа к информации о деятельности государственных органов Санкт-Петербурга(с изменениями от 27.12.2013 № 729-132)
2.	Постановление правительства Санкт-Петербурга от 29.06.2011 № 864 О мерах по реализации закона Санкт-Петербурга «Об обеспечении доступа к информации о деятельности государственных органов Санкт-Петербурга» (с изменениями от 04.07.2013 № 461)

IV Перечень основных действующих документов в области обеспечения безопасности ключевых систем информационной инфраструктуры (КСИИ)

Документы Совета безопасности Российской Федерации	
1.	Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
2.	«Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий» (утв. Секретарем Совета Безопасности Российской Федерации 08.11.2005).
Руководящие документы ФСТЭК России **Нормативно-методические и методические документы**	
1.	Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 18.05.2007)
2.	Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утверждены заместителем директора ФСТЭК России 19.11.2007)
3.	Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена заместителем директора ФСТЭК России 18.05.2007)
4.	Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утверждена заместителем директора ФСТЭК России 18.05.2007)
5.	Методические рекомендации по организации контроля состояния обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации (утверждены заместителем директора ФСТЭК России 18.11.2008, №246дсп)
6.	Положение о Реестре ключевых систем информационной инфраструктуры (утверждено приказом ФСТЭК России от 04.03.2009 №74)
7.	Методические рекомендации по формированию аналитического прогноза по комплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период (утверждено ФСТЭК России 23.04.2011)

	Государственные стандарты (ГОСТы)
1.	ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения»
2.	ГОСТ РО 0043-002-2012 «Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Система документов»