АДМИНИСТРАЦИЯ
КРАСНИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ЛИПЕЦКОЙ ОБЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

П О С Т А Н О В Л Е Н И Е

28.11.2013 с.Красное № 688

Об организации защиты персональных данных

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и в целях приведения в соответствие с действующим законодательством порядка обработки персональных данных администрация района **п о с т а н о в л я е т:**

1. Утвердить:

1.1. Перечень персональных данных, обрабатываемых в администрации района (Приложение 1);

1.2. Перечень исходных персональных данных, необходимых для проведения работы с личными делами и ведения бухгалтерского учета (Приложение 2);

1.3. Перечень сведений конфиденциального характера и места их хранения (Приложение 3);

1.4. Перечень защищаемых ресурсов информационных систем персональных данных (Приложение 4);

1.5. Список сотрудников, обслуживающих информационную систему персональных данных (Приложение 5).

2. Назначить ответственными:

2.1. за организацию работ по защите персональных данных, в т.ч. при обработке в информационных системах персональных данных заместителя главы администрации района М.И.Конаныхина;

2.2. за обработку персональных данных:

- Богрянцеву Т.И., начальника отдела организационно-кадровой и правовой работы;
- Бочарову В.В., начальника отдела бухгалтерского учета;
- Поняеву Е.А., начальника отдела опеки и попечительства;
- Бобровицкую М.В., старшего специалиста 1 разряда отдела опеки и попечительства.

3. Назначить Ульмасова М.А., старшего программиста администратором сети, администратором безопасности.

4. Ответственным за обработку персональных данных использовать в работе формы документов согласно утвержденным образцам:

4.1. Соглашение о неразглашении персональных данных субъекта (Приложение 6);

4.2. Заявление – согласие субъекта на обработку его персональных данных (Приложение 7);

4.3. Заявление – согласие субъекта на обработку персональных данных подопечного (Приложение 8);

4.4. Заявление – согласие опекуна на обработку своих персональных данных (Приложение 9);

4.5. Заявление – согласие субъекта на получение его персональных данных у третьей стороны (Приложение 10);

4.6. Заявление – согласие субъекта на передачу его персональных данных третьей стороне (Приложение 11);

4.7. Заявление о прекращении обработки персональных данных (Приложение 12);

4.8. Акт уничтожения персональных данных по достижении цели обработки (Приложение 13);

4.10. Акт уничтожения съемных носителей персональных данных (Приложение 14);

4.11. Журнал учета съемных носителей персональных данных (Приложение 15).

5. Создать комиссию по классификации ИСПДн в следующем составе:

Конаныхин М.И. - заместитель главы администрации района, председатель комиссии;

Члены комиссии:

Богрянцева Т.И. - начальник отдела организационно-кадровой и правовой работы;

Ульмасов М.А. - старший программист.

6.Отделу организационно-кадровой и правовой работы (Т.И.Богрянцева) настоящее постановление довести до сведения работников, осуществляющих обработку персональных данных под роспись.

7. Считать утратившими силу пункты 1-3 распоряжения администрации района от 19.06.2012 года № 85-ра «О мерах по реализации Федерального закона № 152-ФЗ «О персональных данных».

8. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации района М.И.Конаныхина.

Глава района А. В. Филимонов

Богрянцева Татьяна Ивановна
20555

Приложение 1
к постановлению администрации
от 28.11.13 № 688

Перечень
персональных данных, обрабатываемых
в администрации района

№ п/п	Содержание сведений	Срок хранения, условия прекращения обработки
1	2	3
Персональные данные 1 категории:		
1.	Данные об опекунах и опекаемых детях и недееспособных граждан, включая их личные дела и иные сведения (в целях оформления документов для установления опеки (попечительства)	75 лет ЭПК
2.	Данные об усыновителях и усыновленных детях, включая их личные дела и иные сведения (в целях оформления документов на усыновление)	75 лет ЭПК
Персональные данные 2 категории:		
3.	Анкетные данные сотрудников и граждан, обратившихся для трудоустройства, включая личные дела и иные сведения (в целях формирования и учета кадров)	75 лет ЭПК
4.	Анкетные данные сотрудников и граждан, обратившихся для участия в конкурсных процедурах по формированию кадрового резерва или замещения вакантной должности (в целях формирования кадрового резерва или назначения на должность)	на период действия кадрового резерва (3 года), или отзыва согласия субъекта ПД (не прошедшего конкурсные процедуры)
5.	Анкетные данные руководителей, включая личные дела и иные сведения (в целях формирования и учета кадров)	75 лет ЭПК
6.	Данные о несовершеннолетних детях в отношении которых принимаются решения о замене их фамилий и имен, включая их дела (в целях оформления документов на замены фамилий и имен)	75 лет ЭПК
7.	Ответы на обращения граждан, депутатов и организаций, содержащие персональные данные	5 лет ЭПК

	граждан (в целях подготовки и направления ответов)	
8.	Данные о доходах работников (в целях бухгалтерского учета заработной платы и премий и подготовки сведений в Пенсионный фонд Российской Федерации, осуществления кадровой работы)	75 лет ЭПК
Персональные данные 3 категории:		
9.	Идентификационные данные граждан для ответов на их обращения (в целях идентификации при рассмотрении повторных обращений граждан и отправке ответов почтовой связью)	5 лет
10.	Контактные данные работников для трудоустройства или участия в конкурсах (в целях идентификации в деятельности управления труда)	до минования служебной необходимости

Приложение 2
к постановлению администрации
от 28.11. 2013 № 688

Перечень
исходных персональных данных, необходимых для проведения работы с личными делами и ведения бухгалтерского учета

1. Фамилия, имя, отчество
2. Пол
3. Дата рождения
4. Место рождения
5. Адрес места жительства
6. Семейное положение
7. Сведения о месте работы или учебы членов семьи и родственников
8. Социальное положение
9. Имущественное положение
10. Сведения о доходах, информации о выплатах и удержаниях
11. Сведения об образовании
12. Профессия
13. Сведения о документах, удостоверяющих личность
14. Реквизиты ИНН
15. Реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС)
16. Реквизиты полиса обязательного медицинского страхования
17. Сведения о трудовой деятельности, в том числе о стаже работы
18. Сведения о социальных льготах
19. Сведения о воинском учете
20. Контактные телефоны (домашний, мобильный)
21. Сведения о квалификационном разряде, званиях и чинах
22. Общие сведения о состоянии здоровья
23. Фотография

Приложение 3
к постановлению администрации
от 28.11. 2013 № 688

Перечень
сведений конфиденциального характера

№ п/п	Наименование сведений	Типы документов, места хранения, классификация сведений
1.	Личные дела сотрудников	На бумажном носителе документы хранятся в кабинете № 35, металлический шкаф (инв. № 10616100) Персональные данные категории 2 (Доступ ограничен)
2.	Карточка – справка (согласно инструкции по бюджетному учету, утвержденному приказом Минфина России)	На бумажном носителе документы хранятся в кабинете № 15, металлический шкаф Персональные данные категории 2 (Доступ ограничен)
3.	Личные дела детей у которых заменены фамилия и имя	На бумажном носителе документы хранятся в кабинете № 5, металлический шкаф (инв. №10616455) Персональные данные категории 2 (доступ ограничен)
4.	Личные дела опекунов и опекаемых детей и недееспособных граждан, а так же усыновителей и усыновленных детей.	На бумажном носителе документы хранятся в кабинете № 5, металлический шкаф (инв. № 10616455) Персональные данные категории 1 (доступ ограничен)

Приложение 4
к постановлению администрации
от 28.11. 2013 № 688

Перечень защищаемых ресурсов информационных систем персональных данных

1. Файлы с конфиденциальной информацией на жестком магнитном диске в составе персонального компьютера (инв. № 104141263), содержащие персональные данные, кабинет № 35 *(отдел организационно-кадровой и правовой работы);*

2. Файлы с конфиденциальной информацией на жестком магнитном диске в составе персонального компьютера (инв. № 01360775), содержащие персональные данные, кабинет № 15 *(отдел бухгалтерского учета);*

3. Файлы с конфиденциальной информацией на жестких магнитных дисках в составе персональных компьютеров (инв.№№ 10414469, 10414465), содержащие персональные данные, кабинет № 5 *(отдел опеки и попечительства)*

Приложение 5
к постановлению администрации
от 28.11.2013 № 688

СПИСОК
сотрудников, обслуживающих информационную систему персональных данных

№ п/п	Должность	Фамилия, имя, отчество
1.	Начальник отдела организационно-кадровой и правовой работы	Богрянцева Татьяна Ивановна
2.	Начальник отдела бухгалтерского учета	Бочарова Валентина Васильевна
3.	Начальник отдела опеки и попечительства	Поняева Елена Андреевна
4.	Старший специалист 1 разряда отдела опеки и попечительства	Бредихина Татьяна Ивановна
5.	Старший специалист 1 разряда отдела опеки и попечительства	Бобровицкая Маргарита Викторовна

Приложение 6
к постановлению администрации
от 28.11.2013 № 688

Соглашение о неразглашении персональных данных субъекта

Я, _____, паспорт _____, выданный _____ «____» _____ _____, понимаю, что получаю доступ к персональным данным работников и/или других субъектов персональных данных (ПДн), в порядке работы в администрации.

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;

- копии отчетов, направляемые в органы статистики.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных, или их утраты я несу ответственность в соответствии с действующим законодательством. Ответственность: административная, уголовная, гражданская, дисциплинарная.

« ___ » _____ 20__ г. _____

Приложение 7
к постановлению администрации
от 28.11. 2013 № 688

Главе района
_____

Заявление – согласие гражданина (субъекта)
на обработку своих персональных данных (ПД)

Я, _____, проживающий (ая) по адресу: _____: паспорт _____, выдан _____ _____, в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» подтверждаю свое согласие на обработку администрацией района (далее – Оператор) моих персональных данных, включающих следующие данные:

- фамилия, имя, отчество,
- пол,
- дата рождения,
- место рождения,
- адрес места жительства,
- семейное положение,
- сведения о месте работы или учебы членов семьи и родственников,
- социальное положение,
- имущественное положение,
- сведения о доходах, информации о выплатах и удержаниях,
- образование,
- профессия,
- сведения о документах, удостоверяющих личность,
- реквизиты ИНН,
- реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС),
- реквизиты полиса обязательного медицинского страхования,
- сведения о трудовой деятельности, в том числе о стаже работы,
- сведения о социальных льготах,
- сведения о воинском учете,
- контактные телефоны (домашний, мобильный),
- сведения о званиях и чинах,
- общие сведения о состоянии здоровья,
- фотография.

в целях ведения моего личного дела и бухгалтерского ведения моего лицевого счета при условии, что их обработка осуществляется уполномоченными лицами, обязанными сохранять режим секретности (конфиденциальности).

Все перечисленные выше персональные данные предоставляются мною Оператору лично.

Оператор вправе обрабатывать мои персональные данные любым способом. Обрабатывать персональные данные с использованием средств автоматизации, а

так же без таковых. Оператор вправе осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Я утверждаю, что ознакомлен (а) с документами администрации района, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Срок хранения моих персональных данных соответствует сроку хранения материалов личного дела и лицевых счетов.

Я подтверждаю своё согласие на передачу моих персональных данных:

- администрация области (фамилия, имя, отчество, дата и место рождения, должность, информация о классных чинах, образование, повышение квалификации и профессиональная переподготовка, сведения о награждении и поощрении, присвоении почетных званий, дата поступления на работу, стаж, прохождение аттестации, имущественное положение, участие в выборных органах, трудовая деятельность, денежное содержание, данные о включении в кадровый резерв, паспортные данные);

-Пенсионный фонд Российской Федерации (фамилия, имя, отчество, дата и место рождения, должность, дата поступления на работу, стаж, трудовая деятельность, сведения о доходах, адрес места жительства, паспортные данные, СНИЛС);

- Управление Федерального казначейства (фамилия, имя, отчество, лицевой счет, открытый в банке, сумма перечисленных средств);

-ОАО «Сбербанк России» (фамилия, имя, отчество, паспортные данные, адрес места жительства, дата и место рождения, лицевой счет, сумма перечисленных средств);

- налоговая служба (фамилия, имя, отчество, дата рождения, паспортные данные, адрес места жительства, сведения о доходах и налогах);

-страховые медицинские организации (фамилия, имя, отчество, дата рождения, паспортные данные, СНИЛС, адрес по месту регистрации);

- размещение на сайте администрации района (сведения о доходах, имуществе).

Передача моих персональных данных другим субъектам может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной и действует бессрочно.

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.

Подпись гражданина
(субъекта) _____ (ФИО)

«_____» _____ _____ г.

Приложение 8
к постановлению администрации
от 28.11. 2013 № 688

Главе района
_____

Заявление – согласие
субъекта на обработку персональных данных подопечного

Я, _____, паспорт номер _____, выданный _____ "___"_____ _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие отделу опеки и попечительства администрации района расположенному по адресу: село Красное, ул. Первомайская, д. 7, на обработку персональных данных моего/ей сына (дочери, подопечного)

_____
(Ф.И.О. сына, дочери, подопечного)

а именно: (фамилия, имя, отчество, данные свидетельства о рождении ребенка, паспортные данные ребенка старше 14 лет, дата и место рождения, данные свидетельства о браке родителей ребенка или свидетельства об установлении отцовства, образование, денежное содержание, сведения о состоянии здоровья, сведения о смерти родителей или об отсутствии родительского попечения, фото, сведения о регистрации по месту жительства ребенка, сведения об имущественном положении ребенка, сведения о медицинском полис, данные страхового свидетельства

_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес...)

для обработки в целях оформления документов на опеку (попечительство), усыновление

(указать цели обработки)

Я сообщаю, что ознакомлен с документами, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___"_____ 20____ г. _____
(подпись)

Приложение 9
к постановлению администрации
от 28.11. 2013 № 688

Главе района

_____

Заявление – согласие
опекуна на обработку своих персональных данных (ПД)

Я, _____, паспорт номер _____, выданный _____ "___" _____ _____ года, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие отделу опеки и попечительства администрации района, расположенному по адресу: село Красное, ул. Первомайская, д.7, на обработку моих персональных данных

а именно:

- фамилия, имя, отчество, пол, дата рождения, место рождения, адрес места жительства, семейное положение, сведения о месте работы и занимаемой должности, сведения о доходах, социальное положение, имущественное положение, характеризующие данные с места работы и с места жительства, сведения о судимости, фото, сведения о регистрации по месту жительства, сведения об образовании, данные паспорта, реквизиты ИНН, реквизиты страхового номера Индивидуального лицевого счета в Пенсионном фонде Российской Федерации (СНИЛС), общие сведения о состоянии здоровья, данные свидетельства о браке, сведения финансового лицевого счета открытого по месту жительства, сведения об отсутствии долгов за коммунальные услуги, сведения из Роспотребнадзора.

_____

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес...)

Я сообщаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

"___"_____ 20____ г. _____

(подпись)

Приложение 10
к постановлению администрации
от 28.11. 2013 № 688

Главе района
_____

Заявление – согласие
субъекта на получение его персональных данных у третьей стороны

Я, _____, паспорт номер _____, выданный _____ "___" _____ ____ года, в соответствии со статьей 86 Трудового кодекса Российской Федерации _____ на получение моих
(согласен/не согласен)
персональных данных, а именно:
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес)
для обработки в целях _____
_____
_____
(указать цели обработки)
у следующих лиц _____
_____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

"___"_____ 20____ г. _____
(подпись)

Приложение 11
к постановлению администрации
от 28.11 2013 № 688

Главе района

_____

Заявление – согласие
субъекта на передачу его персональных данных третьей стороне

Я, _____, паспорт _____, выданный _____ "___"_____ _____ года, в соответствии со статьей 86 Трудового кодекса Российской Федерации _____
(согласен/не согласен)
на передачу моих персональных данных, а именно:

_____
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес...)
для обработки в целях _____
_____
_____
(указать цели обработки)
следующим лицам _____
_____
_____
(указать Ф.И.О, физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их передачу.

"___"_____ 20____ г. _____
(подпись)

Приложение 12
к постановлению администрации
от 28.11 2013 № 688

Главе района

_____

_____
(Ф.И.О. субъекта персональных данных)

_____
(адрес, где зарегистрирован субъект ПД)

_____
(номер документа, удостоверяющего личность)

_____
(дата выдачи указанного документа)

_____
(наименование органа, выдавшего документ)

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с

_____
_____
_____
_____
(указать причину)

"___"_____ 20____ г. _____
(подпись)

1.3. В своей деятельности Ответственный руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных (указанных в п. 2.1.) и обеспечивает их выполнение.

1.4. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в администрации Краснинского муниципального района (далее – администрация района).

1. Задачи и функции Ответственного

2.1. Основными задачами Ответственного являются:

- разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн;
- доведение до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- осуществление внутреннего контроля за соблюдением требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн;
- организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;
- заполнение и отправка уведомления об обработке (о намерении осуществлять обработку) персональных данных;
- контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

2.2.1. Организация допуска пользователей (разработчиков, эксплуатационного персонала) к техническим, программным средствам и информационным ресурсам ИСПДн в соответствии с «Матрицей доступа пользователей к защищаемым персональным данным ИСПДн» на всех стадиях жизненного цикла ИСПДн.

2.2.2. Участие на стадии проектирования (внедрения) ИСПДн, в разработке технологии обработки персональных данных по вопросам:

- организации порядка учета, хранения и обращения с документами и носителями информации;

- подготовка новых инструкций и внесение изменений и дополнений в настоящую Инструкцию, определяющих задачи, функции, ответственность, права и обязанности администраторов и пользователей ИСПДн по вопросам защиты персональных данных, а также ответственных по защите персональных данных в процессе их автоматизированной обработки.

2.2.3. Контроль выполнения требований действующих нормативных документов по вопросам защиты информации при обработке персональных данных в ИСПДн.

2.2.4. Оперативный контроль за ходом технологического процесса обработки персональных данных.

2.2.5. Методическое руководство работой пользователей ИСПДн в вопросах обеспечения информационной безопасности.

2. Обязанности Ответственного

3.1. Для реализации поставленных задач и возложенных функций Ответственный обязан:

3.1.1. Разработать и вести:

– Журнал по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн;

– Журнал учета носителей персональных данных;

– Журнал учета передачи персональных данных;

– Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации;

– Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

3.1.2. Разработать перечень ПДн.

3.1.3. Разрабатывать решения по:

– составу рабочей группы в защищаемом сегменте сети, системы доверительных отношений между членами группы;

– определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

– определению списка устройств, логических дисков, каталогов общего пользования на серверах с указанием состава допущенных к ним пользователей и режимом допуска;

– разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, использованию СЗИ при передаче конфиденциальных документов).

3.1.4. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ПЭВМ, на которых ведется обработка ПДн.

3.1.5. Своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ от НСД, установленных на ПЭВМ.

3.1.6. Контролировать обеспечение защиты персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

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

3.1.8. Контролировать эффективность защиты персональных данных:

- Проводить работу по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам ПЭВМ.
- Проводить занятия с администраторами и пользователями ИСПДн по правилам работы на ПЭВМ, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков выявленных при контроле эффективности защиты информации.

3.1.9. Организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования.

3.1.10. Осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

3.1.11. Участвовать в проведении внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

3.2. Ответственному запрещается:

3.2.1. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

3.2.2. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокировке, потери информации и предупреждения пользователей.

3.2.3. Допускать к работе на ПЭВМ и серверах посторонних лиц.

3. Права Ответственного

4.1. Ответственный имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и ПЭВМ пользователей.

4.1.2. Требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности персональных данных в ИСПДн.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности. НСД. утраты, порчи защищаемой информации и технических компонентов ИСПДн.

4.1.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим отчетом первому заместителю главы администрации Липецкой области.

4.2. Лицо. ответственное за организацию обработки ПДн. несет ответственность за:

4.2.1. Реализацию, утвержденных в администрации района. требований документов. регламентирующих порядок обеспечения безопасности персональных данных.

4.2.2. Программно - технические и криптографические средства защиты информации, средства вычислительной техники. информационно - вычислительные комплексы. сети и автоматизированные системы обработки информации. закрепленные за ним руководителем администрации района и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.2.3. Разглашение персональных данных и сведений ограниченного распространения. ставших известными ему по роду работы.

4.2.4. Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

4. Порядок учета, хранения и выдачи носителей ПДн

5.1. Ответственный организует учет. хранение и выдачу носителей ПДн.

5.2. Носителями документированных персональных данных могут быть:

- для традиционных текстовых документов - специальный блокнот с отрывными листами и корешком. выполняющим функцию учета листов. нанесения отметок о целевом их использовании; рабочая тетрадь для больших по объему документов; отдельные пронумерованные листы бумаги. типографские формы и бланки документов;
- для чертежно-графических документов - пронумерованные листы ватмана. кальки. пленки. координатной бумаги и т.п.;
- для машиночитаемых документов - маркированные и пронумерованные магнитные ленты. диски. дискеты. карты и т.п.;

- для фотодокументов - маркированные и пронумерованные кассеты с фотопленкой, фотобумага, микрофиши, слайды, кассеты с микрофотопленкой.

5.3. Основные задачи учета носителей персональных данных:

- закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;
- присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки наличия;
- документирование фактов перемещения носителя между сотрудниками администрации района, закрепление персональной ответственности за его сохранность;
- контроль работы исполнителя над документом и своевременного уничтожения носителя или его частей, потерявших практическое значение и составлению акта об уничтожении носителя персональных данных.

5.4. При учете носителей реализуются следующие требования обеспечения защиты персональных данных:

- формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;
- предупреждение возможности нецелевого использования носителя или его неправильного хранения;
- формирование грифа конфиденциальности будущего документа;
- предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, частей фото-, видео- или магнитной пленки), для чего фиксируются технические характеристики носителя (количество листов, длина ленты, наличие склеек и др.);
- предупреждение технической возможности тайной разборки кассет, пеналов, футляров, конвертов и иных оболочек, содержащих технические носители информации;
- включение носителя в сферу регулярного контроля сохранности и местонахождения.

5.5. Обязательному инвентарному учету и маркировке подлежат магнитные носители персональных данных, для которых любые угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений.

5.6. Этапы оформления и учета носителей персональных данных, выдачи их исполнителям и приема от исполнителей выполняются как в традиционном, так и автоматизированном режимах и включают в себя следующие процедуры:

- первичное оформление носителя, в процессе которого выполняются специализированные операции, позволяющие в дальнейшем контролировать подлинность носителя и сохранность всех его элементов;
- традиционный или автоматизированный учет носителя, при котором документируется факт включения носителя в категорию носителей ограниченного доступа с присвоением ему инвентарного номера;
- окончательное оформление носителя, в процессе которого учетные данные переносятся на носитель и его составные части для их идентификации;
- выдача учтенного, укомплектованного носителя персональных данных исполнителю, закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование;
- выдача исполнителю при необходимости дополнительных учтенных листов, форм и бланков;
- прием от исполнителя носителя информации, в процессе которого проверяются комплектность носителя, наличие оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя;
- ежедневная проверка правильности учета носителей и их наличия.

6. Порядок применения средств организации архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных

6.1. Ответственный осуществляет контроль за процессом архивирования, резервирования и восстановления прикладного программного обеспечения и персональных данных.

6.2. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники, эксплуатируемых в администрации района.

6.3. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения устанавливается с учетом соблюдения следующих требований:

- обязательное хранение всех архивов в защищенном месте;
- частота архивации данных зависит от их важности и частоты их изменения;
- системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;
- данные, которые изменяются очень редко, не имеет смысла архивировать.
- восстановление работоспособности программных средств и информационных

массивов, в случае утери и повреждения.

6.4. Организации архивирования и восстановления прикладного программного обеспечения подлежат следующие файлы и документы:

- все файлы операционной системы и установленных приложений. Архивирование системных файлов должно производиться только после установки новых приложений или обновления самой операционной системы;
- личные профили пользователей;
- папки, содержащие важные документы;
- базы данных;
- другие файлы и папки, представляющие ценность.

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

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

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

6.6. Все критичные помещения администрации района (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

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

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы;
- системы обеспечения отказоустойчивости (кластеризация; технология RAID).

6.9. Резервное копирование и хранение данных должно осуществлять на периодической основе:

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

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

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

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

7. Проведение внутреннего расследования по фактам разглашения персональных данных, нарушения условий функционирования системы обработки и защиты персональных данных

7.1. Основными целями проведения внутреннего расследования являются:

— выявление предпосылок утраты персональных данных в результате нарушения порядка их обработки;

— выявления лиц из числа сотрудников администрации района виновных в утрате персональных данных;

— определение ущерба в результате утраты персональных данных;

— проверка полноты и качества исполнения нормативных документов по работе со средствами защиты персональных данных;

— документальное подтверждение соответствия обработки, хранения и передачи персональных данных нормам и правилам, установленным федеральными правовыми и нормативными актами;

— определение фактического состояния системы защиты персональных данных.

7.2. Работник, по вине которого произошло нарушение, обязан по требованию Ответственного представить объяснения в письменной форме не позднее одного рабочего дня с момента получения соответствующего требования. Ответственный вправе увеличить указанный срок, а также поставить перед работником перечень вопросов, на которые работник обязан ответить.

7.3. В целях внутреннего расследования все работники администрации района, по первому требованию Ответственного, должны предъявить для проверки все числящиеся за ними материалы, содержащие персональные данные, представить устные или письменные объяснения, в том числе об известных им фактах разглашения персональных данных, утраты документов и изделий, содержащих персональные данные.

7.4. В случае давления на работника со стороны других работников или третьих лиц (просьб, угроз, шантажа и др.) по вопросам, связанным с проведением внутреннего расследования, работник обязан сообщить об этом Ответственному.

7.5. Для проведения внутреннего расследования глава района формирует комиссию из опытных и квалифицированных работников в составе не менее трех человек. Председателем комиссии является Ответственный.

7.6. До вынесения решения, членам комиссии запрещается разглашать сведения остальным работникам администрации района о ходе проведения внутреннего расследования и ставших известными им в связи с этим обстоятельствах.

7.7. В процессе проведения внутреннего расследования выясняются:

- перечень разглашенных сведений, составляющих персональные данные;
- причины разглашения персональных данных;
- круг лиц, виновных в разглашении персональных данных;
- размер причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с персональными данными;
- иные обстоятельства.

7.8. По результатам расследования, комиссией составляется акт, с отражением в нем лиц, виновных в разглашении персональных данных, размера причиненного ущерба администрации района, наличии ущерба субъектам персональных данных, а также иных выясненных обстоятельствах.

7.9. На основании акта комиссия выносит решение о:

- применении мер дисциплинарного воздействия к работнику;
- информировании регулятора о факте нарушения;
- информировании правоохранительных органов;
- информировании субъектов персональных данных.

8. Порядок реагирования на аварийную ситуацию

8.1. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

8.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться Ответственным в «Журнале по учету мероприятий по контролю».

8.3. В кратчайшие сроки, не превышающие одного рабочего дня, Ответственный за реагирование предпринимает меры по восстановлению нарушенной работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

8.4. При реагировании на инцидент, важно правильно классифицировать критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 – Незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

Уровень 2 – Авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты.

Уровень 3 – Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к нарушению работоспособности ИСПДн и средств защиты на сутки и более.

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

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

Системы жизнеобеспечения ИСПДн включают:

— пожарные сигнализации и системы пожаротушения;

— системы вентиляции и кондиционирования;

— системы резервного питания.

8.6. Все критичные помещения администрации _____ (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.10. Ответственным должно быть проведено обучение должностных лиц, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

— оказание первой медицинской помощи;

— пожаротушение;

— эвакуация людей;

— защита материальных и информационных ресурсов;

— методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

— выключение оборудования, электричества, водоснабжения, газоснабжения.

8.11. Администратор безопасности должен быть дополнительно обучен методам частичного и полного восстановления работоспособности элементов ИСПДн.

8.12. Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

9. Организация режима безопасности помещений, где осуществляется работа с персональными данными

9.1. Первичный (основной) метод – система контроля и управления доступом в здание организации, включает в себя:

— наличие при входе в здание пункта контрольного пропуска;

— наличие ведомственной службы охраны;

— определение внешнего контролируемого периметра.

9.2. Вторичный (дополнительный) метод – система контроля перемещения лиц в здании и управления доступом в помещения, включает в себя:

— наличие помещений с активным сетевым оборудованием с определенными правами доступа;

— наличие охранной и пожарной сигнализаций в помещениях администрации _____;

— использование кодовых замков и иных технических средств ограничения доступа в помещения;

— использование сейфов, шкафов, а также хранение информации с ПДн на внутренних и внешних носителях.

9.3. Ограничение доступа посторонних лиц в помещения, предназначенные для осуществления профессиональной деятельности, связанной с эксплуатацией ИСПДн, предусматривает следующие:

— Исключение возможности бесконтрольного проникновения в эти помещения посторонних лиц, включая работников других структурных подразделений.

— После окончания рабочего дня двери помещений, в которых эксплуатируется ИСПДн, закрываются на ключ и опечатывается персональным пломбиром. Все помещения имеют разные замки. Дубликаты ключей хранятся в запираемом шкафу у Ответственного. В случае выхода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ.

— Уборка помещения производится в присутствии одного из сотрудников, работающего в этом помещении.

— Доступ работников в помещения подразделения по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.

— Строгое ограничение доступа посторонних лиц к серверам, а также сетевому оборудованию.

— Защита мест хранения носителей (USB flash-накопитель, CD, ГМД) от беспрепятственного доступа посторонних лиц.

10. Приостановление обработки персональных данных

10.1. При выявлении недостоверных персональных данных или неправомерных действий с ними при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных необходимо осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных (приостановки предоставления персональных данных пользователям ИСПДн), с момента такого обращения или получения такого запроса на период проверки.

10.2. В случае подтверждения факта недостоверности персональных данных на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов требуется уточнить персональные данные и снять их блокирование.