

**Государственное автономное учреждение Саратовской области
«Региональный центр оценки качества образования»
(ГАУ СО «РЦОКО»)**

**Утверждено приказом ГАУ СО
«Региональный центр оценки
качества образования» от «18»
декабря 2015 г. № 50 «О назначении
ответственных и организации работ
по защите информации, содержащей
персональные данные»**

**ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО
ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ИХ ОБРАБОТКЕ
ГОСУДАРСТВЕННОМ АВТОНОМНОМ УЧРЕЖДЕНИИ
САРАТОВСКОЙ ОБЛАСТИ «РЕГИОНАЛЬНЫЙ ЦЕНТР ОЦЕНКИ
КАЧЕСТВА ОБРАЗОВАНИЯ»**

Саратов, 2015

Содержание

1 Введение	5
2 Назначение и область действия	6
3 Роли персонала	6
4 Обязательные мероприятия по обеспечению безопасности ИСПДн	7
4.1 Общие требования	7
4.2 Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн	8
4.3 Требования к выводу ИСПДн из эксплуатации	10
5 Обеспечение технической защиты ПДн	11
5.1 Общие требования	11
5.2 Контроль за выполнением требований по защите ПДн	14
5.3 Учет отчуждаемых электронных носителей ПДн	14
6 Обязанности персонала.....	15
6.1 Обязанности Администраторов ИСПДн	15
6.2 Обязанности Ответственного за организацию обработки ПДн.....	16
6.3 Обязанности Ответственного за обеспечение безопасности ПДн	17
6.4 Обязанности Координатора по обращениям и запросам.....	18
7 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных.....	19
7.1 Цели организации внутреннего контроля	19
7.2 Проведение контрольных мероприятий	20
8 Условия обработки ПДн	22
9 Обязанности ГАУ СО «РЦОКО»	23
10 Процессы обработки ПДн.....	25
10.1 Сбор ПДн	25
10.2 Использование ПДн.....	26
10.3 Хранение ПДн	26
10.4 Передача ПДн.....	27
10.5 Уточнение ПДн	28
10.6 Блокирование ПДн.....	29
10.7 Уничтожение ПДн	29
11 Обеспечение конфиденциальности ПДн	31
Приложение А Форма Журнала учета отчуждаемых защищаемых электронных носителей	33

Приложение Б Форма Журнала учета технических средств защиты информации.....	34
Приложение В Описание ИСПДн (шаблон)	35
Приложение Г Форма письменного Согласия субъекта на обработку ПДн	36
Приложение Д Форма Уведомления субъекта об обработке ПДн	38
Приложение Е Перечень должностей работников, допущенных к работе с персональными данными	39
Приложение Ж Форма Приказа о ведении журнала учета заявителей.....	40
Приложение З Форма Акта об уничтожении ПДн	41
Приложение И Дополнения в трудовые договоры (должностные инструкции) работников.....	42
Приложение К Положения типового договора о неразглашении ПДн	43

Контроль версий документа

Версия	Описание изменений	Дата
1.0	Первая редакция	

1 Введение

1.1 Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн, в том числе при их обработке в информационных системах ПДн (далее – ИСПДн) государственном автономном учреждении Саратовской области «Региональный центр оценки качества образования» (далее – ГАУ СО «РЦОКО»).

1.2 Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

– Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

– Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

1.3 Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов ПДн и взаимодействия с уполномоченным органом по защите прав субъектов ПДн приказом Директора ГАУ СО «РЦОКО» назначается работник, ответственный за организацию обработки персональных данных, ответственный за обеспечение безопасности ПДн и Координатор по обращениям и запросам.

1.4 Настоящее Положение подлежит пересмотру и при необходимости актуализации в случае изменений в законодательстве Российской Федерации о ПДн.

2 Назначение и область действия

2.1 Настоящее Положение предназначено для организации процесса обеспечения безопасности ПДн в соответствии с требованиями действующего федерального законодательства.

2.2 Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

2.3 Положение обязательно для ознакомления и исполнения работником ГАУ СО «РЦОКО», являющимся Ответственным за организацию обработки ПДн, работником ГАУ СО «РЦОКО», являющимся Ответственным за обеспечение безопасности персональных данных, Администраторами ИСПДн и Координатором по обращениям и запросам.

3 Роли персонала

3.1 Во исполнение положений настоящего документа и соответствия требованиям законодательства Российской Федерации о ПДн, в ГАУ СО «РЦОКО» введены следующие роли персонала:

- Ответственный за организацию обработки ПДн;
- Ответственный за обеспечение безопасности ПДн;
- Координатор по обращениям и запросам;
- Администраторы ИСПДн.

3.2 Назначение вышеуказанных работников на роли Ответственного за организацию обработки ПДн, Ответственного за обеспечение безопасности ПДн и Координатора по обращениям и запросам осуществляется приказом директора ГАУ СО «РЦОКО».

4 Обязательные мероприятия по обеспечению безопасности ИСПДн

4.1 Общие требования

4.1.1 На основании инвентаризации ИС установлены ИСПДн, в которых осуществляется автоматизированная обработка ПДн, и процессы, в которых осуществляется неавтоматизированная обработка ПДн.

4.1.2 Для всех эксплуатируемых ИСПДн с автоматизированной обработкой ПДн определены уровни защищённости ПДн в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.3 В случае создания новых ИСПДн, расширении состава данных в существующих ИСПДн, модернизации ИСПДн, определение уровня защищенности ПДн в ИСПДн проводится в следующей последовательности:

1) на этапе создания ИС или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИС) приказом Директора ГАУ СО «РЦОКО» создается комиссия по проведению определения уровней защищенности ПДн в ИСПДн;

2) комиссия в указанный приказом «Об организации работ по защите информации, содержащей персональные данные и назначении ответственных» срок устанавливает категории и объем обрабатываемых ПДн в ИСПДн, а также определяет тип угроз безопасности ПДн, актуальных для ИС, наличие при обработке сведений о состоянии здоровья субъектов, принятия решений, влекущих юридические последствия, на основании исключительно автоматизированной обработки ПДн;

3) комиссия формирует Акты определения уровней защищенности ПДн для каждой ИСПДн, в которых указываются типы угроз безопасности ПДн в ИСПДн, перечень обрабатываемых категорий ПДн и количество записей, содержащих ПДн.

4.1.4 В ГАУ СО «РЦОКО» разработаны Модели угроз безопасности ПДн для всех ИСПДн. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с частью 5 статьи 19 ФЗ «О персональных данных».

4.1.5 На основании Моделей угроз и в зависимости от уровня защищенности ПДн в ИСПДн проведены выбор и реализация методов и способов защиты информации в ИСПДн.

4.1.6 Выбранные и реализованные методы и способы защиты ПДн в ИСПДн обеспечивают нейтрализацию выявленных угроз безопасности ПДн при их обработке в ИСПДн в составе системы защиты ПДн.

4.1.7 Для проведения работ по выбору и реализации методов и способов защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т. д.) могут по договору привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4.1.8 Общие технические требования по защите ПДн в ИСПДн ГАУ СО «РЦОКО» приведены в пункте 5.

4.2 Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн

4.2.1 Разработка ИСПДн должна включать следующие стадии:

– предпроектная стадия (включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн, на основании которого определяется предварительный класс ИСПДн, степень участия должностных лиц, актуализируются угрозы безопасности);

– стадия проектирования системы защиты ПДн для ИСПДн;

– стадия ввода в действие ИСПДн.

4.2.2 По результатам проведенного анализа и с учетом действующих требований законодательства РФ о ПДн и регуляторов разрабатываются:

– модель угроз безопасности персональных данных при их обработке в ИСПДн;

- акт об установлении уровня защищенности ПДн в ИСПДн;
- требования к защите ПДн при их обработке в ИСПДн.

4.2.3 При определении отсутствия недеklarированных возможностей в системном и/или программном прикладном обеспечении выполняются следующие мероприятия для подтверждения типа угроз безопасности ПДн в ИСПДн:

- проверка системного и/или прикладного программного обеспечения, включая программный код, на отсутствие недеklarированных возможностей с использованием автоматизированных средств и (или) без использования таковых;
- тестирование ИС на проникновения;
- использование в ИС системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

4.2.4 Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн производится с учетом введенной в промышленную эксплуатацию ГАУ СО «РЦОКО» системы защиты ПДн, включающей комплекс организационных и технических мер.

4.2.5 На стадии ввода в эксплуатацию ИСПДн проводятся следующие мероприятия:

- установка пакета прикладных программ ИСПДн совместно со средствами защиты информации (встроенными и наложенными);
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

4.2.6 В случае внедрения дополнительных средств защиты составляются Акты внедрения СЗИ по результатам их приемо-сдаточных испытаний.

4.2.7 Перед вводом новой ИСПДн в опытную эксплуатацию составляется соответствующий Акт о вводе в опытную эксплуатацию ИСПДн, а также Акт определения уровня защищенности ПДн в ИСПДн.

4.2.8 В случае успешного функционирования ИСПДн на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию составляется соответствующий Акт.

4.3 Требования к выводу ИСПДн из эксплуатации

4.3.1 В случае принятия решения о выводе ИСПДн из промышленной эксплуатации составляется Акт о выводе ИСПДн из промышленной эксплуатации.

4.3.2 При выводе ИСПДн из промышленной эксплуатации с целью обеспечения справочной поддержки, доступ к ней ограничивается определенным составом лиц с правами только на чтение.

4.3.3 После подписания Акта о выводе ИСПДн из промышленной эксплуатации ИСПДн переводится в архивный фонд ГАУ СО «РЦОКО»(в соответствии с ч. 2 ст. 13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

- доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководства ГАУ СО «РЦОКО» по согласованию с Ответственным за организацию обработки ПДн и владельцем ИСПДн;

- ПДн, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в соответствии с требованиями законодательства РФ;

- обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

- доступ в помещения, где осуществляется хранение выводимой из эксплуатации ИСПДн, должен быть ограничен;

- регламентирован перечень лиц, допущенных к работе с ИСПДн, переданной в архив;

- все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.) должны храниться в сейфах;
- разработано описание ИСПДн, переведенной в архивный фонд ГАУ СО «РЦОКО».

5 Обеспечение технической защиты ПДн

5.1 Общие требования

5.1.1 Обеспечение безопасности ПДн при их обработке в ИСПДн осуществляется на всех стадиях жизненного цикла ИСПДн и состоит из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования ИСПДн в случае реализации угроз.

5.1.2 В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности ПДн для каждой ИСПДн включают:

1) определение уровней защищенности ПДн в ИСПДн на основании Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2) выявление и закрытие технических каналов утечки ПДн на основе анализа и актуализации Модели угроз безопасности ПДн;

3) выбор и реализацию организационных и технических методов и способов защиты информации в ИС в зависимости от уровня защищенности ПДн в ИСПДн с учетом особенностей инфраструктуры и с учетом актуальных угроз безопасности ПДн в ИСПДн;

4) установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных СЗИ;

5) разработку дополнений к трудовым договорам (или должностных инструкций) по обеспечению безопасности ПДн при их обработке в ИСПДн для работников, задействованных в эксплуатации данной ИСПДн.

5.1.3 Предотвращение утечки ПДн по техническим каналам за счет побочных электромагнитных излучений и наводок реализуется в ГАУ СО «РЦОКО» организационными мерами и не требует специальных технических решений.

5.1.4 Защита ПДн при их обработке в ИСПДн от несанкционированного доступа и иных неправомерных действий осуществляется в ГАУ СО «РЦОКО» следующими методами и способами:

- введение разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая ПДн), ИСПДн и связанным с ее использованием работам, документам;

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также к местам хранения носителей информации, содержащей ПДн;

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая ПДн), программным средствам обработки (передачи) и защиты ПДн;

- регистрация действий пользователей и обслуживающего персонала ИСПДн, мониторинг попыток несанкционированного доступа;

- учет и хранение съемных носителей информации с ПДн и их обращение, исключаящее хищение, подмену и уничтожение;

- резервирование технических средств, дублирование массивов и носителей ПДн;

- использование защищенных каналов связи, используемых для передачи ПДн;

- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах контролируемой территории;

- периодический анализ защищенности распределенных ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);

- предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) и программных закладок;

- регистрация событий и мониторинг процессов обработки информации;
- контроль целостности программных средств;
- идентификация защищаемых ресурсов по именам;
- регистрация запуска/остановки программ обработки ПДн;
- регистрация вывода ПДн на печать;
- регистрация доступа процессов к защищаемым ресурсам;
- очистка оперативной памяти.

5.1.5 При организации взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами применяются следующие дополнительные методы и способы защиты ПДн от несанкционированного доступа:

- идентификация и аутентификация субъектов доступа и объектов доступа и управления доступом субъектов доступа к объектам доступа с целью защиты ПДн;
- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИСПДн;
- обнаружение вторжений в ИСПДн, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;
- защита ПДн при их передаче по каналам связи;
- использование средств антивирусной защиты;
- централизованное управление системой защиты ПДн.

5.1.6 Периодически производится проверка электронных журналов безопасности, в которых регистрируются события безопасности. К электронным журналам безопасности относятся:

- журнал безопасности операционной системы;
- журнал событий системы управления базой данных;
- журнал событий СЗИ;
- журнал событий системы контроля и управления физическим доступом.

5.1.7 К событиям безопасности в ИСПДн относятся следующие события:

- доступ (входа и выхода в систему и доступа к объектам);

- создание и удаление пользователей;
- изменение прав доступа и привилегий;
- подключение и отключение внешних устройств;
- изменение настроек средств защиты;
- события, генерируемые средствами защиты.

5.1.8 В ГАУ СО «РЦОКО» также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

5.1.9 Все технические СЗИ снабжены инструкциями по эксплуатации.

5.1.10 В ГАУ СО «РЦОКО» ведется учет технических СЗИ. Форма Журнала учета технических СЗИ приведена в приложении (Приложение Б).

5.1.11 Ответственность за ведение и поддержание в актуальном состоянии Журнала учета технических СЗИ возлагается на Ответственного за обеспечение безопасности ПДн.

5.2 Контроль за выполнением требований по защите ПДн

5.2.1 В соответствии с документом «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства РФ от 01 ноября 2012 г. № 1119, проводится периодический контроль за выполнением требований по обеспечению безопасности ПДн (не реже одного раза в три года).

5.2.2 Контроль функций системы защиты производится в рамках мероприятий, описанных в пункте 7.2 настоящего Положения.

5.2.3 Ответственность за контроль функций системы защиты ПДн возлагается на Ответственного за обеспечение безопасности ПДн.

5.3 Учет отчуждаемых электронных носителей ПДн

5.3.1 В ГАУ СО «РЦОКО» ведется учет защищаемых носителей ПДн. К защищаемым носителям ПДн относятся следующие:

- носители информации серверов;
- носители информации автоматизированного рабочего места (далее – АРМ);

– внешние запоминающие устройства (дискеты, флеш-накопители и т. п.), содержащие ПДн.

5.3.2 Форма учета защищаемых электронных носителей приведена в приложении (Приложение А).

5.3.3 Ответственность за учет защищаемых электронных носителей ПДн возлагается на Ответственного за обеспечение безопасности ПДн.

6 Обязанности персонала

Должностные инструкции Ответственного за организацию обработки ПДн, Ответственного за обеспечение безопасности ПДн, Администраторов ИСПДн и Координатора по обращениям и запросам расширены с учетом специфики обработки и защиты ПДн. Работники, назначаемые на данные роли, обязаны ознакомиться со своими должностными инструкциями.

В ГАУ СО «РЦОКО» не допускается совмещение ролей Администратора ИСПДн и Ответственного за обеспечение безопасности ПДн в лице одного работника в целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения критичных для безопасности ПДн полномочий у одного лица.

6.1 Обязанности Администраторов ИСПДн

В обязанности Администраторов ИСПДн входит:

- управление учетными записями пользователей комплекса ИСПДн;
- поддержание штатной работы комплекса ИСПДн;
- предоставление и прекращение доступа пользователей к ПДн в ИСПДн в соответствии с утвержденным Перечнем должностей работников, допущенных к работе с ПДн или с утвержденными заявками на доступ к ПДн;

- установка и конфигурирование аппаратного и программного обеспечения комплекса ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн;

- уточнение ПДн в случаях, определенных настоящим Положением и внутренним документом «Положение о порядке обработки обращений субъектов персональных данных и порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных»;

- блокирование ПДн в случаях, определенных настоящим Положением и внутренними документами «Положение о порядке обработки обращений субъектов персональных данных» и «Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных»;

- уничтожение ПДн в случаях, определенных настоящим Положением и внутренними документами «Положение о порядке обработки обращений субъектов персональных данных» и «Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных».

6.2 Обязанности Ответственного за организацию обработки ПДн

6.2.1 В обязанности Ответственного за организацию обработки ПДн входят:

- осуществление внутреннего контроля за соблюдением ГАУ СО «РЦОКО» и ее работниками законодательства РФ о ПДн, в том числе требований к защите ПДн;

- информирование работников ГАУ СО «РЦОКО» положений законодательства РФ о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

- осуществление контроля за приемом и обработкой обращений и запросов субъектов ПДн или их представителей;

- уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн, об изменениях реквизитов оператора ПДн;

- уведомление уполномоченного органа по защите прав субъектов ПДн по запросу этого органа с предоставлением необходимой информации в течение тридцати дней¹ с даты получения такого запроса.

6.2.2 Ответственный за организацию обработки ПДн обязан:

- запрашивать необходимую информацию у руководства и работников ГАУ СО «РЦОКО», относящуюся к обработке ПДн и необходимую для выполнения его обязанностей;

- контролировать выполнение обязанностей Ответственным за обеспечение безопасности ПДн, Координатором по обращениям и запросам, Администраторами

¹ Статья 20 ч.4 ФЗ «О персональных данных»

ИСПДн, а также выполнение требований законодательства и внутренних нормативных документов ГАУ СО «РЦОКО», регламентирующих обработку и обеспечение безопасности ПДн;

– назначать ответственного за уничтожение ПДн и контролировать выполнение процедуры уничтожения ПДн. Для выполнения уничтожения ПДн на бумажном носителе, в качестве лица, ответственного за уничтожение ПДн, назначается Администратор ИСПДн; в случае с другими носителями ПДн или если обработка ПДн осуществляется в ИСПДн, то в качестве лица, ответственного за уничтожение ПДн, назначается оператор ИСПДн;

– согласовывает заявки временного или разового допуска работника к работе с ПДн в связи со служебной необходимостью.

6.3 Обязанности Ответственного за обеспечение безопасности ПДн

6.3.1 В обязанности Ответственного за обеспечение безопасности ПДн входит:

- проведение контрольных мероприятий (см. пункт 5.2);
- предоставление сведений о ПДн Ответственному за организацию обработки ПДн в рамках проведения учета защищаемых носителей и проведения инвентаризации (см. пункт 5.3);
- установка, конфигурирование и администрирование аппаратных и программных средств защиты информации (далее – СЗИ) комплекса ИСПДн;
- учет защищаемых носителей ПДн (см. пункт 5.3);
- учет технических СЗИ (см. пункт 5.1, подпункты 5.1.9, 5.1.10);
- периодические ежемесячные² проверки журналов безопасности (см. пункт 5.1, подпункт 5.1.6);
- анализ защищенности ИСПДн;
- организация процесса обучения работников по направлению обеспечения безопасности ПДн;

² Периодичность проверки зависит от срока хранения информации в журналах безопасности, например, если информация в журнале безопасности хранится одну неделю, то проверки необходимо проводить еженедельно

– участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн (см. пункты 8 и 9).

6.3.2 Ответственный за обеспечение безопасности ПДн обладает следующими полномочиями:

– проводить плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности ПДн;

– запрашивать необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности ПДн.

6.4 Обязанности Координатора по обращениям и запросам

6.4.1 В обязанности Координатора по обращениям и запросам входит:

– обработка обращений субъектов ПДн;

– ведение Журнала учета обращений субъектов ПДн;

– обработка запросов уполномоченного органа по защите прав субъектов ПДн;

– ведение Журнала учета запросов уполномоченного органа по защите прав субъектов ПДн;

– ведение и хранение Журнала учета проверок уполномоченным органом по защите прав субъектов ПДн

– уведомление оператора об уничтожении и блокировании ПДн субъектов.

6.4.2 Описание процессов обработки обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов ПДн представлено внутренними документами «Положение о порядке обработки обращений субъектов персональных данных» и «Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных».

6.4.3 Координатор по обращениям и запросам обязан:

– запрашивать необходимую информацию у Администраторов ИСПДн;

– выдавать Администраторам ИСПДн распоряжения касательно блокирования, уточнения, уничтожения ПДн;

- оценивать правомерность полученных запросов уполномоченного органа по защите прав субъектов ПДн;

- созывать комиссию для решения вопросов по возражениям субъектов ПДн против принятия решений на основании исключительно автоматизированной обработки ПДн.

7 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

7.1 Цели организации внутреннего контроля

7.1.1 Организация внутреннего контроля процесса обработки ПДн в ГАУ СО «РЦОКО» осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2 Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на выполнение следующих задач:

- обеспечение соблюдения работниками ГАУ СО «РЦОКО» требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных;

- оценка компетентности персонала, задействованного в обработке ПДн;

- обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;

- выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений;

- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;

- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;

– осуществление контроля за исполнением рекомендаций и указаний по устранению нарушений.

7.2 Проведение контрольных мероприятий

7.2.1 Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости – внепланово.

7.2.2 Решение о необходимости проведения внеплановых контрольных мероприятий принимает Ответственный за обеспечение безопасности ПДн в ГАУ СО «РЦОКО». Данное решение должно быть обосновано возросшими рисками информационной безопасности для обрабатываемых ПДн и при существенных изменениях в среде обработки ПДн.

7.2.3 Контрольные мероприятия (проверки) организуются Ответственным за обеспечение безопасности ПДн.

7.2.4 Проведение контрольных мероприятий по обеспечению безопасности ПДн должно включать:

– проведение проверок деятельности работников ГАУ СО «РЦОКО», допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами;

– проведение проверок состояния защищенности ПДн, обрабатываемых в ИСПДн, включая проверку доступов пользователей к ПДн, выполнение требований по защите каждой конкретной ИСПДн, корректности работы системы защиты ПДн и т. д.

7.2.5 Плановые проверки включают в себя следующие типы проверок:

– проверка правильности приема и обработки обращений и запросов субъектов ПДн или их законных представителей;

– проверка работоспособности и эффективности технических средств ИСПДн и средств защиты;

– проверка ведения эталонных копий средств защиты, контроль их работоспособности;

- проверка соответствия предоставленных прав доступа пользователей к ПДн утвержденной матрице доступа;
- проверка настроек внутренней политики, определяющая минимальную длину и сложность паролей, периодичность смены паролей;
- проверка отсутствия на АРМ пользователей средств разработки;
- проверка отсутствия на АРМ пользователей нештатного программного обеспечения;
- периодическое тестирование функций системы защиты ПДн.

7.2.6 Периодическое тестирование функций системы защиты ПДн проводится при изменении программной среды и пользователей ИСПДн с помощью тест-программ, имитирующих попытки несанкционированного доступа, в том числе анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИСПДн.

7.2.7 Ответственный за обеспечение безопасности ПДн составляет план контрольных мероприятий на полугодие, в котором определяет состав и периодичность проведения проверок на данный период времени.

7.2.8 План контрольных мероприятий утверждает Ответственный за организацию обработки ПДн в ГАУ СО «РЦОКО».

7.2.9 Результаты проверок оформляются Актом о результатах проведения проверки (см. Приложение Г) и представляются Ответственному за организацию обработки ПДн для проведения анализов результатов.

7.2.10 Выявленные в ходе проверок нарушения, а также отметки об их устранении, фиксируются в Журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности ПДн. Форма Журнала приведена в приложении (Приложение В).

7.2.11 Выявленные нарушения расследуются в соответствии с Порядком проведения разбирательств настоящего Положения.

7.2.12 При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационной безопасности.

7.2.13 В случае передачи части функций в области информационных технологий третьим лицам, указанные контрольные мероприятия осуществляют

последние. Требования по осуществлению контрольных мероприятий указываются в договорах с этими третьими лицами.

8 Условия обработки ПДн

8.1 Обработка персональных данных может осуществляться в ГАУ СО «РЦОКО» с согласия субъектов персональных данных, за исключением случаев, предусмотренных законодательством, в частности:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

8.2 В следующих случаях требуется письменное согласие субъекта на обработку его ПДн:

1) включение ПДн субъекта в общедоступные источники ПДн;

2) обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

3) условием для осуществления деятельности ГАУ СО «РЦОКО» с ПДн является запрет на передачу ПДн третьим лицам без согласия в письменной форме субъекта ПДн.

8.3 В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает в письменной форме законный представитель субъекта ПДн.

8.4 Форма письменного согласия субъекта на обработку его ПДн для случаев, указанных в п. 3.2.2 приведена в Приложении Г.

8.5 При отсутствии письменного согласия субъекта на обработку его ПДн в форме, определенной законодательством, для возможности доказательства получения согласия субъекта на обработку ПДн рекомендуется брать согласие субъекта в произвольной форме.

8.6 Для каждого процесса ГАУ СО «РЦОКО», в рамках которого производится обработка ПДн, и для осуществления которого требуется письменное согласие субъекта ПДн, по приведенной форме составляется отдельный шаблон согласия на обработку с указанием целей обработки персональных данных в рамках данного процесса, видов персональных данных и необходимого периода их хранения.

8.7 В случае если ГАУ СО «РЦОКО» в соответствии с договором поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также обязательное указание целей передачи персональных данных и перечня видов, передаваемых на обработку персональных данных.

8.8 ГАУ СО «РЦОКО» и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

9 Обязанности ГАУ СО «РЦОКО»

В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных» ГАУ СО «РЦОКО» обязано:

а) предоставлять субъекту ПДн по его запросу, информацию, касающуюся обработки его ПДн, либо на законных основаниях предоставляет отказ в течение тридцати дней³ с даты получения запроса субъекта ПДн или его представителя;

б) уточнять обрабатываемые ПДн по требованию субъекта ПДн, блокирует или удаляет, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в

³ Статья 20 ч.1, 2 ФЗ «О персональных данных»

срок, не превышающий семи рабочих дней⁴ со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих эти факты;

в) вести Журнал учета обращений субъектов ПДн, в котором должны фиксироваться запросы субъектов ПДн на получение персональных данных, а также факты предоставления персональных данных по этим запросам;

г) уведомлять субъекта ПДн об обработке ПДн в том случае, если ПДн были получены не от субъекта ПДн (за исключением случаев, оговоренных в п. 4.2.1). Форма уведомления находится в Приложении Д;

д) в случае достижения цели обработки персональных данных незамедлительно прекращать обработку персональных данных и уничтожать соответствующие персональные данные в срок, не превышающий тридцати дней⁵, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между ГАУ СО «РЦОКО» и субъектом ПДн, либо если ГАУ СО «РЦОКО» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами;

е) в случае отзыва субъектом ПДн согласия на обработку своих ПДн прекращает обработку ПДн и уничтожает ПДн в следующие сроки:

1) в срок, не превышающий тридцати дней⁶ с даты достижения цели обработки ПДн, в соответствии с согласием субъекта на обработку его ПДн;

2) в срок, не превышающий тридцати дней⁷, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между ГАУ СО «РЦОКО» и субъектом ПДн, либо если ГАУ СО «РЦОКО» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами.

ж) уведомлять субъекта ПДн об уничтожении его ПДн;

⁴ Статья 21 ч.2 ФЗ «О персональных данных»

⁵ Статья 21 ч.4 ФЗ «О персональных данных»

⁶ Статья 21 ч.5 ФЗ «О персональных данных»

⁷ Статья 21 ч.4 ФЗ «О персональных данных»

и) немедленно прекращать обработку ПДн субъекта ПДн в случае поступления требования субъекта ПДн о прекращении обработки его ПДн в целях продвижения товаров, работ, услуг на рынке.

10 Процессы обработки ПДн

Обработка ПДн в ИСПДн включает в себя следующие основные процессы:

- сбор ПДн;
- использование ПДн;
- хранение ПДн в ИСПДн;
- передача ПДн;
- уточнение ПДн;
- блокирование ПДн;
- уничтожение ПДн.

10.1 Сбор ПДн

10.1.1 В случаях, если ПДн получены не от субъекта ПДн, то до начала обработки таких ПДн субъекту ПДн предоставляется следующая информация:

- наименование и адрес ГАУ СО «РЦОКО»;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные 152-ФЗ права субъекта ПДн;
- источник получения ПДн.

10.1.2 Форма уведомления субъекта об обработке ПДн приведена в приложении (Приложение Д).

10.1.3 Уведомление субъекта об обработке ПДн, полученных от других лиц, не осуществляется в следующих случаях:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим оператором;
- ПДн получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

– ПДн предоставлены общедоступными субъектом ПДн или получены из общедоступного источника;

– ГАУ СО «РЦОКО» осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн.

10.1.4 ГАУ СО «РЦОКО» может получать, обрабатывать и приобщать к личному делу работника данные о состоянии его здоровья при отсутствии письменного согласия, так как обработка ПДн осуществляется или необходима:

– для защиты жизни, здоровья или иных жизненно важных интересов работника ГАУ СО «РЦОКО», либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;

– для установления или осуществления прав ПДн работника ГАУ СО «РЦОКО», или третьих лиц;

– в соответствии с законодательством об обязательных видах страхования.

10.2 Использование ПДн

Использование ПДн, собранных в соответствии с разделом 10.1, в ИСПДн ГАУ СО «РЦОКО» осуществляется работниками подразделений, указанных в Перечне должностей работников, допущенных к работе с ПДн, в целях принятия решений или совершения иных действий в отношении субъекта персональных данных и обеспечения функционирования ГАУ СО «РЦОКО». Шаблон указанного перечня приведен в Приложении Е.

10.3 Хранение ПДн

10.3.1 Хранение ПДн в ГАУ СО «РЦОКО» осуществляется в соответствии со следующими требованиями:

– хранение каждой категории ПДн должно быть определено с указанием места их хранения;

– хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн в срок не более, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

– не осуществляется несанкционированное копирование ПДн на отчуждаемые носители информации;

– при хранении ПДн в ИСПДн соблюдаются условия, обеспечивающие конфиденциальность и сохранность ПДн;

– исключен несанкционированный доступ к ПДн (доступ разрешен только работникам ГАУ СО «РЦОКО», включенным в Перечень должностей работников, допущенных к работе с ПДн).

10.3.2 Работники ГАУ СО «РЦОКО», обладающие правом доступа к ПДн, несут ответственность за хранение ПДн на своих автоматизированных рабочих местах.

10.3.3 Копирование ПДн на внешние электронные носители, такие как флеш-накопители, внешние жесткие диски, CD, DVD и т. д., осуществляется только для выполнения должностных обязанностей.

10.4 Передача ПДн

10.4.1 Передача ПДн другим работникам ГАУ СО «РЦОКО» или третьим лицам осуществляется в следующих случаях:

– если передача ПДн необходима для исполнения работником трудовых обязанностей, связанных с обработкой ПДн;

– если она нужна для исполнения федерального законодательства.

10.4.2 Работникам ГАУ СО «РЦОКО», допущенных к работе с ПДн запрещено сообщать устно или письменно ПДн другим работникам или сторонним лицам, которые не участвуют в процессах обработки ПДн.

10.4.3 Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме и в том объеме запрашиваемой информации, который позволяет не разглашать дополнительную информацию о субъекте ПДн.

10.4.4 При передаче ПДн работники ГАУ СО «РЦОКО» запрещено сообщать ПДн субъекта ПДн третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы

жизни и здоровью субъекта ПДн, а также случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

10.4.5 Передача ПДн возможна только в том случае, если исключен несанкционированный доступ к ПДн в процессе передачи и обеспечивается конфиденциальность передаваемой информации. Если ГАУ СО «РЦОКО» на основании договора поручает обработку ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности ПДн при их передаче.

10.4.6 Согласие субъекта на передачу его ПДн не требуется, если сообщение информации или предоставление документов, содержащих ПДн, предусмотрено законодательством Российской Федерации.

10.4.7 Работники ГАУ СО «РЦОКО» осуществляют передачу ПДн субъекта ПДн представителю субъекта ПДн, проверив его полномочия в порядке, установленном законодательством Российской Федерации и ограничиваться только теми ПДн, которые необходимы для выполнения указанными представителями их функций.

10.4.8 В случаях поручения обработки ПДн другому лицу, ГАУ СО «РЦОКО» заключает договор с этим лицом, существенным условием которого является обязанность обеспечения указанным лицом конфиденциальности и безопасности ПДн при их обработке.

10.5 Уточнение ПДн

10.5.1 В случае выявления работником ГАУ СО «РЦОКО» недостоверных ПДн или неправомерных действий с ними работник информирует о данном факте ответственного за организацию обработки ПДн. Ответственный за организацию обработки ПДн в срок, не превышающий трех рабочих дней⁸ с даты этого выявления, инициирует выполнение действий, описанных в Положении о порядке обработки обращений субъектов персональных данных.

⁸ Статья 21 ч.3 ФЗ «О персональных данных»

10.5.2 В случае уточнения (изменения) ПДн необходимо известить третьих лиц, которым ранее были сообщены или переданы неверные или неполные ПДн, обо всех исключениях, исправлениях и дополнениях в них.

10.5.3 Об устранении допущенных нарушений или об уничтожении ПДн требуется уведомить субъекта ПДн или его законного представителя либо уполномоченный орган по защите прав субъектов ПДн в случае, если соответствующую проверку инициировал указанный орган.

10.6 Блокирование ПДн

10.6.1 В случае выявления работником ГАУ СО «РЦОКО» неправомерной обработки ПДн или выявления неточных ПДн при обращении субъекта или его представителя либо по запросу уполномоченного органа по защите прав субъектов ПДн, Ответственный за организацию обработки ПДн инициирует блокирование ПДн, относящихся к этому субъекту ПДн, и выполнение действий, описанных в Положении о порядке обработки обращений субъектов ПДн.

10.6.2 В случаях отсутствия возможности уничтожения ПДн, ГАУ СО «РЦОКО» осуществляет блокирование таких ПДн и обеспечивает уничтожение в срок не более шести месяцев.

10.7 Уничтожение ПДн

10.7.1 ПДн подлежат уничтожению (или обезличиванию) в следующих случаях в указанные сроки:

- по достижении целей обработки ПДн – в 30-дневный срок⁹;
- в случае утраты необходимости в достижении целей обработки ПДн – в 30-дневный срок¹⁰;
- в случае отзыва субъектом ПДн согласия на обработку своих ПДн – в 30-дневный¹¹ срок, если иной срок не предусмотрен договором или соглашением между ГАУ СО «РЦОКО» и субъектом ПДн, либо если ГАУ СО «РЦОКО» не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

⁹ Статья 21 ч.4 ФЗ «О персональных данных»

¹⁰ Статья 21 ч.4 ФЗ «О персональных данных»

¹¹ Статья 21 ч.5 ФЗ «О персональных данных»

10.7.2 ПДн подлежат уничтожению (или обезличиванию) в срок, не превышающий десяти рабочих дней¹² с даты выявления неправомерной обработки ПДн в следующих случаях:

- в случае если ПДн являются неполными, устаревшими, неточными (при условии, что уточнение ПДн невозможно);
- в случае если ПДн являются незаконно полученными;
- в случае если ПДн не являются необходимыми для заявленной цели обработки.

10.7.3 Процесс уничтожения ПДн при достижении целей их обработки либо в случае утраты необходимости в достижении этих целей инициирует Администратор ИСПДн, в которой эти ПДн обрабатываются.

10.7.4 Процесс уничтожения ПДн при отзыве субъектом ПДн согласия на обработку своих ПДн инициируется Координатором в соответствии с Положением о порядке обработки обращений субъектов ПДн.

10.7.5 В остальных случаях процесс уничтожения ПДн инициирует Ответственный за организацию обработки ПДн.

10.7.6 Администратор ИСПДн, в которой обрабатываются ПДн, согласовывает уничтожение ПДн с Ответственным за организацию обработки ПДн с использованием средств информационно-телекоммуникационной инфраструктуры.

10.7.7 Ответственный за организацию обработки ПДн на основании информации, указанной Перечне персональных данных, обрабатываемых в ГАУ СО «РЦОКО», определяет перечень ИСПДн осуществляется обработка ПДн.

10.7.8 Ответственный за организацию обработки ПДн назначает лицо, ответственное за уничтожение ПДн. В случае с бумажными носителями ПДн в качестве лица, ответственного за уничтожение ПДн, назначается Администратор ИСПДн. В случае с другими носителями ПДн или если обработка ПДн осуществляется в ИСПДн, то в качестве лица, ответственного за уничтожение ПДн, назначается владелец ИСПДн.

¹² Статья 21 ч.3 ФЗ «О персональных данных»

10.7.9 Лицо, ответственное за уничтожение ПДн, производит уничтожение ПДн, составляет соответствующий Акт об уничтожении ПДн, форма которого представлена в приложении (Приложение 3). После этого он направляет Акт об уничтожении ПДн Ответственному за организацию обработки ПДн.

10.7.10 Ответственный за организацию обработки ПДн утверждает Акт об уничтожении ПДн и уведомляет субъекта ПДн или его представителя.

10.7.11 В случае уничтожения ПДн по результатам проверки или запроса уполномоченного органа по защите прав субъектов ПДн, Координатор уведомляет об уничтожении ПДн субъекта ПДн или его представителя, а также указанный орган. Порядок уведомления описан в Положении о порядке обработки обращений субъектов ПДн.

10.7.12 В случае отсутствия возможности уничтожения ПДн в течение сроков, указанных в пунктах 10.7.1, 10.7.2, ПДн должны быть заблокированы, после чего ПДн должны быть уничтожены в срок, не превышающий шести месяцев. Порядок блокировки ПДн описан в Положении о порядке обработки обращений субъектов ПДн.

10.7.13 При уничтожении обеспечивается гарантированное уничтожение ПДн, исключающее возможность их восстановления программными или физическими методами.

10.7.14 Уничтожение бумажных носителей ПДн производится путем измельчения, сжигания или преобразования в целлюлозную массу таким образом, чтобы гарантировать, что их невозможно восстановить.

10.7.15 Уничтожение ПДн в ручном режиме составляется соответствующий Акт (Приложение 3).

11 Обеспечение конфиденциальности ПДн

11.1 ГАУ СО «РЦОКО» и иные лица, обладающие правом доступа к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено ФЗ «О персональных данных».

11.2 Для обеспечения безопасности персональных данных от неправомерных действий выполняются следующие организационные меры:

– информирование работников ГАУ СО «РЦОКО» по обеспечению безопасности ПДн при их обработке;

– своевременное выявление нарушений работниками требований к режиму конфиденциальности;

– все работники, имеющие действующие трудовые отношения, деятельность которых связана с получением и обработкой ПДн, подписывают обязательство о неразглашении ПДн либо заключают дополнительное соглашение к трудовым договорам.

– со всеми принимаемыми на работу работниками, деятельность которых будет связана с обработкой ПДн, заключаются трудовые договоры, работниками подписываются и соответствующие должностные инструкции, в которых отражены вопросы, обязанности обеспечения конфиденциальности ПДн (Приложение И);

– осуществляется разделение полномочий пользователей в ИСПДн в зависимости от их должностных обязанностей;

– наличие формализованной процедуры по предоставлению доступа к ИСПДн, а также по регулярному пересмотру (ревизии) прав доступа работников ГАУ СО «РЦОКО» в зависимости от занимаемой ими должности.

11.3 ГАУ СО «РЦОКО» передает ПДн на обработку третьим лицам (принимающей стороне), только если это необходимо для достижения целей обработки ПДн, причем существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности ПДн и безопасности ПДн при их обработке.

11.4 Передача ПДн третьим лицам без заключенного договора и без применения мер защиты ПДн не допускается.

11.5 Положения типового договора о неразглашении ПДн приведены в приложении (Приложение К).

Директор

А.А. Иванов

Приложение А
Форма Журнала учета отчуждаемых защищаемых электронных носителей

№ п/п	Тип носителя	Наименование модели	Инвентарный номер	Владелец информации	Ответственное лицо	Дата поступления носителя

Приложение Б
Форма Журнала учета технических средств защиты информации

№ п/п	Тип СЗИ	Наименование СЗИ	Индекс или условное наименование* (для сертифицированных СЗИ)	Регистрационный номер* (для сертифицированных СЗИ)	ИСПДн, в которой(ых) применяется СЗИ	Наличие и место хранения документации
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

* Перечень индексов, условных наименований и регистрационных номеров определяется ФСТЭК России и ФСБ России в пределах их полномочий

Приложение В Описание ИСПДн (шаблон)

1. Общее описание

Разработчик ИС:

Статус системы:

Пользователи:

2. Обрабатываемые в системе персональные данные

Сводная информация по обрабатываемым в АС персональным данным, представлена в таблице 1:

Таблица 1 – Обрабатываемые ПДн

№ п/п	Категория субъекта ПДн	Тип отношений	Перечень персональных данных	Хранение данных		
				Период/ способ уничтожения	Объем (записей)	Место и форма хранения

3. Структура системы

ИС состоит из следующих компонентов:

- 1)
- 2)

Сводная информация по ресурсам системы представлена в таблице 2:

Таблица 2 – Ресурсы системы

Сервер АС	Компонент	Установленное ПО			Кол-во	Физическое размещение
		ОС	СУБД	ШО		
Основные ресурсы						
Вспомогательные ресурсы						

Приложение Г

Форма письменного Согласия субъекта на обработку ПДн

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

(Ф.И.О. полностью) _____,
зарегистрированный по адресу: _____,
удостоверение личности (паспорт, _____)
серии _____ № _____ выдан _____
_____ « ____ » _____ Г.,

От лица (Ф.И.О. полностью) _____,
зарегистрированного по адресу: _____,
удостоверение личности (паспорт, _____)
серии _____ № _____ выдан _____
_____ « ____ » _____ Г.,

На основании _____
(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

в соответствии с требованиями статьи 9 Федерального закона № 152-ФЗ «О персональных данных» от 27.07.06 г. **передаю персональные данные и даю согласие на их обработку** с использованием и без использования средств автоматизации ГАУ СО «РЦОКО» (далее – Оператор), расположенного по адресу: 410028, г. Саратов, ул. им. Мичурина И. В., д. 89.

Цели обработки, состав данных, срок действия и порядок отзыва данного согласия определены в таблице ниже.

№	Цель обработки	Состав персональных данных	Срок обработки (с момента подписания согласия)	Порядок отзыва согласия

Настоящее согласие распространяется на сбор, запись, систематизацию, накопление, хранение, запись на электронные носители и их хранение, уточнение,

обновление, изменение, извлечение, использование (в том числе передача в случаях, прямо предусмотренных целями обработки и действующим законодательством), обезличивание, блокирование, удаление, уничтожение и иные способы обработки.

По поручению Оператора обработка персональных данных может производиться:

(Наименование или Ф.И.О. Уполномоченного лица) _____,
находящимся по адресу: _____.

« ____ » _____ 20__ г. _____ / _____

Приложение Д

Форма Уведомления субъекта об обработке ПДн

Субъекту персональных данных:
(Ф.И.О.)

Адрес:

УВЕДОМЛЕНИЕ об обработке персональных данных

Оператор персональных данных: ГАУ СО «РЦОКО»,
находящийся по адресу: г. Саратов, ул. им. Мичурина И. В., д. 89,
руководствуясь _____

(правовое основание обработки персональных данных)

с целью _____

(цель обработки персональных данных)

осуществляет обработку Ваших персональных данных, включая:

_____ (перечисление персональных данных, находящихся в обработке: Ф.И.О., адрес, телефон...)

полученных _____

(источник получения персональных данных)

Обработка вышеуказанных персональных данных осуществляется путем:

_____ (перечень действий с персональными данными,

_____ общее описание используемых оператором способов обработки персональных данных)

К персональным данным имеют или могут получить доступ следующие лица:

_____ (перечень конкретных лиц или должностей)

Обработка указанных персональных данных будет являться основанием для

_____ (решения, принимаемые на основании обработки; возможные юридические последствия обработки)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:

_____ (должность)

_____ (подпись)

_____ (Ф.И.О.)

« ___ » _____ 201__ г.

Приложение Е

Перечень должностей работников, допущенных к работе с персональными данными

№ п/п	Вид ПДн (из перечня)	Должность	Цель доступа	Права доступа	Срок доступа	Примечание

Приложение Ж Форма Приказа о ведении журнала учета заявителей

П Р И К А З

№ _____

« ____ » _____ 20__ г.

О пропуске заявителей
на территорию ГАУ СО «РЦОКО»

П Р И К А З Ы В А Ю:

С целью обеспечения пропускного режима разрешать допуск заявителей на территорию ГАУ СО «РЦОКО»

(помещения, предназначенные для приема заявителей)

по предъявлении паспорта или иного документа, удостоверяющего личность заявителя ГАУ СО «РЦОКО», с одновременной регистрацией факта посещения в Журнале учета заявителей.

В Журнал учета заявителей должны заноситься время посещения, фамилия, имя, отчество заявителя, паспортные данные или данные иных документов, удостоверяющих личность заявителей ГАУ СО «РЦОКО», название организации, которую представляет заявитель, а также фамилия, имя, отчество и должность работника, являющегося представителем принимающего данного заявителя работника ГАУ СО «РЦОКО».

Ответственность за сохранность и ведение Журнала учета заявителей возложить на _____.

(ответственное подразделение)

Определить срок обработки персональных данных, заносящихся в Журнал учета заявителей, в 3 года.

Директор А.А. Иванов

Приложение 3
Форма Акта об уничтожении ПДн

УТВЕРЖДАЮ

«__» _____ 20__ г.

Акт № _____

об уничтожении персональных данных

№ п/п	Дата	Место и форма хранения ПДн	Тип носителя ПДн и его регистрационный номер/уничтожаемые ПДн

Всего уничтожено носителей (прописью): _____.

Уничтожение произведено путем

_____.

Ответственный за уничтожение (Ф.И.О., должность):

_____.

Дата: _____.

Подпись: _____.

Приложение И

Дополнения в трудовые договоры (должностные инструкции) работников

В раздел трудовых договоров (должностных инструкций) персонала ИСПДн, закрепляющий должностные обязанности, необходимо включить следующий пункт:

1) При работе с информационными системами персональных данных следует руководствоваться требованиями к порядку обработки и обеспечения безопасности персональных данных, закрепленными в Положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУ СО «РЦОКО».

В раздел «Ответственность» трудовых договоров (должностных инструкций) работников ГАУ СО «РЦОКО», допущенных к обработке ПДн для выполнения своих должностных обязанностей, необходимо включить следующие пункты:

1) Работник ГАУ СО «РЦОКО» несет ответственность за обеспечение конфиденциальности ПДн, ставших ему известными в связи с выполнением должностных обязанностей.

2) Работник ГАУ СО «РЦОКО» несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности ПДн, установленных в Положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУ СО «РЦОКО».

3) В случае нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения ГАУ СО «РЦОКО», его работникам или клиентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение К

Положения типового договора о неразглашении ПДн

ДОГОВОР

о неразглашении ПДн

ТЕРМИНЫ

В настоящем Договоре используются следующие термины, если иное не следует из контекста:

«Персональные данные» означают любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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

«Субдоговор» и «заключение субдоговора» означает процесс, когда Стороны договариваются с третьей стороной о выполнении обязательств в соответствии с настоящим Договором, а «субконтрактор» означает сторону, с которой заключен «субдоговор»;

«Технические и организационные меры обеспечения безопасности» означают меры, предпринимаемые для обеспечения безопасности персональных данных от случайного или незаконного уничтожения, или случайной утраты, неавторизованной модификации, неправомерного раскрытия или доступа, а также от всех иных незаконных форм обработки.

РАЗДЕЛ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

1. Обязанности, связанные с безопасностью

1.1. Обработчик обязан совершать какие-либо свои действия в отношении персональных данных, которые он обрабатывает от имени Оператора, исключительно в соответствии с указаниями Оператора.

1.2. Обработчик обязан принимать надлежащие технические и организационные меры по обеспечению безопасности ПДн в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

2. Конфиденциальность

2.1. Обработчик соглашается с тем, что он обязан обрабатывать персональные данные от имени Оператора, соблюдая конфиденциальность обработки. В частности, Обработчик соглашается с тем, что, если он не получил письменного согласия от Оператора, он не будет раскрывать персональные данные, переданные Обработчику Оператором/для Оператора/от имени Оператора третьим лицам.

2.2. Обработчик не должен использовать персональные данные, переданные ему Оператором, кроме как в соответствии с существом услуг, оказываемых им Оператору.

3. Заключение «субдоговора»

3.1. Обработчик не должен заключать «субдоговор» по исполнению своих обязательств, налагаемых настоящим Договором, без предварительного письменного согласия Оператора.

3.2. В том случае, если Обработчик с согласия Оператора заключает «субдоговор», он обязан заключать этот договор в письменной форме, а сам договор должен содержать все те обязательства в отношении безопасности обработки, которые накладываются на Обработчика в соответствии с настоящим Договором.

3.3. Если «субконтрактор» не в состоянии выполнять свои обязательства, вытекающие из «субдоговора», Обработчик несет полную ответственность перед Оператором за выполнение обязательств, накладываемых на него настоящим Договором.

4. Порядок действий с персональными данными после прекращения действия Договора

В течение [] дней со дня окончания действия настоящего Договора Обработчик обязан по указанию Оператора:

– вернуть все персональные данные, переданные для обработки Обработчику Оператором, или

– по указанию Оператора уничтожить все персональные данные, если это не запрещено законодательством, или

– выполнить все дополнительные соглашения между Сторонами в части возвращения или уничтожения данных.