ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ

ПРИКАЗ

20 ОКТ 2015 № 1622-п

г. Екатеринбург

Об организационных мерах защиты персональных данных

В целях реализации мероприятий по созданию Регионального фрагмента Единой государственной информационной системы в сфере здравоохранения Свердловской области в части защиты персональных данных, обрабатываемых в медицинских организациях Свердловской области, на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», приказов ФСТЭК от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», 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»

П Р И К А З Ы В А Ю:

1. Утвердить перечень внутренних организационно-распорядительных документов по защите персональных данных в медицинских организациях (Приложение № 1).

2. Руководителям государственных учреждений Свердловской области, подведомственных Министерству здравоохранения Свердловской области в срок до 01.11.2015:

1) назначить приказом ответственное лицо за обработку персональных данных;

2) уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому Федеральному округу о намерении осуществлять обработку персональных данных;

3) опубликовать на официальном сайте медицинской организации документ, определяющий политику в отношении обработки персональных данных;

4) обеспечить разработку внутренних документов по защите персональных данных, обрабатываемых в медицинской организации, в соответствии с перечнем, утвержденным настоящим приказом, при необходимости привлечь Государственное бюджетное учреждение здравоохранения «Медицинский информационно-аналитический центр» (далее - ГБУЗ СО «МИАЦ»);

Отпечатано для Министерства здравоохранения Свердловской области, заказ №1415, тираж 20000

5) направить отчет о проведенных мероприятиях в ГБУЗ СО «МИАЦ» на электронный адрес: ib@miacso.ru.

3. Начальнику ГБУЗ СО «МИАЦ» А.А. Григоряну:

1) разместить на сайте ГБУЗ СО «МИАЦ» в разделе «Информационная безопасность» методические рекомендации по созданию пакета организационно-распорядительных документов и образцы документов в соответствии с перечнем;

2) осуществлять консультативную и методическую помощь медицинским организациям при подготовке внутренних организационно-распорядительных документов по защите персональных данных в медицинских организациях;

3) обеспечить контроль выполнения мер защиты персональных данных в медицинских организациях на регулярной основе.

4. Рекомендовать начальнику Управления здравоохранения Администрации г. Екатеринбурга А.А. Дорнбушу обеспечить проведение следующих организационных мер защиты персональных данных в подведомственных муниципальных учреждениях г. Екатеринбурга:

1) назначить приказом ответственное лицо за обработку персональных данных;

2) уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций по Уральскому Федеральному округу о намерении осуществлять обработку персональных данных;

3) опубликовать на официальном сайте подведомственного муниципального учреждения г. Екатеринбурга документ, определяющий политику в отношении обработки персональных данных;

4) обеспечить разработку внутренних документов по защите персональных данных, обрабатываемых в подведомственном муниципальном учреждении г. Екатеринбурга, в соответствии с перечнем, утвержденным настоящим приказом.

5. Контроль за исполнением настоящего приказа возложить на заместителя Министра здравоохранения Свердловской области С.П. Золотова.

Министр А.Р. Белявский

Приложение № 1
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

Перечень
внутренних организационно-распорядительных документов по защите персональных данных в медицинских организациях

1. Приказ о назначении должностного лица, ответственного за организацию обработки персональных данных в информационных системах (Приложение № 2);
2. Приказ о допуске сотрудников к обработке персональных данных (Приложение № 3);
3. Приказ о порядке допуска лиц в защищаемые помещения (Приложение № 4);
4. Приказ о назначении администратора информационной безопасности (Приложение № 5);
5. Приказ о назначении ответственных за обезличивание персональных данных (Приложение № 6);
6. Приказ об утверждении положения об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации (Приложение № 7);
7. Приказ об утверждении положения об обработке персональных данных (Приложение № 8);
8. Приказ об определении границ контролируемой зоны (Приложение № 9);
9. Приказ об утверждении правил рассмотрения запросов субъектов персональных данных (Приложение № 10);
10. Приказ об утверждении формы согласия пациента на обработку персональных данных (Приложение № 11);
11. Приказ об утверждении формы согласия работника на обработку персональных данных (Приложение № 12);
12. Приказ об обеспечении выполнения требований по использованию и обслуживанию средств криптографической защиты информации (Приложение № 13);
13. Приказ о создании комиссии по классификации информационных систем персональных данных Приложение № 14);
14. Акт определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных (Приложение № 15);
15. Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных (Приложение № 16);

16. Приказ об утверждении правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение № 17);

17. Приказ о порядке обработки персональных данных без использования средств автоматизации (Приложение № 18);

18. Приказ о создании комиссии по уничтожению персональных данных (Приложение № 19).

Образец

Приложение № 2
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от _____ №_____

ПРИКАЗ

О назначении должностного лица, ответственного за организацию обработки персональных данных в информационных системах
(название Медицинской организации)

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в информационных системах персональных данных _____
(название МО)

_____ .
(должность, Ф.И.О сотрудника)

2. Утвердить «Инструкцию ответственного лица за обработку персональных данных в _____ (Приложение № 1).
(название МО)

3. Возложить на _____ следующие обязанности:
(Ф.И.О сотрудника)

- предоставление на утверждение списка лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных _____
(название МО)

необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;

- осуществление внутреннего контроля за соблюдением работниками _____
(название МО)

законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения работников (оператора) положения законодательства Российской Федерации о персональных данных, локальных

актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организация приема и обработка обращений субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____

(Ф. И. О.)

Приложение № 1
к приказу _____
(название МО)

от _____№_____

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в *(название МО)*

I. Общие положения

1. Настоящая должностная инструкция определяет права, ответственность и обязанности ответственного (далее - Ответственный) за организацию обработки персональных данных (далее - ПДн) в _____.
(название МО)

2. Методическое руководство и контроль работы должностных лиц в _____
(название МО)
осуществляет ответственный за организацию обработки персональных данных.

II. Обязанности ответственного за организацию обработки персональных данных

3. Должностное лицо, ответственное за организацию обработки ПДн в _____, обязано:
(название МО)

- знать и выполнять требования действующего законодательства РФ, а также внутренних инструкций и положений, регламентирующих деятельность по обработке и защите ПДн;
- отслеживать изменения действующего законодательства РФ по вопросам защиты и обработки ПДн;
- согласовывать свои действия по обработке и защите ПДн с сотрудниками отдела информационной безопасности _____;
(название МО)
- участвовать в проведении служебных расследований по фактам нарушения функционирования информационной системы персональных данных, а также других случаев нарушения правил обработки и защиты ПДн в соответствующем структурном подразделении;
- организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
- организовать ведение журнала учета обращений субъектов ПДн;
- организовать инструктаж должностных лиц, уполномоченных на обработку ПДн в информационных системах персональных данных.

III. Права ответственного за организацию обработки персональных данных

4. Должностное лицо, ответственное за организацию обработки ПДн в _____ имеет право:
(название МО)

- требовать от должностных лиц, уполномоченных на обработку персональных данных, безусловного соблюдения установленных правил обработки и защиты ПДн;
- требовать от должностных лиц, уполномоченных на обработку персональных данных прекращения обработки ПДн, в случаях их неправомерного использования и нарушения установленного порядка обработки;
- обращаться к ответственному (подразделение учреждения, назначенное ответственным) за организацию защиты персональных данных _____
(название МО)

с запросом об оказании необходимой технической и методической помощи в работе;
- доступа во все помещения соответствующего структурного подразделения, где осуществляется обработка ПДн.

IV. Ответственность

5. Должностное лицо, ответственное за организацию обработки ПДн в _____ несет ответственность:
(название МО)

- за качество и полноту проводимых им работ по организации обработки ПДн в соответствии с функциональными обязанностями, определенными настоящей Инструкцией;
- за сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты ПДн.

Образец

Приложение № 3
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от _____ № _____

ПРИКАЗ

О допуске сотрудников *(название Медицинской организации)*
к обработке персональных данных

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1. Утвердить список сотрудников _____,
(название МО)

доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей (прилагается).

2. Допустить указанных сотрудников к обработке персональных данных.

Главный врач _____
(Ф.И.О.)

Приложение к приказу

_____
(название МО)

от _____№_____

Список
сотрудников *(название МО)*, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных (трудовых) обязанностей

№	Фамилия Имя Отчество	Должность	Информационная система персональных данных
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Образец

Приложение № 4
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

О порядке допуска лиц в защищаемые помещения

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»,приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

ПРИКАЗЫВАЮ:

1. Утвердить список помещений, предназначенных для обработки персональных данных (Приложение).

2. Руководителям структурных подразделений медицинской организации:

1) в срок до _____ представить в отдел _____ списки сотрудников для организации допуска сотрудников в помещения, утвержденные списком;

2) разместить списки лиц, имеющих право самостоятельного доступа в помещения для обработки ПДн на дверях помещений с внутренней стороны.

3. Запретить нахождение в помещениях, предназначенных для обработки ПДн, посторонних лиц без сопровождения лиц, имеющих право самостоятельного доступа.

4. В нерабочее время помещения для обработки ПДн должны закрываться на ключ и сдаваться под охрану.

5. Установку и замену оборудования в помещениях, предназначенных для обработки ПДн, а также ремонт помещений проводить по согласованию с отделом _____.

6. Возложить ответственность за соблюдение режима доступа в помещения, предназначенные для обработки ПДн, на лиц, постоянно работающих в помещениях, и руководителей структурных подразделений.

7. Возложить на _____
(должность, Ф.И.О)

контроль за списками лиц, допущенных для работы в помещениях, предназначенных для обработки ПДн.

8. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О)

Приложение к приказу

_____
(название МО)

от_____№_____

Перечень защищаемых помещений

№ п/п	Наименование помещения	Адрес и место расположения
1		
2		
3		
4		
5		
6		
7		

Образец

Приложение № 5
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

О назначении администратора информационной безопасности в
(название Медицинской организации)

Во исполнение постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», 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»
ПРИКАЗЫВАЮ:

1. Назначить ответственным за выполнение работ по технической защите персональных данных (администратором информационной безопасности) в _____
(название МО)

_____ .
(должность, Ф.И.О)

2. Выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) возложить на _____
(название подразделения)

(начальник _____).
(Ф.И.О начальника подразделения)

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

– план мероприятий по обеспечению защиты персональных данных;

– перечень персональных данных, подлежащих защите;

– положение о порядке обработки и обеспечении безопасности персональных данных;

– определить уровни защищенности персональных данных при их обработке в ИСПДн для каждой ИСПДн с оформлением актов;

– частную модель угроз для каждой ИСПДн;

– матрицу доступа сотрудников к персональным данным;

– журнал учета 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 носителей персональных данных;

– журнал регистрации и учета обращений субъектов персональных данных;

– инструкцию администратора безопасности ИСПДн;

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____

(Ф.И.О)

Образец

Приложение № 6
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

О назначении ответственных за обезличивание персональных данных

Во исполнение постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», 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»

ПРИКАЗЫВАЮ:

1.Утвердить Перечень сотрудников _____
(название МО)

ответственных за проведение мероприятий по обезличиванию персональных данных (Приложение).

2.Указанным в перечне сотрудникам производить выполнение обезличивание персональных данных в соответствии с правилами, определенными приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О)

Приложение к приказу

_____
(название МО)

от _____№_____

ПЕРЕЧЕНЬ
сотрудников *(название МО)*, ответственных за проведение мероприятий по обезличиванию персональных данных

№ п/п	Ф.И.О, должность	Примечание
1.		
2.		

Образец

Приложение № 7
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об утверждении Положения об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации

Во исполнение Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, на основании Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

ПРИКАЗЫВАЮ:

1.Утвердить:

1) Положение об организации и проведении работ в _____
(название МО)

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение № 1).

2) типовые формы журналов:

- учета установленных средств защиты информации (Приложение № 2);
- журнала учета машинных носителей (Приложение № 3);
- журнала учета хранилищ (Приложение № 4);
- журнала периодического тестирования средств защиты (Приложение № 5);
- журнала учета нештатных ситуаций информационных систем персональных данных (далее-ИСПДн), выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн (Приложение № 6);
- журнала учета пользователей, допущенных к информационным системам персональных данных (Приложение № 7);
- журнала проверок электронных журналов (Приложение № 8);
- журнала учета обращений субъектов персональных данных (далее-ПДн) о выполнении их законных прав (Приложение № 9).

2 _____ завести журналы согласно типовым формам.
(должность, Ф.И.О)

3. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О)

Приложение № 1
к приказу _____
(название МО)
от _____№_____

ПОЛОЖЕНИЕ
об организации и проведении работ по обеспечению безопасности персональных данных обрабатываемых в информационных системах персональных данных и/или без использования средств автоматизации.

1. Общие положения.

1.1. Данное «Положение об организации и проведении работ в _____
(название МО)
по обеспечению безопасности персональных данных при их автоматизированной обработке и/или без использования средств автоматизации в информационных системах персональных данных» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационных системах персональных данных (далее – ИСПДн).

1.2. Положение определяет порядок работы пользователей и администраторов ИСПДн, сотрудников, ответственных за техническое обеспечение, а также администратора информационной безопасности, в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ИСПДн, порядок создания резервных копий ИСПДн, правила хранения и регистрации носителей информации а также порядок обезличивания ПДн.

1.3. При обеспечении безопасности персональных данных в ИСПДн с

использованием криптографических средств защиты информации все сотрудники

(название МО)

обязаны выполнять требования, изложенные в документе «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» (ФСБ России, № 149/6/6-622, 2008).

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа, который издается руководителем _____ (далее руководитель), и в соответствии со

(название МО)

списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за нормальное функционирование и контроль работы средств защиты информации в ИСПДн руководителем назначается администратор информационной безопасности; с целью контроля выполнения необходимых мероприятий по обеспечению безопасности назначается ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются в матрице доступа, которая создается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн и утверждается руководителем организации. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, может, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей.

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ,

установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ в помещение, в котором производится обработка ПДн, аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и ***обязан***:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;
- хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);
- хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе, или ящике, закрывающемся на ключ;
- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн и (или) администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным защищаемым СВТ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

2.8. Пользователю категорически ***запрещается***:

- использовать компоненты программного и аппаратного обеспечения персонального компьютера в неслужебных целях;
- вносить какие-либо изменения в конфигурацию аппаратных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные

средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания информации.

2.9. **Лица, ответственные за защиту персональных данных в** _____.
(название МО)

Ответственный за обработку ПДн - штатный сотрудник определяющий уровень доступа и ответственность лиц участвующих в обработке ПДн. Назначается приказом по учреждению.

Ответственный за обеспечение безопасности персональных данных – штатный сотрудник (или подразделение) отвечающий за проведение мероприятий, связанных с защитой ПДн (организационных и технических), а также осуществляющий контроль за соблюдением требований по защите ПДн в подразделениях. Назначается приказом по учреждению.

Администратор информационной безопасности – штатный сотрудник, ответственный за защиту автоматизированной системы (АС) от несанкционированного доступа (НСД) к информации. Назначается приказом по учреждению.

2.10. Администратор информационной безопасности (при его отсутствии ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого

пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;
- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;
- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;
- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;
- контролировать своевременное (не реже чем один раз в течение 60 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале;
- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в месяц;
- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;
- сопровождать подсистемы обеспечения целостности информации в ИСПДн;
- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки СЗИ при сбоях совместно с лицами, ответственными за техническое обеспечение.
- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;
- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;
- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования:

• проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

• сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;

• контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

• обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

• присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

• вести журнал учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн;

• поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения;

• в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

• докладывать ответственному за обработку персональных данных о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

• вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.11. Администратор информационной безопасности и ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок обработки персональных данных без использования средств автоматизации.

3.1. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях.

3.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.3. 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.

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

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

3.4.2. 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;

3.4.3. 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;

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

3.5. 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.

4. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации.

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. Резервному копированию подлежат базы данных ПДн, а так же прикладное программное обеспечение, предназначенное для работы с этими базами данных в случае, если оно подвергается модификации со стороны разработчиков ИСПДн.

4.3. Резервное копирование должно осуществляться в специально отведенный сетевой каталог на файловом сервере, а так же путем записи на отчуждаемый носитель.

4.4. Права доступа к сетевым каталогам должны исключать возможность доступа пользователей к резервным копиям других ИСПДн, хранящихся на сервере, при отсутствии допуска к работе в этих ИСПДн.

4.5. Базы данных и программное обеспечение должны копироваться в разные папки на файловом сервере.

4.6. На файловом сервере, помимо актуального состояния баз данных и программного обеспечения, должны храниться минимум два их исторических состояния.

4.7. Раз в месяц администратор ИСПДн создает резервную копию баз данных и программного обеспечения ИСПДн на отчуждаемый носитель, хранящийся у администратора информационной безопасности в закрывающемся на ключ хранилище.

4.8. К использованию, для создания резервных копии в ИСПДн, допускаются только зарегистрированные в журнале учета носители.

4.9. Резервное копирование на файловый сервер должно осуществляться непосредственно после любого изменения состояния баз данных или программного обеспечении этих баз, но не реже, чем раз в неделю.

4.10. Если программный продукт, на основе которого функционирует ИСПДн, имеет функцию резервного копирования, то администратор ИСПДн создает резервную копию при помощи данной функции.

4.11. Специалист, ответственный за техническое обеспечение учреждения создает резервную копию сетевого каталога, в котором хранятся резервные копии всех ИСПДн не реже чем раз в месяц.

4.12. Специалист, ответственный за техническое обеспечение учреждения, при помощи специализированного программного обеспечения, средств создает образы дисков всех рабочих мест ИСПДн не реже, чем раз в квартал.

4.13. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов либо полного

восстановления системы с образа диска.

4.14. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

4.15. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.16. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.17. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств на зарегистрированный носитель.

4.18. Ответственность за проведение резервного копирования ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИСПДн.

4.19. Ответственность за проведение резервного копирования сетевого каталога хранения резервных копий ИСПДн возлагается на специалистов, ответственных за техническое обеспечение учреждения.

4.20. Мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных организуются и проводятся специалистов, ответственных за техническое обеспечение учреждения, привлечением ответственного пользователя той ИСПДн, функционирование которой было нарушено.

5. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий.

5.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

5.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях _____, (название МО)

учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

- выявление демаскирующих признаков объектов ИСПДн;

- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

5.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн _____ (название МО)

и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

5.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее – ОБ ПДн) мерам, предписанным законодательством РФ и установленным нормативными документами предприятия;

- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность проведения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

5.5. Основными видами технического контроля являются визуально-

оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

5.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор информационной безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

5.7. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию руководителя или ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора информационной безопасности. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

5.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора информационной безопасности и (или) ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн, в соответствии с утвержденным планом или по согласованию с руководителем.

5.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора информационной безопасности, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн информации, администратор ИСПДн. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

5.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в «Аттестате соответствия» (если проводилась аттестация) и (или) требованиям по безопасности персональных данных.

5.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;
- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;
- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем положении;
- выполнение требований по защите информационных систем от несанкционированного доступа;
- выполнение требований по антивирусной защите.

6. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных.

6.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

6.2.Пользователи должны продемонстрировать администратору информационной безопасности наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор информационной безопасности должен вести журнал учета пользователей, допущенных к информационным системам персональных данных.

6.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего положения, к работе в ИСПДн не допускаются.

6.4. Ответственным за организацию обучения и оказание методической помощи в _____
(название МО)

является администратор информационной безопасности.

6.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

6.6. К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж по обеспечению безопасности в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чём делается соответствующая запись в Журнале учёта допуска к работе в ИСПДн.

6.7. Администратор информационной безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

7. Порядок проверки электронного журнала обращений к ИСПДн.

7.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

7.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

7.3. Право проверки электронного журнала обращений имеют:

- администратор информационной безопасности;
- ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн;
- руководитель

7.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее – СЗИ) типа «Страж», «Secret Net», DallasLock и другие, проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

7.5. Если в ходе периодических, плановых или внеплановых проверок ИСПДн выявлены случай несанкционированного доступа (далее-НСД) к информации конфиденциального характера, то вступает в силу п.п. 3.7., 3.8. данного Положения.

7.6. Проверке подлежат все электронные журналы ИСПДн.

7.7. Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

7.8. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки администратор информационной безопасности делает соответствующую отметку в журнале и ставит свою роспись.

8. Правила антивирусной защиты.

8.1. На каждом компьютере ИСПДн должны быть установлены лицензионные антивирусные средства, сертифицированные ФСТЭК РФ.

8.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется специалистами, ответственными за техническое обеспечение информационных систем учреждения.

8.3. Специалисты, ответственные за техническое обеспечение информационных систем учреждения, осуществляют периодическое обновление антивирусных пакетов и контроль их работоспособности.

8.4.Установку и удаление средств антивирусной защиты также может осуществлять администратор информационной безопасности.

8.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

8.6. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройку средств антивирусной защиты выполняет администратор информационной безопасности, либо специалисты, ответственные за техническое обеспечение учреждения, по согласованию администратором информационной безопасности.

8.7. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

8.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором информационной безопасности должна быть выполнена антивирусная проверка ИСПДн.

8.9. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

8.10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором информационной безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора информационной безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

8.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора информационной безопасности.

8.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на специалистов по техническому обеспечению, администратора информационной безопасности и всех пользователей данной ИСПДн.

9. Правила парольной защиты.

9.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения

действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

9.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора информационной безопасности.

9.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями объекта вычислительной техники самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;

- в числе символов пароля ***обязательно*** должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;

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

- при смене пароля новое значение должно отличаться от предыдущих;

- пользователь не имеет права сообщать личный пароль другим лицам.

9.4. Администратор ИСПДн передает свои аутентификационные данные для запуска прикладного ПО БД ИСПДн на бумажном носителе в опечатанном конверте администратору информационной безопасности, который в свою очередь хранит их в закрывающемся на ключ хранилище.

9.5. В случае имеющейся служебной необходимости, продиктованной возникновением нештатных ситуаций или других форс-мажорных факторов, при условии отсутствия на рабочем месте пользователя ИСПДн, руководитель подразделения оформляет в письменном виде заявку на сброс пароля отсутствующего пользователя и направляет ее ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн. В заявке должно быть изложено обоснование необходимости сброса пароля, указаны Ф.И.О. пользователя, чей пароль необходимо сбросить, Ф.И.О., должность специалиста, который будет осуществлять обработку ПДн от имени отсутствующего пользователя, а так же временной отрезок, в течение которого им будет производиться обработка ПДн.

9.6. В случае, если основания, указанные в заявке, являются достаточными для сброса пароля, ответственный за защиту информации поручает администратору информационной безопасности сбросить, установленный в СЗИ от НСД, личный пароль указанного в заявке пользователя.

9.7. В случае, если прикладное ПО БД ИСПДн обладает системой аутентификации, пароль для запуска прикладного ПО сбрасывает администратор ИСПДн, либо ответственный пользователь, по той же заявке, в случае их отсутствия пароль имеет право сбросить администратор информационной

безопасности, воспользовавшись для входа в систему управления аутентификационными данными администратора ИСПДн.

9.8. После выполнения необходимых работ все пароли изменяются и на бумажных носителях в опечатанных конверте, передаются пользователям ИСПДн. После этого пользователи устанавливают себе новые пароли.

9.9. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 60 дней.

9.10. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

9.11. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) администратора информационной безопасности.

9.12. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

9.13. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора информационной безопасности.

10. Правила обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.

10.1.Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления и конфигурирования программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн.

10.2. Все изменения программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, должны производиться администратором информационной безопасности и/или лицами ответственными за техническое обеспечение учреждения (при согласовании с администратором информационной безопасности), на основании заявки администратора ИСПДн, направляемой ответственному за обработку персональных данных.

10.3. Обновление и конфигурация программного обеспечения, не используемого для непосредственной обработки ПДн и не являющегося ПО СЗИ, а также аппаратной составляющей элементов ИСПДн, осуществляется сотрудниками отдела технического обеспечения учреждения в обычном порядке.

10.4. В случае если АРМ проходил аттестацию соответствия требованиям защиты информации, изменение аппаратно – программной составляющей ИСПДн также производится основании заявки.

10.5. Изменение конфигурации программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных сотрудников ***запрещено***.

10.6. Процедура внесения изменений в конфигурацию программного обеспечения СЗИ и Прикладного программного обеспечения, используемого для обработки ПДн, инициируется заявкой администратора ИСПДн.

10.7. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);
- обновление(замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

10.8. Заявку администратора ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается администратору информационной безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке самостоятельно или с привлечением сотрудников, ответственных за техническое обеспечение учреждения.

10.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии администратора ИСПДн.

10.10. Установка или обновление подсистем ИСПДн должны проводиться в соответствии с технологией проведения модификаций программных комплексов данных подсистем, указанной в технической документации, если таковая имеется.

10.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт-дисков и т.п.), прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

10.12. ПО средств защиты информации устанавливается с носителей, обладающих специальной голографической наклейкой, подтверждающей их подлинность, если иное не указано в документации к данному ПО.

10.13. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также на совместимость с установленными программным обеспечением и операционной системой.

10.14. После установки (обновления) ПО, администратор информационной безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера, проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки, модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

10.15. Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя Организации.

10.16. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. При этом администратор информационной безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн.

10.17. Копии заявок могут храниться у администратора информационной безопасности:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
-для проверки правильности установки и настройки средств защиты ИСПДн

10.18. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора информационной безопасности и администратора ИСПДн.

11. Управление учетными записями пользователей.

11.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должна быть создана уникальная учетная запись пользователя.

11.2. Работу в ИСПДн сотрудник должен осуществлять только с использованием своего уникального имени пользователя. Работа в ИСПДн под чужой учетной записью, кроме случаев, описанных в п.9.5, ***запрещена.***

11.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой администратора ИСПДн по прилагаемой форме к настоящему Положению.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

11.4. Заявку рассматривает руководитель, визируя её, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору информационной безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

11.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор информационной безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 60 дней.

11.6. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя – администратор информационной безопасности.

11.7. Исполненные заявка и задание хранятся у администратора информационной безопасности.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

12. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических.

12.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

12.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

12.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками обрабатывающими конфиденциальную информацию, так и администратором информационной безопасности.

12.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за обработку персональных данных;
- администратор информационной безопасности.

12.5. Пользователю ИСПДн категорически запрещается:

- отключать СЗИ;
-производить обработку конфиденциальной информации в случае неработоспособности средств ее защиты (СЗИ);
- менять настройки СЗИ.

12.6. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5. то подлежат применению п.п. 3.7., 3.8. данного Положения.

12.7. Криптографические средства защиты информации должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

13. Порядок охраны и допуска посторонних лиц в защищаемые помещения.

13.1. Данный раздел Положения устанавливает порядок охраны помещений ИСПДн.

13.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

13.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа. Комиссией составляется акт вскрытия.

13.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убирают для хранения в опечатываемый сейф (металлический шкаф). Закрываемое помещение опечатывается личной печатью сотрудника, ответственного за помещение.

13.5. Постановка и снятие помещений под охрану производится охранником после окончания и перед началом рабочего дня соответственно.

13.6. Сотрудник, имеющий право на вскрытие помещений:

- производит проверку оттиска печати на двери помещения и исправность запоров;

- вскрывает помещение.

13.7. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и (или) ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия должностных лиц в помещение никто не допускается.

13.8. Руководитель, ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн и администратор информационной безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

13.9. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за обеспечение безопасности персональных данных при их обработке в ИСПДн, или руководителю, или администратору информационной безопасности. Помещения вскрывать запрещается.

13.10. Помещения вскрываются ответственным за помещение, или руководителем, или ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн в присутствии сотрудника охраны с составлением акта.

13.11. При передаче дежурства, если помещение в течение дня не вскрывалось, а также в выходные и праздничные дни принимающая дежурство смена поста охраны проверяет целостность печатей на дверях и пенале с ключами

13.12. Порядок пребывания посторонних лиц на территории

устанавливается соответствующим приказом.

14. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации.

14.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускается стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим порядком.

14.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

14.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

14.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

14.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

14.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: администратор ИСПДн, ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн, администратор информационной безопасности.

15. Обезличивание персональных данных.

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

15.2. 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.

15.3. Способы обезличивания при условии дальнейшей обработки персональных данных:

- метод введения идентификаторов;
- метод изменения состава или семантики;

- обобщение (понижение точности некоторых 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).

15.4. Для обезличивания персональных данных используются способы обезличивания, определенные приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» в соответствии с рекомендациями по использованию этих методов.

15.5. Решение о необходимости обезличивания персональных данных принимает руководитель Учреждения.

15.6. Начальники отделов, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

15.7. Сотрудники подразделений, обслуживающих базы данных с персональными данными, осуществляют непосредственное обезличивание выбранным способом.

15.8. Порядок работы с обезличенными персональными данными:

15.8.1. Обезличенные персональные данные не подлежат разглашению.

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

15.8.3. 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;

15.8.4. 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.

16. Порядок хранения медицинской документации.

Под Медицинской документацией в настоящем положении понимается медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях, медицинская карта стационарного больного, другие документы на бумажном носителе, находящиеся на постоянном хранении в медицинской организации.

Основанием для организации порядка хранения медицинской документации в медицинской организации являются Федеральные законы от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», от 27.07.2006 № 152-ФЗ «О персональных данных», приказ Министерства

здравоохранения Российской Федерации от 15.12.2014 № 834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению», письмо Минздравсоцразвития Российской Федерации от 04.04.2005 № 734/МЗ-14 «О порядке хранения амбулаторной карты».

16.1. На Медицинскую документацию в полной мере распространяются положения настоящего документа об особенностях обработки персональных данных без использования средств автоматизации .

16.2. Пациент, либо его законный представитель, в соответствии с положениями ч. 4 ст. 22 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», имеют право знакомиться с содержанием Медицинской документации в части информации, отражающей состояние здоровья пациента, получать выписки и копии.

16.3. Медицинская документация, выписки и копии из нее, предоставляется лечащим врачом лично пациенту или его законному представителю при наличии документов, подтверждающих его законное представительство.

16.4. Информация, содержащаяся в Медицинской документации или выписки из нее могут предоставляться третьим лицам с письменного согласия пациента. Без согласия пациента информация, содержащая в Медицинской документации, может предоставляться третьим лицам только по основаниям, изложенным в п.4 ст.13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в российской Федерации». Такая информация может предоставляться на основании мотивированного, надлежащим образом оформленного официального запроса соответствующего органа органам дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, органам прокуратуры в связи с осуществлением ими прокурорского надзора, органам уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно и пр.

Приложение № 2
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала учета установленных средств защиты информации

№ п/п	Наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Место установки СЗИ	Организация, установившая СЗИ Ф.И.О. установившего СЗИ, дата, подпись	Отметка об изъятии СЗИ: Ф.И.О. производившего изъятие СЗИ, дата, подпись	Примечание
1	2	3	4	5	6	7	8

Приложение № 3
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала учета машинных носителей информации

№ п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступления
1	2	3	4	5

Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
6	7	8	9	10

Приложение № 4
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата
1	2	3	4	5

Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
6	7	8

Приложение № 5
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование
1	2	3	4	5

Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
6	7	8

Приложение № 6
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО исполнителей и их подписи
1	2	3	4

ФИО ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
5	6	7

Приложение № 7
к приказу _____
(название МО)

от _____№_____

ТИПОВАЯ ФОРМА
журнала учета пользователей, допущенных к информационным системам персональных данных

№ п/п	Дата	Фамилия, имя, отчество пользователя	Наименование ИСПДн
1	2	3	4

Подпись пользователя об ознакомлении с Положением и требованиями по безопасности	Подпись администратора безопасности о готовности пользователя к работе в ИСПДн	Примечание
5	6	7

Приложение № 8
к приказу _____
(название МО)
от _____№_____

ТИПОВАЯ ФОРМА
Журнала проверок электронных журналов

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала
1	2	3	4

Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание
5	6	7

Приложение № 9
к приказу _____
(название МО)
от _____№_____

ТИПОВАЯ ФОРМА
Журнала учета обращений субъектов ПДн о выполнении их законных прав

№ п/п	Ф.И.О	Дата	Цель обращения	Регистрационный номер обращения
1	2	3	4	5

Образец

Приложение № 8
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1624-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об утверждении Положения об обработке персональных данных в
(название Медицинской организации)

Во исполнение ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке персональных данных в _____ _____ (Приложение).
(название МО)

2. _____ в срок до _____
(должность, Ф.И.О)

ознакомить с Положением под роспись сотрудников _____.
(название МО)

3. _____ в срок до _____
(должность, Ф.И.О)

разместить Положение на сайте _____
(название МО)

во исполнение п.2 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.Контроль за исполнением настоящего оставляю за собой.

Главный врач _____

(Ф.И.О.)

Приложение
к приказу _____
(название МО)
от _____№_____

Положение об обработке персональных данных в *(название МО)*

1. Настоящее Положение об обработке персональных данных устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований (далее – Положение).

Обработка персональных данных в _____
(название МО)
выполняется с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных субъектов, персональные данные которых обрабатываются в _____.
(название МО)

2. _____
(название МО)
в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – оператор персональных данных).

3. Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), гл. 14 Трудового кодекса Российской Федерации от 13.12.2001 № 197-ФЗ.

4. Субъектами персональных данных являются сотрудники _____,
(название МО)
граждане Российской Федерации, информация о которых содержится в информационных системах _____.
(название МО)

5. Целями Положения являются:

а) обеспечение защиты прав и свобод при обработке персональных данных сотрудников _____,
(название МО)

персональных данных граждан, содержащихся в информационных системах _____;
(название МО)

б) установление ответственности сотрудников _____
(название МО)

за невыполнение нормативных правовых актов, регулирующих обработку и защиту персональных данных.

6. Процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных:

а) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных;

б) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых _____
(название МО)

мер, направленных на обеспечение выполнения обязанностей оператора персональных данных, предусмотренных Федеральным законом;

в) ознакомление сотрудников _____,
(название МО)

непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, с требованиями по защите персональных данных.

7. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором персональных данных, оператор персональных данных в срок, не превышающий 3 рабочих дня с даты выявления неправомерной обработки персональных данных, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных.

В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор персональных данных в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении неправомерной обработки персональных данных или об уничтожении персональных данных оператор персональных данных обязан уведомить субъекта персональных данных или его представителя.

8. В случае достижения цели обработки персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 рабочих дней с даты достижения цели обработки персональных данных.

9. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор персональных данных обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий три рабочих дня с даты получения указанного отзыва. Об

уничтожении персональных данных оператор персональных данных в течении трех рабочих дней обязан уведомить субъекта персональных данных.

10. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в пунктах 7 – 9 Правил, оператор персональных данных осуществляет блокирование таких персональных данных, обеспечивает уничтожение персональных данных в срок до 6 месяцев, если иной срок не установлен действующим законодательством Российской Федерации.

11. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели хранения персональных данных, если срок хранения персональных данных не установлен Федеральным законом.

Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

12. Обработка персональных данных в информационных системах

_____
(название МО)

(далее – информационные системы персональных данных) осуществляется 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».

13. Обеспечение безопасности персональных данных в информационных системах персональных данных достигается путем:

а) определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

б) применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

в) применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

г) оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных;

д) учета машинных носителей персональных данных;

е) обнаружения фактов несанкционированного доступа к персональным данным и принятием мер по прекращению несанкционированного доступа;

ж) восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

з) установления правил доступа (пароль, логин и др.) к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.

14. Сотрудники _____*(название МО)*,

имеющие доступ к информационным системам персональных данных, обязаны:

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

б) вести учет электронных носителей информации, содержащих персональные данные, и осуществлять их хранение в металлических шкафах или сейфах;

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

г) соблюдать установленный порядок и правила доступа в информационные системы, не допускать передачу персональных кодов и паролей к информационным системам персональных данных;

д) принимать все необходимые меры к надежной сохранности кодов и паролей доступа к информационным системам персональных данных;

е) работать с информационными системами персональных данных в объеме своих полномочий, не допускать их превышения;

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

15. При работе сотрудников _____
(название МО)

в информационных системах персональных данных запрещается:

а) записывать значения кодов и паролей доступа к информационным системам персональных данных;

б) передавать коды и пароли доступа к информационным системам персональных данных другим лицам;

в) пользоваться в работе кодами и паролями других пользователей доступа к информационным системам персональных данных;

г) производить подбор кодов и паролей доступа к информационным системам персональных данных других пользователей;

д) записывать на электронные носители с персональными данными посторонние программы и данные;

е) копировать информацию с персональными данными на неучтенные электронные носители информации;

ж) выносить электронные носители с персональными данными за пределы территории _____;
(название МО)

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

и) приносить, самостоятельно устанавливать и эксплуатировать на персональном компьютере любые программные продукты, не принятые к эксплуатации;

к) открывать, разбирать, ремонтировать персональные компьютеры, вносить изменения в конструкцию, подключать нештатные блоки и устройства;

б) передавать информацию, содержащую персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и иное), а также использовать сведения, содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону.

16. Сбор, систематизацию, накопление, хранение, обновление, изменение, передачу, уничтожение (далее – обработка) документов работников _____,
(название МО)

содержащих персональные данные на бумажном носителе, осуществляют сотрудники _____
(подразделение, название МО)

в соответствии с гл.14 Трудового Кодекса Российской Федерации.

17. Все персональные данные должны быть получены непосредственно от сотрудников _____.
(название МО)

18. Документы, содержащие персональные данные, уничтожаются путем измельчения в бумагорезательной машине.

19. При смене сотрудника, ответственного за учет документов на бумажном носителе, содержащих персональные данные, составляется акт приема-сдачи этих материалов, который утверждается руководителем соответствующего структурного подразделения _____*(название МО)*.

20. При работе с документами на бумажном носителе, содержащими персональные данные, уполномоченные на обработку персональных данных сотрудники _____*(название МО)* обязаны:

а) ознакомиться только с теми документами, содержащими персональные данные, к которым получен доступ в соответствии со служебной необходимостью;

б) хранить в тайне ставшие известными им сведения, содержащие персональные данные, подлежащие защите, информировать непосредственного руководителя о фактах нарушения порядка работы с персональными данными и о попытках несанкционированного доступа к ним;

в) о допущенных нарушениях установленного порядка работы, учета и хранения документов, содержащих персональные данные, а также о фактах разглашения сведений, содержащих персональные данные, подлежащих защите, представлять непосредственным руководителям письменные объяснения.

21. Сотрудники, виновные в разглашении или утрате информации, содержащей персональные данные, несут ответственность в соответствии с законодательством Российской Федерации.

22. Контроль за исполнением сотрудниками _____ *(название МО)* требований настоящих Правил возлагается на руководителей структурных подразделений _____ *(название МО)* и назначенного приказом _____ *(название МО)* ответственного лица за организацию обработки персональных данных.

Образец

Приложение № 9
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об определении границ контролируемой зоны

В целях исключения неконтролируемого пребывания посторонних лиц при обработке персональных данных и в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации», утвержденными приказом Гостехкомиссии России от 30.08.2002 за № 282, приказом 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», рекомендациями ФСБ России «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ РФ 21.02.2008 № 149/54-144)
ПРИКАЗЫВАЮ:

1. Границами контролируемой зоны _____ (название МО)

считать периметр ограждающих конструкций главного лечебного корпуса по адресу _____.

2. Утвердить порядок доступа работников _____ (название МО)

в помещения, в которых ведется обработка персональных данных.

3. Контроль за актуализацией и выполнением настоящего приказа возложить на _____. (должность, Ф.И.О сотрудника)

Главный врач _____ (Ф.И.О.)

УТВЕРЖДЕН
Приказом _____
(название МО)

от_____№ _____

ПОРЯДОК

доступа работников *(название МО)* в помещения, в которых ведется обработка персональных данных

1. Настоящий Порядок доступа работников _____ *(название МО)* в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

2. Персональные данные относятся к конфиденциальной информации. Должностные лица, уполномоченные на обработку персональных данных, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях, исключая возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

4. При хранении носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только должностные лица, уполномоченные на обработку персональных данных приказом _____*(название МО)*.

6. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных, являются руководители структурных подразделений _____*(название МО)*.

7. Нахождение лиц, в помещениях _____*(название МО)*, предназначенных для обработки персональных данных, не являющихся уполномоченными на обработку персональных данных, возможно только в сопровождении сотрудника, уполномоченного на обработку персональных данных на время, обусловленное производственной необходимостью.

8. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за безопасность персональных данных.

Образец

Приложение № 10
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об утверждении Правил рассмотрения запросов субъектов ПДн в

(название Медицинской организации)

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1. Утвердить Правила рассмотрения запросов субъектов ПДн в _____, представленные в Приложении.
(название МО)

2. _____
(должность, Ф.И.О сотрудника)

в срок с _____ г. ознакомить под роспись субъектов ПДн _____
(название МО)

с правилами рассмотрения запросов субъектов ПДн в _____.
(название МО)

3. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О.)

Приложение
к приказу _____
(название МО)

от _____ № _____

Правила рассмотрения запросов субъектов персональных данных или их представителей в *(название МО)*

1. Настоящие Правила устанавливают порядок рассмотрения запросов субъектов персональных данных или их представителей в целях предотвращения нарушений законодательства Российской Федерации при обработке персональных данных, в том числе Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», 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 правыми актами, операторами, являющимися государственными или муниципальными органами» (далее – Правила).

2. _____
(название МО)

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» является оператором, осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (далее – оператор персональных данных).

3. Субъектами персональных данных являются сотрудники _____,
(название МО)

граждане Российской Федерации, информация о которых содержатся в информационных системах _____
(название МО)

(далее – субъекты персональных данных).

4. Субъект персональных данных или его представитель имеет право на получение следующей информации:

а) подтверждение факта обработки персональных данных оператором персональных данных;

б) правовые основания, цели и способы обработки персональных данных оператором персональных данных;

г) наименование и место нахождения оператора персональных данных, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором персональных данных или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);

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

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

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;

з) название или фамилию, имя, отчество (если имеется) и адрес лица, осуществляющего обработку персональных данных по поручению оператора персональных данных, если обработка поручена или будет поручена такому лицу;

и) иные сведения, предусмотренные Федеральным законом.

6. Обязанности оператора персональных данных при обращении к нему либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

а) оператор персональных данных обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение 30 рабочих дней с даты получения запроса субъекта персональных данных или его представителя;

б) в случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор персональных данных обязан дать в письменной форме мотивированный ответ, с указанием основания для такого отказа, в срок, не превышающий 30 рабочих дней со дня обращения субъекта персональных данных или его представителя либо от даты получения запроса субъекта персональных данных или его представителя.

7. Субъект персональных данных вправе требовать от оператора персональных данных 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.

8. Запрашиваемые сведения должны быть предоставлены субъекту персональных данных или его представителю оператором персональных данных 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.

9. В случае, если запрашиваемые сведения, а также обрабатываемые персональные данные не были предоставлены субъекту персональных данных для ознакомления в полном объеме, субъект персональных данных вправе обратиться повторно к оператору персональных данных или направить ему повторный запрос в целях получения дополнительных сведений и ознакомления с такими персональными данными не ранее чем через 30 рабочих 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. Повторный запрос должен содержать обоснование направления повторного запроса.

10. Оператор персональных данных вправе отказать субъекту персональных данных в выполнении запроса, не соответствующего условиям, предусмотренным Правилами. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении запроса лежит на операторе персональных данных _____.
(название МО)

Образец

Приложение № 11
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об утверждении формы согласия пациента на обработку персональных данных в *(название Медицинской организации)*

В соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1.Утвердить форму согласия пациента на обработку персональных данных в _____ (Приложение).
(название МО)

2. _____
(должность, Ф.И.О сотрудника)

обеспечить с _____ г. получение согласия пациентов на обработку персональных данных в _____
(название МО)

по форме, представленной в Приложении.

3. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О.)

Приложение
к приказу _____
(название МО)

от _____№_____

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(Ф.И.О. полностью)

проживающий (ая) по адресу_____,
(по месту регистрации)

паспорт _____,
(серия, номер, дата выдачи

_____,
наименование выдавшего органа)

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 «О персональных данных» № 152-ФЗ, подтверждаю свое согласие на обработку _____
(название МО, адрес МО в соответствии с учредительными документами)

(далее - Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, реквизиты полиса ОМС, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью, в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг, данные о праве на льготные рецепты, выписанные льготные рецепты при условии, что их **обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну**.

В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных.

Оператор вправе поручить обработку моих персональных данных с правами осуществлять все действия включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ГБУЗ СО «Медицинский информационно-аналитический центр», 620078, г. Екатеринбург ул. Гагарина 53; ГБУ СО ОПЕРАТОР «ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА» 620094, Россия, Свердловская область, Екатеринбург, ул. Большакова, 105; ООО «Фирма «Эскейп», 129010, г. Москва, Проспект Мира, д. 16, стр. 2; ООО «Корпоративные информационные рутины (КИР)», 420049, г. Казань, ул. 2-ая Газовая, д. 14, ООО «Медотрейд», 117997, г. Москва, ул. Вавилова, д. 69/75, оф. 1101; ООО «ПАРУС-Екатеринбург» (Региональный офис), 620014, г. Екатеринбург, ул. Маршала Жукова, д.13; ПАО «Ростелеком», 191002, Россия, г. Санкт-Петербург, ул. Достоевского, д. 15 с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будет осуществляться лицом, обязанным сохранять конфиденциальность.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (двадцать пять лет - для стационара, двадцать пять лет – для поликлиники).

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «___»_____ 20___г. и действует до окончания сроков хранения первичной медицинской документации.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Контактный телефон(ы) _____ **и почтовый адрес** _____
Подпись субъекта персональных данных _____

Образец

Приложение № 12
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-р

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от _____ №_____

ПРИКАЗ

Об утверждении формы согласия работника *(название Медицинской организации)* ***на обработку персональных данных***

В соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
ПРИКАЗЫВАЮ:

1.Утвердить форму согласия работника _____
(название МО)

на обработку персональных данных (Приложение).

2._____
(должность, Ф.И.О сотрудника)

в срок до _____ г. обеспечить получение согласия работников _____
(название МО)

на обработку персональных данных по форме, представленной в Приложении.

3.Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О.)

Приложение
к приказу _____
(название МО)
от _____№_____

СОГЛАСИЕ
на обработку персональных данных работника

Я, _____,
(Ф.И.О. полностью)
проживающий по адресу_____ ,
(по месту регистрации)
паспорт _____,
(серия, номер, дата выдачи
_____,
наименование выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 «О персональных данных» № 152-ФЗ, подтверждаю свое согласие на обработку _____
(название МО, адрес МО в соответствии с учредительными документами)

(далее - Оператор) моих персональных данных, содержащихся в личном деле и документах кадрового делопроизводства, включающих: фамилию, имя, отчество, гражданство, пол, дату рождения, место рождения, адрес местожительства, дата регистрации, контактный телефон, данные паспорта, должность, квалификационный уровень, сведения о заработной плате (доходах), банковских счетах, картах, семейное положение и данные о составе и членах семьи, данные трудовой книжки (вкладыша к трудовой книжке), данные документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, аттестации, подтверждении специальных знаний, присвоении ученой степени, ученого звания, сведения о наградах и званиях (при наличии), данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН), данные документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу), данные страхового свидетельства государственного пенсионного страхования (СНИЛС), сведения о социальных льготах, пенсионном обеспечении и страховании, данные документов об инвалидности (при наличии), данные страхового медицинского полиса обязательного медицинского страхования, медицинское заключение.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, передачу, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных.

Оператор вправе поручить обработку моих персональных данных с правами осуществлять все действия включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, передачу, уничтожение. ГБУЗ СО «Медицинский информационно-аналитический центр», 620078, г. Екатеринбург ул. Гагарина 53; ГБУ СО ОПЕРАТОР «ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА» 620094, Россия, Свердловская область, Екатеринбург, ул. Большакова, 105; ООО «Фирма «Эскейп», 129010, г. Москва, Проспект Мира, д. 16, стр. 2; ООО «Корпоративные информационные рутины (КИР)», 420049, г. Казань, ул. 2-ая Газовая, д. 14, ООО «Медотрейд», 117997, г. Москва, ул. Вавилова, д. 69/75, оф. 1101; ООО «ПАРУС-Екатеринбург» (Региональный офис), 620014, г. Екатеринбург, ул. Маршала Жукова, д.13; ОАО «Ростелеком», 191002, Россия, г. Санкт-Петербург, ул. Достоевского, д. 15 с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будет осуществляться лицом, обязанным сохранять конфиденциальность.

Срок хранения моих персональных данных соответствует сроку хранения личных дел в _____.
(название МО)

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «___»_____ 20___г. и действует до дня увольнения из

_____.
(название МО)

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для увольнения работника _____.
(название МО)

Контактный телефон(ы) _____ и почтовый адрес _____

Подпись субъекта персональных данных _____

Образец

Приложение № 13
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

Об обеспечении выполнения требований по использованию и обслуживанию СКЗИ

Во исполнение постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
ПРИКАЗЫВАЮ:

1. Назначить _____
(должность, Ф.И.О сотрудника)

ответственным за эксплуатацию криптографических средств защиты информации в информационных системах персональных данных

_____.
(название МО)

2. Утвердить должностную инструкцию сотрудника, ответственного за использование криптосредств (Приложение).

3. _____
(должность, Ф.И.О сотрудника)

в работе, связанной с использованием криптографических средств руководствоваться утвержденной должностной инструкцией, приказом ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств

криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» и приказом 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».

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____

(Ф.И.О.)

Приложение
к приказу _____
(название МО)
от _____№_____

Должностная инструкция сотрудника, ответственного за использование криптосредств

1. Общие положения.

1.1. Настоящий документ разработан в соответствии с положениями документа «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 (ФСБ России, № 149/6/6-622, 2008)» (далее Типовые требования) и приказом 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».

1.2. Настоящий документ определяет права и обязанности сотрудника, ответственного за использование криптосредств в организации.

1.3. Ответственный пользователь криптосредства назначается приказом руководителя.

2. Ответственный пользователь криптосредства обязан:

2.1. Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним;

2.2. Вести учет лиц, допущенных к работе с криптосредствами;

2.3. Производить установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

2.4. Проверять готовность криптосредств к использованию с составлением заключений о возможности их эксплуатации;

2.5. Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

2.6. Обеспечивать в соответствии с положениями Типовых требований обеспечение с использованием криптосредств безопасности персональных данных, выполнение требований к обеспечению безопасности криптосредств и ключевых документов к ним;

2.7. Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним ответственному за защиту информации;

2.8. Немедленно уведомлять руководство учреждения о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений,

хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;

2.9. Сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным Типовыми требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

3. Ответственный пользователь криптосредства имеет право:

3.1. Инициировать разбирательство и составление заключений по фактам нарушения условий, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

3.2. Ответственному пользователю запрещается разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

С должностной инструкцией
ознакомлен _____
(Ф.И.О.)

Образец

Приложение № 14
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

О создании комиссии по классификации информационных систем персональных данных

В целях исполнения положений статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», для проведения классификации информационных систем, обрабатывающих персональные данные
ПРИКАЗЫВАЮ:

1. Утвердить состав Комиссии по классификации информационных систем персональных данных в составе:

председатель комиссии - _____;
(должность, Ф.И.О сотрудника)

члены комиссии: _____.
(должность, Ф.И.О сотрудников)

2. Комиссии провести классификацию информационных систем персональных данных

_____
(название МО)

до _____ года в соответствии с требованиями законодательства Российской Федерации с оформлением актов классификации информационных систем персональных данных.

3. При проведении классификации комиссии руководствоваться требованиями постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных.

4. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач _____
(Ф.И.О.)

Образец

Приложение № 15
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

УТВЕРЖДАЮ
Главный врач_____
(название МО)

_____
(Ф.И.О)

«___» _____ 20___ г.
М.П.

АКТ
определения уровня защищенности
персональных данных при их обработке в информационной системе
персональных данных *(название ИСПДн)*

Комиссия, назначенная приказом №_____ от _____г., в составе:

председатель комиссии – _____ _____
(Ф.И.О сотрудника) (должность)

члены комиссии: _____ _____
(Ф.И.О сотрудника) (должность)

_____ _____
(Ф.И.О сотрудника) (должность)

провела классификацию информационной системы персональных данных (ИСПДн)

_____.
(название ИСПДн)

В ходе работы комиссия установила:

1) категория персональных данных (ПД) – _____;
2) тип субъектов – _____;
3) объем обрабатываемых персональных данных – _____;
4) актуальный тип угроз – _____;
5) заданные характеристики безопасности персональных данных, обрабатываемые в информационной системе ПДн: _____;
6) структура информационной системы: _____;
7) наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена: ___;
8) режим обработки персональных данных: _____;

9) режим разграничения прав доступа пользователей информационной системы: _____;

10) местонахождение технических средств: _____;

11) последствия для субъектов ПД при нарушении заданных характеристик безопасности ПД: _____.

12) Является ли ИСПДн ГИС: _____.

По результатам анализа исходных данных ИСПДн _____
(название ИСПДн)

присваивается уровень защищенности _____.

Председатель комиссии – _____ _____
Ф.И.О должность

Члены комиссии: _____ _____
Ф.И.О должность

_____ _____
Ф.И.О должность

Образец

Приложение № 16
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

УТВЕРЖДАЮ
Главный врач_____
(название МО)

_____
(Ф.И.О)

«___» _____ 20___ г.
М.П.

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных *(название ИСПДн)*

СОГЛАСОВАНО

_____	_____	_____
должность	подпись, дата	Ф.И.О

г. _____ 20___г.

Содержание

Определения

В настоящем документе используются следующие термины и определения:

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вирус (компьютерный, программный)– исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации - возможность получения информации и ее использования.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Не декларированные возможности– функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия)– доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся 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.

Побочные электромагнитные излучения и наводки– электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Обозначения и сокращения

АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ИС– информационная система
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
СФ СЗПДн – среда функционирования системы (подсистемы) защиты персональных данных
УБПДн – угрозы безопасности персональных данных

Введение

Модель угроз безопасности персональных данных (далее – Модель) при их обработке в ИСПДн

(название МО)

строится на основании отчета о результатах проведения внутренней проверки.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификация потенциальных нарушителей, оценка исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- Описание угроз;
- Оценку вероятности возникновения угроз;
- Оценку реализуемости угроз;
- Оценку опасности угроз;
- Определение актуальности угроз.

Модель угроз разработана на основании следующих документов:

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- 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»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной 15.02.2008 Заместителем директора ФСТЭК России;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной 14.02.2008 заместителем директора ФСТЭК России.
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждённые ФСБ РФ 21.02.2008 № 149/54-144.

Описание ИСПДн *(название ИСПДн)*

Описание условий создания и использования персональных данных.

Цель обработки ПДн.

ИСПДн

_____
(название ИСПДн)

предназначена для _____.

В ИСПДн обрабатываются следующие ПДн:

_____.
(список ПДн)

Исходя из состава обрабатываемых персональных данных, можно сделать вывод, что они относятся **к** _____.
(категория персональных данных)

Субъектами персональных данных являются _____.

Действия, осуществляемые с данными в ходе их обработки

В ИСПДн _____
(название ИСПДн)

оператором ПДн осуществляются следующие операции с персональными данными: _____.

Условия прекращения обработки ПДн: _____.

Правила доступа к защищаемой информации

Доступ к информации, содержащей персональные данные, регламентируется списком лиц, допущенных к обработке персональных данных, и осуществляется по уникальным имени пользователя и паролю.
ИСПДн осуществляет непосредственно обработку ПДн, разработчиком программного обеспечения для ИСПДн является _____.
Сотрудники_____
(название МО)

осуществляют обновление программного обеспечения и устранение неполадок в его работе.

Информационные технологии, базы данных, технические средства, используемые для создания и обработки персональных данных:

_____

Описание форм представления персональных данных

Персональные данные в ИСПДн _____
(название МО)

представлены в виде IP-протоколов, электрических сигналов, бит, байт, и файлов.

Матрица доступа

Матрица доступа в табличной форме отражает права всех групп пользователей ИСПДн на действия с персональными данными. Действия (операции) включают сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных).

Основные группы пользователей ИСПДн:

- **Администраторы ИСПДн**, осуществляющие настройку и установку технических средств ИСПДн и обеспечивающие ее бесперебойную работу;
- **Операторы ИСПДн**, осуществляющие текущую работу с персональными данными.
- **Разработчики ИСПДн**, осуществляющие разработку и поддержку программного обеспечения собственной разработки или стандартных программ, специально доработанных под нужды организации;

Таблица 1.

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Администратор 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*** ***передача*** ***блокирование*** ***уничтожение***
Оператор ИСПДн	Обладает правами доступа к подмножеству ПДн. Располагает информацией о топологии ИСПДн на базе локальной и (или) распределенной информационной системам, через которую он осуществляет доступ, и составе технических средств ИСПДн.	***сбор*** ***систематизация*** ***накопление*** ***хранение*** ***уточнение*** ***использование*** ***передача*** ***уничтожение***

Типовая роль	Уровень доступа к ПДн	Разрешенные действия
Разработчик ИСПДн	Обладает информацией об алгоритмах и программах обработки информации на ИСПДн. Обладает правами внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения. Располагает всей информаций о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн	

Характеристики ИСПДн

По структуре ИСПДн является _____.
По наличию подключений к сетям связи _____.
По режиму обработки персональных данных _____.
По разграничению прав доступа пользователей _____.
Все элементы ИСПДн находятся на территории РФ.

Классификация нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:
внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Внешний нарушитель.

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Внутренний нарушитель

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПДн обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I);
- администраторы конкретных подсистем или баз данных ИСПДн (категория II);
- пользователи ИСПДн (категория III);

- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);
- лица, обладающие возможностью доступа к системе передачи данных (категория V);
- сотрудники учреждения, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПДн, но не имеющие права доступа к ним (категория VI);
- обслуживающий персонал (охрана, работники инженерно–технических служб и т.д.) (категория VII);
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование, либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников). Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об ИС можно выделить следующие:

- общая информация – информации о назначения и общих характеристиках ИСПДн;
- эксплуатационная информация – информация, полученная из эксплуатационной документации;
- чувствительная информация – информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно-технических средств ИСПДн;
- данные о реализованных в ПСЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в ИС, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИС, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в ИС.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПДн включая информацию об уязвимостях технических и программных средств ИСПДн. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПДн в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об ИС являются лица категории III и лица категории VIII.

С целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

Предположения об имеющихся у нарушителя средствах реализации угроз.

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение;
- специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Для создания устойчивой СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

Оценка уровня исходной защищенности ИСПДн *(название ИСПДн)*

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1),

Результаты оценки уровня исходной защищенности ИСПДн, зависящие от технических и эксплуатационных характеристик ИСПДн, приведены в таблице №2

Таблица 2.

№ п/п	Технические и эксплуатационные характеристики ИСПДн	Оценка	Уровень защищенности
1.	По территориальному размещению		
2.	По наличию соединения с сетями общего пользования		
3.	По встроенным (легальным) операциям с записями баз персональных данных		
4.	По разграничению доступа к персональным данным		
5.	По наличию соединений с другими базами ПДн иных ИСПДн		
6	По уровню обобщения		
7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн, без предварительной обработки		
Исходный уровень защищенности ИСПДн:			

В результате оценки исходной защищенности ИСПДн установлено, что _____% характеристик соответствует уровню _____. В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной 14.02.2008 заместителем директора ФСТЭК России, исходная степень защищенности информационной системы персональных данных: _____.

Коэффициент защищенности Y_1 = _____ (0 – для высокой степени исходной защищенности ,5 – для средней, 10 – для низкой)

Оценка вероятности реализации угроз

Таблица 3.

Вероятность	Описание
маловероятно($Y_2 = 0$)	отсутствуют объективные предпосылки для осуществления угрозы (например, угроза утечки речевой информации при отсутствии в ИСПДн функций голосового ввода ПД)
низкая вероятность($Y_2 = 2$)	объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации)
средняя вероятность($Y_2 = 5$)	объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны
высокая вероятность($Y_2 = 10$)	объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты

Таблица 4.

Тип угроз безопасности ПДн	Вероятность	Комментарий
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		
1.3. Угрозы утечки информации по каналам ПЭМИН		
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		
2.1.2. Кража носителей информации		
2.1.3. Кража ключей и атрибутов доступа		
2.1.4. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ		
2.1.5.Несанкционированное отключение средств защиты		
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)		
2.2.2.Недекларированные возможности системного ПО и ПО для обработки персональных данных		
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей		
2.2.4. Перехват управления сетевым оборудованием ПО		
2.2.5. Загрузка ОС с недостоверных внешних носителей		
2.2.6.Несанкционированное использование систем удаленного администрирования		
2.3. Угрозы непреднамеренных 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		
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками		
2.3.3. Непреднамеренное отключение		

Тип угроз безопасности ПДн	Вероятность	Комментарий
средств защиты		
2.3.4. Выход из строя аппаратно-программных средств		
2.3.5. Сбой системы электроснабжения		
2.3.6. Стихийное бедствие		
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке		
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке		
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 пределами контролируемой зоны		
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями		
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.		
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.		
2.5.3.Угрозы выявления паролей по сети		
2.5.4.Угрозы навязывание ложного маршрута сети		
2.5.5.Угрозы подмены доверенного объекта в сети		
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях		
2.5.7.Угрозы типа «Отказ в обслуживании»		
2.5.8.Угрозы удаленного запуска приложений		
2.5.9.Угрозы внедрения по сети вредоносных программ		

Определение коэффициента реализуемости угроз (Y)

По итогам оценки уровня защищенности (Y_1)и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y)

Коэффициент реализуемости угрозы (Y):

$$Y = \frac{Y_1 + Y_2}{20}$$

Таблица 5.

Значение	Описание
$0 < Y < 0,3$	возможность реализации угрозы признается низкой
$0,3 < Y < 0,6$	возможность реализации угрозы признается средней
$0,6 < Y < 0,8$	возможность реализации угрозы признается высокой
$Y > 0,8$	возможность реализации угрозы признается очень высокой

Таблица 6.

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		
1.3. Угрозы утечки информации по каналам ПЭМИН		
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		
2.1.2. Кража носителей информации		
2.1.3. Кража ключей и атрибутов доступа		
2.1.4. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ		
2.1.5. Несанкционированное отключение средств защиты		
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)		
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных		
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей		
2.2.4. Перехват управления сетевым оборудованием		
2.2.5 Загрузка ОС с недостоверных внешних носителей		

2.2.6.Несанкционированное использование систем удаленного администрирования		
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 не антропогенного (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		
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками		
2.3.3. Непреднамеренное отключение средств защиты		
2.3.4. Выход из строя аппаратно-программных средств		
2.3.5. Сбой системы электроснабжения		
2.3.6. Стихийное бедствие		
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке		
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке		
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		
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями		
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.		
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.		
2.5.3.Угрозы выявления паролей по сети		
2.5.4.Угрозы навязывание ложного маршрута сети		
2.5.5.Угрозы подмены доверенного объекта в сети		
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях		
2.5.7.Угрозы типа «Отказ в обслуживании»		
2.5.8.Угрозы удаленного запуска приложений		
2.5.9.Угрозы внедрения по сети вредоносных программ		

Оценка опасности угроз

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

Таблица 6.

Опасность	Описание
низкая	если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных
средняя	если реализация угрозы может привести к негативным последствиям для субъектов персональных данных
высокая	если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных

Таблица 7.

Тип угроз безопасности ПДн	Опасность угрозы
1. УГРОЗЫ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ.	
1.1. Угрозы утечки акустической информации	
1.2. Угрозы утечки видовой информации	
1.3. Угрозы утечки информации по каналам ПЭМИН	
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	
2.1.2. Кража носителей информации	
2.1.3. Кража ключей и атрибутов доступа	
2.1.4. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	
2.1.5. Несанкционированное отключение средств защиты	
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)	
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	
2.2.4. Перехват управления сетевым оборудованием	
2.2.5 Загрузка ОС с недостоверных внешних носителей	
2.2.6.Несанкционированное использование систем удаленного администрирования	
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 не антропогенного (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	
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	
2.3.3. Непреднамеренное отключение средств защиты	

Тип угроз безопасности ПДн	Опасность угрозы
2.3.4. Выход из строя аппаратно-программных средств	
2.3.5. Сбой системы электроснабжения	
2.3.6. Стихийное бедствие	
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	
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	
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	
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.	
2.5.3.Угрозы выявления паролей по сети	
2.5.4.Угрозы навязывание ложного маршрута сети	
2.5.5.Угрозы подмены доверенного объекта в сети	
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	
2.5.7.Угрозы типа «Отказ в обслуживании»	
2.5.8.Угрозы удаленного запуска приложений	
2.5.9.Угрозы внедрения по сети вредоносных программ	

Оценка актуальности угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной (*Таблица 8*), для ИСПДн определяются актуальные и неактуальные угрозы.

После чего делается вывод о наличии актуальных угроз и мер защиты, направленных на снижения риска возникновения и последствий актуальных угроз.

Таблица 8.

Возможность реализации угрозы	Показатель угрозы безопасности		
	Низкая опасность	Средняя опасность	Высокая опасность
Низкая ($0 < Y < 0,3$)	неактуальная	неактуальная	актуальная
Средняя ($0,3 < Y < 0,6$)	неактуальная	актуальная	актуальная
Высокая ($0,6 < Y < 0,8$)	актуальная	актуальная	актуальная
Очень высокая ($Y > 0,8$)	актуальная	актуальная	актуальная

Таблица 9.

Тип угроз безопасности ПДн	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
1. Угрозы утечки по техническим каналам.			
1.1. Угрозы утечки акустической информации			
1.2. Угрозы утечки видовой информации			
1.3. Угрозы утечки информации по каналам ПЭМИН			
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			
2.1.2. Кража носителей информации			
2.1.3. Кража ключей и атрибутов доступа			
2.1.4. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ			
2.1.5. Несанкционированное отключение средств защиты			
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)			
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных			
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей			
2.2.4. Перехват управления сетевым оборудованием			
2.2.5 Загрузка ОС с недостоверных внешних носителей			
2.2.6.Несанкционированное использование систем удаленного администрирования			
2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (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			
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками			
2.3.3. Непреднамеренное отключение средств защиты			
2.3.4. Выход из строя аппаратно-программных средств			
2.3.5. Сбой системы электроснабжения			
2.3.6. Стихийное бедствие 2.3.7.			

Тип угроз безопасности ПДн	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
2.4. Угрозы преднамеренных действий внутренних нарушителей			
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке			
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке			
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			
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями			
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.			
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.			
2.5.3.Угрозы выявления паролей по сети			
2.5.4.Угрозы навязывание ложного маршрута сети			
2.5.5.Угрозы подмены доверенного объекта в сети			
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях			
2.5.7.Угрозы типа «Отказ в обслуживании»			
2.5.8.Угрозы удаленного запуска приложений			
2.5.9.Угрозы внедрения по сети вредоносных программ			

Заключение

Таким образом, актуальными угрозами безопасности ПДн для данной ИСПДн, являются:

_____.

Приложение № 17
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от _____ №_____

ПРИКАЗ

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в *(название Медицинской организации)*

Во исполнение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

ПРИКАЗЫВАЮ:

1.Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____(Приложение № 1).
(название МО)

2.Утвердить План внутренних проверок данных _____ (Приложение № 2).
(название МО)

3.Утвердить форму Протокола проведения внутренней проверки данных _____ (Приложение № 3)
(название МО)

4. Ответственному за обработку персональных данных _____
(Ф.И.О сотрудника)

в срок до _____ г. ознакомить под роспись сотрудников, допущенных к обработке персональных данных с Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____.
(название МО)

5. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач _____

(Ф.И.О.)

Приложение № 1
к приказу_____
(название МО)
от_____№_____

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных *(название МО)*

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных _____ *(название МО)* разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.

2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

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

2.1.1. соответствие полномочий пользователя матрице доступа;

2.1.2. соблюдение пользователями информационных систем персональных данных _____ парольной политики;
(название МО)

2.1.3. соблюдение пользователями информационных систем персональных данных _____ антивирусной политики;
(название МО)

2.1.4. соблюдение пользователями информационных систем персональных данных _____
(название МО)
правил работы со съемными носителями персональных данных;

2.1.5. соблюдение ответственными за криптографические средства защиты информации правил работы с ними;

2.1.6. соблюдение порядка доступа в помещения _____,
(название МО)
в которых расположены элементы информационных систем персональных данных;

2.1.7. соблюдение порядка резервирования баз данных и хранения резервных копий;

2.1.8. соблюдение порядка работы со средствами защиты информации;

2.1.9. знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

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

2.2.1. соблюдение порядка хранения бумажных носителей с персональными данными;

2.2.2. соблюдение порядка доступа к бумажным носителям персональных данных;
2.2.3. соблюдение порядка доступа в помещения, в которых обрабатываются и хранятся бумажные носители с персональными данными.

3. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям _____ (название МО) организует проведение периодических проверок условий обработки персональных данных.
3.2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее Ответственный) либо комиссией, образуемой руководителем _____ *(название МО)*.
3.3. Внутренние проверки проводятся по необходимости в соответствии с поручением руководителя _____ *(название МО)*.
3.4. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.
3.5. По итогам каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 3 к настоящему Приказу.
3.6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.
3.7. Протоколы хранятся у Ответственного либо Председателя комиссии в течение текущего года. Уничтожение Протоколов проводится Ответственным, либо комиссией самостоятельно в январе следующего за проверочным годом.
3.8. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю _____ *(название МО)* докладывает Ответственный либо Председатель комиссии.

Приложение № 2
к приказу_____
(название МО)

от_____№_____

План
внутренних проверок условий обработки персональных данных *(название МО)*

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя матрице доступа	Разрешительная система (матрица) доступа Политика _____ (название МО) в отношении обработки персональных данных		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Положение по защите персональных данных _____, (название МО) обрабатываемых в ИСПДн		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики			
4.	Соблюдение пользователями информационных систем персональных данных правил работы со съемными носителями персональных данных	Положение по защите персональных данных, обрабатываемых в ИСПДн _____ (название МО) Политика _____ (название МО) в отношении обработки персональных данных		
5.	Соблюдение ответственными за криптографические средства защиты информации правил работы с ними	Положение по защите персональных данных, обрабатываемых в ИСПДн _____ (название МО)		
6.	Соблюдение порядка доступа в помещения, где расположены элементы	Список помещений _____, (название МО) в которых обрабатываются		

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
	информационных систем персональных данных	персональные данные		
7.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Положение по защите персональных данных, обрабатываемых в ИСПДн _____ (название МО)		
8.	Соблюдение порядка работы со средствами защиты информации			
9.	Знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях			
10.	Хранение бумажных носителей с персональными данными	Положение по защите персональных данных _____ (название МО)		
11.	Доступ к бумажным носителям с персональными данными			
12.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Положение по защите персональных данных _____ (название МО) Список помещений _____, (название МО) в которых обрабатываются персональные данные		

Председатель комиссии _____

Приложение № 3
к приказу_____
(название МО)

от_____№_____

Форма протокола
проведения внутренней проверки *(название МО)*

Настоящий Протокол составлен в том, что __.__.201_ ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю проведена проверка _____.
тема проверки

Проверка осуществлялась в соответствии с требованиями _____
_____
_____.
название документа

В ходе проверки проверено:
_____
_____
_____
_____
_____
_____
_____.

Выявленные нарушения:
_____
_____
_____
_____
_____
_____
_____.

Меры по устранению нарушений:
_____
_____
_____
_____
_____
_____

_____.

Срок устранения нарушений: _____.

Должность Ответственного _____ Ф.И.О.

либо

Председатель комиссии: _____ Ф.И.О.

Члены комиссии:

Должность _____ Ф.И.О.

Должность _____ Ф.И.О.

Должность руководителя проверяемого подразделения _____ Ф.И.О.

Образец

Приложение № 18
к приказу Министерства здравоохранения
Свердловской области
от 20 ОКТ 2015 № 1622-п

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от_____ №_____

ПРИКАЗ

О порядке обработки персональных данных без использования средств автоматизации

С целью организации работ по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации 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»

ПРИКАЗЫВАЮ:

1.Утвердить список помещений, предназначенных для обработки персональных данных без использования средств автоматизации, Приложение № 1 к настоящему приказу.

2.Утвердить список сотрудников _____,
(название МО)

доступ которым к персональным данным, обрабатываемым без использования средств автоматизации, необходим для выполнения служебных обязанностей, Приложение № 2 к настоящему приказу.

3.Допустить указанных сотрудников к обработке персональных данных.

4.Руководителям структурных подразделений:

1) в срок до _____ представить администратору информационной безопасности _____ списки сотрудников для организации допуска
(Ф.И.О. сотрудника)
сотрудников в указанные помещения;

2) разместить списки лиц, имеющих право самостоятельного доступа в указанные помещения на дверях помещений, предназначенных для обработки персональных данных без использования средств автоматизации с внутренней стороны.

5. Запретить нахождение в указанных помещениях посторонних лиц без сопровождения лиц, имеющих право самостоятельного доступа.

6. В нерабочее время указанные помещения должны закрываться на ключ и сдаваться под охрану.

7. Возложить ответственность за соблюдение режима доступа в защищаемые помещения на лиц, постоянно работающих в помещениях, и руководителей структурных подразделений.

8. Возложить на ответственного за организацию обработки персональных данных в информационных системах персональных данных

_____ _____
(название МО) (Ф.И.О. сотрудника)

контроль за списками лиц, допущенных для работы в защищаемых помещениях.

9. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач

_____
(Ф.И.О.)

Приложение № 1
к приказу_____
(название МО)

от_____№_____

Список помещений, предназначенных для обработки персональных данных без использования средств автоматизации

№ п/п	Наименование помещения	Место хранения носителей персональных данных	Адрес расположения помещения
1			
2			

Приложение № 2
к приказу_____
(название МО)
от_____№_____

Список

сотрудников _____, доступ которым к персональным
(название МО)
данным, обрабатываемым без использования средств автоматизации, необходим для выполнения служебных (трудовых) обязанностей

№	Ф.И.О	Должность	Персональные данные	Категория персональных данных
1				
2				

Образец

Приложение № 19
к приказу Министерства здравоохранения
Свердловской области
от _____№_____

НАИМЕНОВАНИЕ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

от _____ №_____

О создании комиссии по уничтожению персональных данных

В целях исполнения положений статьи ст. 5, ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», для уничтожения персональных данных
ПРИКАЗЫВАЮ:

1.Утвердить состав Комиссии по уничтожению персональных данных в составе:

председатель комиссии – _____;
(должность, Ф.И.О.)

члены комиссии:

- _____
(должность, Ф.И.О.)
- _____
(должность, Ф.И.О.)

2. Утвердить форму акта уничтожения персональных данных (далее – Акт) (Приложение).

3. Комиссии по уничтожению персональных данных производить уничтожение персональных данных и носителей персональных данных _____
(название медицинской организации)
по мере возникновения необходимости. Действия по уничтожению персональных данных оформлять актом уничтожения по форме (Приложение).

4. Акты уничтожения персональных данных оформленные и подписанные членами комиссии хранить в отдельно выделенном деле.

5. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач

_____
(Ф.И.О.)

Приложение
к приказу_____
(название МО)
от_____№_____

Акт уничтожения персональных данных

Комиссия, наделенная полномочиями приказом _____
(название медицинской организации)
_____от _____№ _____,в составе:
_____
(должности, Ф.И.О.)
_____
_____
составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных[1]), подлежит уничтожению.

Учетный номер (при наличии)	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата	Примечание
1	2	3	4	5	6

Правильность произведенных записей в акте проверена.

Регистрационные данные на носителях информации перед стиранием с них информации с записями в акте сверены, произведено стирание содержащейся на носителях информации.

Регистрационные данные на носителях информации (твердой копии) перед их (носителей) уничтожением сверены с записями в акте и полностью уничтожены путем
_____

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

_____
(Ф.И.О., подпись, дата)
_____
(Ф.И.О., подпись, дата)
_____
(Ф.И.О., подпись, дата)

[1] В случае, если объем уничтожаемых документов позволяет перечислять их в Акте.