

БЕЛГОРОДСКАЯ ОБЛАСТЬ
ЧЕРНЯНСКИЙ РАЙОН



АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА
"ЧЕРНЯНСКИЙ РАЙОН" БЕЛГОРОДСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

п. Чернянка

"12" марта 20 21 г.

№ 156-р

**Об утверждении правил осуществления
внутреннего контроля соответствия обработки
персональных данных требованиям к защите
персональных данных администрации
муниципального района
«Чернянский район» Белгородской области**

В соответствии с пунктом 3.1 решения Комиссии по информационной безопасности Совета при полномочном представителе Президента Российской Федерации в Центральном федеральном округе от 26 июня 2019 года N А50-3165 в целях контроля исполнения части 3 статьи 18.1 Федерального закона от 27 июля 2006 года N 152-ФЗ «О персональных данных», а также выполнения постановления Правительства Российской Федерации от 21 марта 2012 года N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» в администрации муниципального района «Чернянский район» Белгородской области:

1. Утвердить правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных администрации муниципального района «Чернянский район» Белгородской области (приложение 1).

2. Утвердить шаблон протокола проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации муниципального района «Чернянский район» Белгородской области (приложение 2).

3. Утвердить шаблон плана устранения нарушений, выявленных в ходе проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение 3).

4. Контроль за исполнением настоящего распоряжения возложить на руководителя аппарата администрации муниципального района «Чернянский район» Белгородской области Овсянникову Л. Н.

Глава администрации
Чернянского района



Т.П. Круглякова

Приложение 1
к распоряжению администрации
муниципального района
«Чернянский район»
Белгородской области
от «12» марта 2021г.
№ 156 - р

**Правила осуществления внутреннего контроля соответствия обработки
персональных данных требованиям к защите персональных данных
администрации муниципального района «Чернянский район»
Белгородской области**

1 Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными, правовыми актами Российской Федерации.

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты персональных данных и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее - законодательство в сфере персональных данных).

1.3. Целями осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям (далее - внутренний контроль) является:

- оценка выполнения требований по обработке и защите персональных данных, установленных законодательством Российской Федерации;
- выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных.

1.4. Внутренний контроль проводится комиссией, назначаемой в порядке, установленном в органе местного самоуправления области (далее - Комиссия).

1.5. В состав Комиссии входят работники администрации муниципального района «Чернянский район» Белгородской области (далее - администрация Чернянского района) и могут привлекаться внешние эксперты. В проведении внутреннего контроля не могут участвовать работники органа местного самоуправления области, прямо или косвенно заинтересованные в его результатах.

1.6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

1.7. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2 Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Внутренний контроль осуществляется в администрации Чернянского района путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов администрации Чернянского района по обработке и защите персональных данных (далее - проверки).

2.2. Проверки проводятся непосредственно на месте обработки персональных данных путем:

- опроса либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных;
- проверки документов, относящихся к деятельности структурного подразделения в части обработки и (или) защиты персональных данных;
- проведения, при необходимости, инструментальных проверок защищенности информационных систем персональных данных.

2.3. Проверки в администрации Чернянского района разделяются на:

- плановые;
- внеплановые.

2.4. Плановые проверки проводятся не реже двух раз в год в соответствии с Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - План внутреннего контроля). Так же не реже двух раз в год оформляются результаты проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, форма которых утверждается соответствующим распоряжением администрации Чернянского района.

Форма плана внутреннего контроля определяется администрацией Чернянского района самостоятельно. План разрабатывается и утверждается ежегодно.

Перечень мероприятий в ходе внутреннего контроля:

- проверка соответствия указанных в «Перечне персональных данных» ПДн фактически обрабатываемым в администрации Чернянского района;
- проверка соответствия установленных прав доступа к ПДн полномочиям в рамках трудовых обязанностей работников;
- проверка актуальности Перечня должностей работников, замещение которых предусматривает осуществление обработки ПДн;
- проверка актуальности Перечня мест хранения материальных носителей персональных данных;
- проверка подтверждения факта ознакомления работников с локальными актами администрации Чернянского района по обработке и обеспечению безопасности ПДн;
- проверка наличия в поручениях оператора сведений, установленных частью 3 статьи 6 Федерального закона «О персональных данных»;
- проверка наличия законных целей и оснований обработки всех ПДн по всем категориям субъектов ПДн;
- проверка соответствия целей обработки содержанию и объему обрабатываемых ПДн;
- выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения

безопасности ПДн;

- проверка соблюдения сроков хранения и порядка уничтожения носителей ПДн;

- проверка соблюдения процедур и сроков подготовки ответов на обращения субъектов ПДн в соответствии со статьями 20 и 21 Федерального закона от 27 июля 2006 года N152-ФЗ «О персональных данных»;

- проверка наличия и (или) необходимости актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки ПДн;

- проверка соблюдения условий использования средств защиты информации, используемых для обеспечения защиты ПДн, входящих в зону ответственности администрации Чернянского района, предусмотренных эксплуатационной и технической документацией на них;

- проверка функционирования технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности администрации Чернянского района;

- проверка выполнения мер по обеспечению безопасности ПДн при их обработке, определенных в соответствии с установленным уровнем защищенности ПДн при их обработке в ИСПДн, включает:

- проверка регулярности обновления средств антивирусной защиты (актуальности вирусных баз);

- проверка проведения резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн;

- проверка установки обновлений безопасности программного обеспечения, в том числе программного обеспечения средств защиты информации;

- проверка регистрации событий информационной безопасности; о проверка реализации процесса управления конфигурациями ИСПДн и системы защиты ПДн;

- проверка реализации процесса управления доступом к ресурсам ИСПДн;

- проверка правильности эксплуатации средств криптографической защиты информации при их использовании в администрации Чернянского района;

- проверка выполнения организационных и технических мероприятий по обеспечению пропускного режима на территорию в администрации Чернянского района.

Перечень и содержание проверок может корректироваться исходя из специфики деятельности администрации Чернянского района.

2.5. План внутреннего контроля разрабатывается Ответственным за организацию обработки персональных данных, либо по его поручению. Разработанный План внутреннего контроля утверждается распоряжением администрации Чернянского района.

2.6. Количество плановых проверок зависит от:

- результатов проведения предыдущих проверок;
- критичности объекта (структурного подразделения, осуществляющего обработку и (или) защиту персональных данных, или процесса обработки персональных данных), по которому планируется проведение проверки;
- предложений руководства и специалистов структурных подразделений администрации Чернянского района.

2.7. Внеплановые внутренние проверки могут проводиться в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных;
- при существенных изменениях процессов или процедур обработки и защиты персональных данных;
- при выявлении большого числа нарушений требований законодательства в сфере персональных данных или повторяемости одних и тех же нарушений от проверки к проверке;
- по указанию руководства администрации Чернянского района.

2.8. Руководители проверяемых структурных подразделений к началу проведения проверок должны обеспечить:

- доступность необходимых для проведения проверок работников;
- доступность необходимых для проведения проверок материалов;
- доступ к информационным ресурсам, владельцами которых они являются;
- доступ в помещения, имеющие отношения к области проведения проверок.

2.9. Результаты проведения внутреннего контроля фиксируются в протоколе проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Протокол).

2.10. В Протоколе должны быть указаны как минимум:

- основание проверки;
- вид проверки (плановая/внеплановая);
- цель проведения проверки;
- выявленные нарушения.

2.11. Протокол подписывают члены Комиссии, председатель Комиссии.

2.12. По результатам проведения внутреннего контроля Комиссией проводится анализ выявленных нарушений и разрабатывается план устранения выявленных нарушений.

2.13. Результаты проведения внутреннего контроля и план устранения выявленных нарушений доводятся до сведения руководителя администрации Чернянского района для принятия решений о необходимости проведения работ по устранению выявленных недостатков.

В зависимости от специфики администрации Чернянского района результаты проведения проверок и план устранения выявленных нарушений доводиться до сведения лица, ответственного за организацию обработки персональных данных.

План устранения нарушений, выявленных в ходе проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, утверждается главой администрации Чернянского района.

2.14. В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

3. Права Комиссии

3.1. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок сотрудников администрации Чернянского района;
- запрашивать у сотрудников администрации Чернянского района необходимую информацию;
- принимать меры по устранению выявленных нарушений;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере персональных данных.

Приложение 2
к распоряжению администрации
муниципального района
«Чернянский район»
Белгородской области
от «16» марта 2021г.
№ 156-р

Утверждаю
должность руководителя
Ф.И.О.
« » 20 года

ПРОТОКОЛ (шаблон)
проведения внутреннего контроля соответствия обработки персональных
данных требованиям к защите персональных данных в администрации
муниципального района «Чернянский район» Белгородской области

Комиссия, назначенная распоряжением _____ от № _____ в составе:

Председатель:	Ф. И. О.	Должность
Члены комиссии:	Ф. И. О.	Должность
	Ф. И. О.	Должность
	Ф. И. О.	Должность

В рамках проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в _____ рассмотрели следующие вопросы:

№ п/п	Проводимые мероприятия и проверяемые вопросы
1.	Документы, определяющие основания обработки персональных данных в структурном подразделении
2.	Соответствие указанных в «Перечне персональных данных» ПДн фактически обрабатываемым в администрации Чернянского района

3.	Актуальность Перечня должностей работников, замещение которых предусматривает осуществление обработки ПДн
4.	Утверждённые перечни должностных лиц структурных подразделений администрации Чернянского района, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей
5.	Актуальность перечня мест хранения материальных носителей персональных данных
6.	Утверждённые перечни информационных систем персональных данных, эксплуатируемых в структурных подразделениях администрации Чернянского района
7.	Подтверждение факта ознакомления работников с локальными актами администрации Чернянского района по обработке и обеспечению безопасности ПДн
8.	Проверка наличия в поручениях оператора сведений, установленных частью 3 статьи 6 Федерального закона «О персональных данных»
9.	Проверка соответствия целей обработки содержанию и объёму обрабатываемых ПДн
10.	Выборочные проверки уровня знания работниками организационно-распорядительных документов в области обработки и обеспечения безопасности ПДн
11.	Проверка соблюдения сроков хранения и порядка уничтожения носителей ПДн
12.	Проверка наличия и (или) необходимости актуализации уведомления уполномоченного органа по защите прав субъектов персональных данных о начале обработки ПДн
13.	Соответствие установленных прав доступа к ПДн полномочиям в рамках трудовых обязанностей работников
14.	Условия хранения и состояние учёта машинных носителей персональных данных
15.	Соблюдение требований к паролям доступа
16.	Отсутствие неправомерно размещённых персональных данных граждан в закреплённых за структурными подразделениями администрации Чернянского района
17.	Проверка соблюдения условий использования средств защиты информации, используемых для обеспечения защиты ПДн, входящих в зону ответственности администрации Чернянского района, предусмотренных эксплуатационной и технической документацией на них
18.	Проверка функционирования технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности администрации Чернянского района
19.	Проверка выполнения мер по обеспечению безопасности ПДн при их обработке, определённых в соответствии с установленным уровнем защищённости ПДн при их обработке в ИСПДн, включает: <ul style="list-style-type: none"> – проверку регулярности обновления средств антивирусной защиты (актуальности вирусных баз); – проверку проведения резервного копирования программных средств,

	<p>архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн;</p> <ul style="list-style-type: none"> – проверку установки обновлений безопасности программного обеспечения, в том числе программного обеспечения средств защиты информации; – проверку регистрации событий информационной безопасности; – проверку реализации процесса управления конфигурациями ИСПДн и системы защиты ПДн; – проверку реализации процесса управления доступом к ресурсам ИСПДн.
20.	Проверка правильности эксплуатации средств криптографической защиты информации при их использовании в администрации Чернянского района (при наличии данных СЗИ)
21.	Проверка выполнения организационных и технических мероприятий по обеспечению пропускного режима на территорию в администрации Чернянского района

Были выявлены следующие несоответствия (нарушения), либо не выявлены нарушения

-
-
-
-
-
-

в количестве _____.

Комиссия решила в целях устранения выявленных нарушений выполнить мероприятия (в зависимости от нарушений) в соответствии с планом устранения недостатков _____.

Комиссия в составе:

Председатель:

Должность

подпись

Ф. И. О.

Члены комиссии:

Должность

подпись

Ф. И. О.

Должность

подпись

Ф. И. О.

Должность

подпись

Ф. И. О.

Приложение 3
к распоряжению администрации
муниципального района
«Чернянский район»
Белгородской области
от «12» марта 2021г.
№ 156 - р

Утверждаю
должность руководителя

Ф.И.О.
«__» _____ 20__ года

План
устранения нарушений, выявленных в ходе проведения внутреннего
контроля соответствия обработки персональных данных требованиям к
защите персональных данных

№ п/п	Недостаток	Решение	Ответственный	Срок	Примечание
1.	Отсутствует ответственный за обработку персональных данных из числа руководителей	Назначить ответственного за организацию обработки персональных данных и соблюдение требований информационной безопасности из числа руководителей	Ф. И. О.	месяц, год	
2.					
3.					
4.					