

**ПРАВИЛА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ  
Государственного бюджетного учреждения «Ингушский научно-  
исследовательский институт гуманитарных наук им. Ч.Э. Ахриева»**

**ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ**

1. Настоящие Правила регулируют отношения, связанные с обработкой персональных данных при осуществлении Государственным бюджетным учреждением «Ингушский научно-исследовательский институт гуманитарных наук им. Ч.Э. Ахриева» (далее - БУ «ИнгНИИ») кадровой работы, а также реализации возложенных на него полномочий с установлением мер, необходимых для обеспечения и выполнения обязанностей государственного органа, как оператора, предусмотренных Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных") и принятыми в соответствии с ним нормативными правовыми актами, в том числе: определяют политику государственного органа в отношении обработки персональных данных, устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований.

2. Настоящие Правила разработаны в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом "О персональных данных", другими федеральными законами, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687, Перечнем 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, утвержденными постановлением Правительства Российской Федерации от 21 марта 2012 года N 211, Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от

1 ноября 2012 года N 1119, составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года N 21, иными нормативными правовыми актами Российской Федерации, законами Республики Ингушетия и иными нормативными правовыми актами Республики Ингушетия.

3. Обработка персональных данных в государственном органе представляет собой действие (операцию) или совокупность действий (операций), совершаемых с Страница 2 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), блокирование, удаление, уничтожение персональных данных.

4. Обработка персональных данных осуществляется в соответствии с принципами и условиями обработки персональных данных, предусмотренными Федеральным законом "О персональных данных", Федеральным законом от 27 июля 2004 года N 79-ФЗ "О государственной гражданской службе Российской Федерации", Трудовым кодексом Российской Федерации, иными нормативными правовыми актами, изданными на основании и во исполнение указанных законов, а также с учетом особенностей, установленных Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 года N 687.

5. В случаях, предусмотренных законодательством Российской Федерации, обработка персональных данных осуществляется при наличии: 1) письменного согласия субъекта персональных данных на обработку его персональных данных в соответствии с типовой формой согласия на обработку персональных данных (Приложение 1 к настоящим Правилам); 2) письменного согласия субъекта персональных данных на получение его персональных данных у третьей стороны в соответствии с типовой формой согласия на получение персональных данных у третьей стороны (Приложение 2 к настоящим Правилам); 3) письменного согласия субъекта персональных данных на предоставление доступа к его персональным данным неограниченному кругу лиц в соответствии с типовой формой согласия на предоставление доступа к персональным данным неограниченному кругу лиц (Приложение 3 к настоящим Правилам); 4) письменного уведомления субъекта персональных данных об осуществлении обработки его персональных данных государственным органом в соответствии с типовой формой уведомления об осуществлении обработки персональных данных государственным органом (Приложение 4 к настоящим Правилам).

6. В случаях отказа субъекта персональных данных предоставить для обработки в государственном органе персональные данные, предоставление

которых обязательно в соответствии с Федеральным законом, указанному субъекту персональных данных разъясняются юридические последствия отказа предоставить свои персональные данные в соответствии с типовой формой разъяснения субъекту персональных данных юридических последствий отказа предоставить персональные данные (Приложение 5 к настоящим Правилам).

## **ГЛАВА 2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ ОРГАНЕ, СОДЕРЖАНИЕ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ, ПЕРСОНАЛЬНЫЕ ДАННЫЕ КОТОРЫХ ОБРАБАТЫВАЮТСЯ, СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ ОРГАНЕ**

7. Целями обработки персональных данных в государственном органе являются:

- 1) осуществление кадровой работы в государственном органе;
- 2) реализация возложенных на государственный орган полномочий, в соответствии с Страница 3 законодательством.

8. В целях осуществления кадровой работы в государственном органе осуществляется обработка персональных данных следующих категорий субъектов:

- 1) лиц, в отношении которых государственный орган осуществляет кадровую работу, а также лиц, претендующих на замещение вакантных должностей государственной гражданской службы Республики Ингушетия в Государственном бюджетном учреждении «Ингушский научно-исследовательский институт гуманитарных наук им. Ч. Э. Ахриева» (далее – ГБУ «ИнгНИИ»), иных вакантных должностей в ГБУ «ИнгНИИ»;

- 2) членов семьи лиц, предусмотренных подпунктом 1 настоящего пункта, а также в случаях, предусмотренных законодательством Российской Федерации, - их близких родственников (в том числе бывших) и свойственников.

9. В целях реализации государственным органом полномочий в соответствии с законодательством осуществляется обработка персональных данных следующих категорий субъектов:

- 1) граждан, обратившихся в государственный орган с обращением независимо от формы подачи обращения;

- 2) граждан, представляющих в отношениях с государственным органом гражданина, организацию, в том числе должностных лиц, представляющих органы государственной власти, иные государственные органы, органы местного самоуправления, муниципальные органы;

- 3) иных граждан.

10. Содержание обрабатываемых персональных данных субъектов, указанных в пунктах 9 и 10 настоящих Правил, определяется в соответствии с законодательством Российской Федерации перечнями персональных данных, утвержденным приказом руководителя ГБУ «ИнгНИИ». Указанными

перечнями также могут уточняться категории субъектов персональных данных, предусмотренные пунктами 9 и 10 настоящих Правил.

11. Срок обработки персональных данных, в том числе и срок их хранения, соответствуют сроку хранения документов, содержащих соответствующие персональные данные, определяемые в соответствии с:

1) приказом Росархива от 20 декабря 2019 года N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения";

2) номенклатурой дел, утвержденной приказом руководителя ГБУ "Ингушетия";

12. В случаях, когда персональные данные, обрабатываемые государственным органом, содержатся в документах, срок обработки которых не может быть определен в соответствии с документами, указанными в пункте 11 настоящих Правил, обработка указанных персональных данных в государственном органе, в том числе их хранение, осуществляется в течение срока, необходимого до достижения целей обработки, или до утраты необходимости в достижении этих целей.

### **ГЛАВА 3. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ ОРГАНЕ**

13. Должностным лицом, ответственным за организацию обработки персональных данных в государственном органе является отдел кадров.

14. Отдел кадров принимает меры, направленные на предотвращение и выявление, Страница 4 нарушений законодательства Российской Федерации в сфере персональных данных, в пределах своих полномочий.

15. Персональные данные обрабатываются лицами, замещающими должности, включенные в перечень (перечни) должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, утвержденный (утвержденные) приказом Руководителя ГБУ «ИнгНИИ» (далее - уполномоченные должностные лица).

16. Уполномоченное должностное лицо знакомится с настоящими Правилами под роспись и дает письменное обязательство о неразглашении персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в соответствии с типовым обязательством о неразглашении персональных данных, ставших известными в связи с исполнением должностных обязанностей (Приложение 6 к настоящим Правилам), а также письменное обязательство прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, в случае расторжения с ним служебного контракта, трудового договора в соответствии с типовым обязательством прекратить обработку персональных данных, ставших известными в связи с исполнением должностных обязанностей (Приложение 7 к настоящим Правилам).

17. Уполномоченное должностное лицо не допускается к обработке персональных данных в государственном органе, если им не даны письменные обязательства, предусмотренные пунктом 16 настоящих Правил.

18. При увольнении либо временном отсутствии уполномоченного должностного лица, имеющиеся у него документы, содержащие персональные данные, передаются другому уполномоченному должностному лицу.

19. Уполномоченное должностное лицо при обработке персональных данных в государственном органе обязано принимать необходимые правовые, организационные меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, в том числе:

1) незамедлительно сообщать управделами: обо всех известных ему фактах или попытках несанкционированного доступа к персональным данным, обрабатываемым в государственном органе; о попытках третьих лиц получить от него персональные данные, ставшие известными ему в связи с выполнением должностных обязанностей; о фактах утраты личного идентификатора для доступа к информационной системе персональных данных в государственном органе, съемного машинного носителя, содержащего персональные данные, а также иных фактах, которые могут привести к разглашению персональных данных, ставших известными ему в связи с выполнением должностных обязанностей;

2) в случае расторжения служебного контракта, трудового договора до дня прекращения служебных, трудовых отношений с государственным органом сдать съемные машинные носители персональных данных, имеющиеся у него в связи с исполнением должностных обязанностей;

3) в случае расторжения служебного контракта, трудового договора со дня прекращения служебных, трудовых отношений с государственным органом: прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей; Страница 5 не использовать известные ему идентификаторы для доступа в информационную систему персональных данных в государственном органе; уничтожить все документы, содержащие персональные данные, ставшие известными ему в результате исполнения должностных обязанностей, не являющиеся служебными документами, в том числе документы, содержащиеся вне информационной системы персональных данных в государственном органе на его личных машинных носителях.

20. Уполномоченному должностному лицу запрещается:

1. разглашать, передавать третьим лицам и распространять персональные данные, которые стали ему известны в связи с выполнением должностных обязанностей;

2. использовать персональные данные, ставшие известными ему в связи с выполнением должностных обязанностей, в личных целях, в том числе с целью получения выгоды;

3. обрабатывать персональные данные в присутствии посторонних лиц;
4. сообщать постороннему лицу свой индивидуальный идентификатор для доступа к информационной системе персональных данных в государственном органе;
5. самостоятельно устанавливать любые системные или прикладные программы при обработке персональных данных в информационной системе персональных данных в государственном органе;
6. отключать (блокировать) программные (аппаратно-программные) средства защиты от несанкционированного доступа к информации и антивирусные средства защиты при обработке персональных данных в информационной системе персональных данных в государственном органе;
7. совершать иные действия, которые могут привести к неправомерному или случайному доступу к персональным данным, а также иным неправомерным действиям с ними.

#### **ГЛАВА 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ГОСУДАРСТВЕННОМ ОРГАНЕ**

21. Обеспечение безопасности персональных данных при их обработке в государственном органе достигается, в частности:

- 1) допуском к обработке персональных данных только уполномоченных должностных лиц;
- 2) ограничением доступа в помещения, в которых осуществляется обработка персональных данных (далее - помещения) лиц, не являющихся уполномоченными должностными лицами;
- 3) обнаружением фактов нарушений законодательства, допущенных при обработке персональных данных в государственном органе, и устранением обнаруженных нарушений;
- 4) обнаружением фактов несанкционированного доступа к персональным данным в государственном органе и принятием мер;
- 5) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

22. Обеспечение безопасности персональных данных при их обработке в информационной системе персональных данных в аппарате помимо мер, предусмотренных пунктом 21 настоящих Правил, достигается в частности:

- 1) определением угроз безопасности персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности Страница 6 персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает уровни защищенности персональных данных;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных в государственном органе;

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

б) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных в государственном органе.

23. Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных в информационных системах персональных данных в государственном органе проводится государственным органом самостоятельно. Указанная оценка проводится не реже одного раза в три года. Решение о проведении оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных в государственном органе принимает управделами.

24. Доступ в помещения разрешается уполномоченным должностным лицам. Иные лица могут находиться в помещении только в присутствии уполномоченных должностных лиц.

25. Рабочие места уполномоченных должностных лиц в помещениях должны располагаться таким образом, чтобы исключалась возможность просмотра информации, содержащейся в документах на бумажных носителях и (или) отображаемой на экране монитора, лицом, не допущенным к обработке соответствующих персональных данных.

26. В отсутствие уполномоченного должностного лица на его рабочем месте не должны находиться документы, содержащие персональные данные, а также на его рабочем месте работа с информационной системой персональных данных в государственном органе должна быть завершена и (или) заблокирована работа операционной системы.

27. Помещения в нерабочее время, а также в рабочее время при отсутствии в них уполномоченных должностных лиц должны быть закрыты на ключ.

28. Допущенные при обработке персональных данных в государственном органе нарушения законодательства в виде неправомерной обработки персональных данных и (или) обработки неточных персональных данных могут быть выявлены:

1. при обращении субъекта персональных данных (его представителя);
2. по запросу субъекта персональных данных (его представителя);
3. по запросу уполномоченного органа по защите прав субъектов персональных данных;
4. по результатам осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям.

29. В случаях выявления неправомерной обработки персональных данных и (или) обработки неточных персональных данных уполномоченными должностными лицами управделами принимает меры, предусмотренные

пунктами 30 - 42 настоящих Правил. В случаях выявления неправомерной обработки персональных данных и (или) Страница 7 обработки неточных персональных данных лицом, которому обработка персональных данных поручена государственным органом, управделами обеспечивает выполнение указанным лицом действий, предусмотренных статьей 21 Федерального закона "О персональных данных".

30. В случаях выявления неправомерной обработки персональных данных и (или) обработки неточных персональных данных уполномоченными должностными лицами управделами принимает решение о проведении проверки фактов указанных нарушений законодательства, решение о блокировании неправомерно обрабатываемых персональных данных, а также, если это не нарушает права и законные интересы субъектов персональных данных и третьих лиц, - решение о блокировании неточных персональных данных. Указанное решение (указанные решения) принимается (принимаются) управделами не позднее рабочего дня, следующего за днем выявления неправомерной обработки персональных данных и (или) обработки неточных персональных данных в государственном органе.

31. При принятии решения о проведении проверки, предусмотренной пунктом 30 настоящих Правил, управделами определяет уполномоченное должностное лицо, которое будет проводить проверку, а также срок проведения проверки, который не может превышать:

1) для проверки фактов неправомерной обработки персональных данных - один рабочий день после дня принятия решения о проведении проверки;

2) для проверки фактов обработки неточных персональных данных - четыре рабочих дня после дня принятия решения о проведении проверки.

32. Решения, предусмотренные пунктом 30 настоящих Правил, доводятся до сведения соответствующих уполномоченных должностных лиц не позднее рабочего дня, следующего за днем выявления неправомерной обработки персональных данных и (или) обработки неточных персональных данных.

33. Уполномоченные должностные лица, осуществляющие обработку персональных данных, в отношении которых принято решение о блокировании, обязаны блокировать эти персональные данные не позднее рабочего дня, следующего за днем выявления неправомерной обработки персональных данных и (или) обработки неточных персональных данных. Блокирование персональных данных осуществляется на период проведения соответствующей проверки.

34. Если при проведении проверки фактов обработки неточных персональных данных уполномоченным должностным лицом будет установлено, что сведений, представленных субъектом персональных данных (его представителем) и (или) уполномоченным органом по защите прав субъектов персональных данных, недостаточно для проверки указанных фактов, уполномоченное должностное лицо делает запрос (запросы) с целью получения информации, подтверждающей или опровергающей факт обработки неточных персональных данных. В этом случае течение срока проверки факта

обработки неточных персональных данных приостанавливается со дня направления соответствующего запроса (соответствующих запросов) до рабочего дня, следующего за днем получения ответа на него (последнего ответа на них).

35. По результатам проведения проверки, предусмотренной пунктом 30 настоящих Правил, уполномоченное должностное лицо составляет акт проверки, содержащий один из следующих выводов:

1) о подтверждении факта неправомерной обработки персональных данных;

Страница 8

2) о неподтверждении факта неправомерной обработки персональных данных;

3) о подтверждении факта обработки неточных персональных данных;

4) о неподтверждении факта обработки неточных персональных данных.

36. В акте проверки, предусмотренном подпунктом 1 пункта 35 настоящих Правил, должны содержаться предложения по обеспечению правомерности обработки соответствующих персональных данных либо сведения об отсутствии возможности обеспечить правомерность обработки соответствующих персональных данных. В акте проверки, предусмотренном подпунктом 3 пункта 35 настоящих Правил, должны содержаться предложения по уточнению соответствующих персональных данных.

37. В случаях установления при проведении проверки, предусмотренной пунктом 30 настоящих Правил, фактов неисполнения или ненадлежащего исполнения уполномоченным должностным лицом по его вине возложенных на него обязанностей, в результате которых персональные данные обрабатывались государственным органом неправомерно и (или) государственным органом обрабатывались неточные персональные данные, акт проверки, предусмотренный подпунктами 1, 3 пункта 35 настоящих Правил, должен содержать предложения по применению мер ответственности к такому уполномоченному должностному лицу.

38. Акт проверки, предусмотренный пунктом 35 настоящих Правил, должен соответствовать требованиям, предусмотренным для актов внеплановых проверок Правилами осуществления внутреннего контроля обработки персональных данных в государственном органе, утвержденными приказом руководителем ГБУ «ИнгНИИ».

39. Уполномоченное должностное лицо представляет управделами акт проверки, предусмотренный пунктом 35 настоящих Правил, не позднее рабочего дня, следующего за днем окончания срока проверки.

40. По результатам рассмотрения акта проверки, предусмотренного пунктом 35 настоящих Правил, управделами принимает одно из следующих решений:

1) об оставлении обработки соответствующих персональных данных без изменения;

2) о прекращении обработки персональных данных, неправомерно обрабатываемых в государственном органе, и об обеспечении правомерности их обработки;

3) об уничтожении персональных данных, неправомерно обрабатываемых в государственном органе;

4) об уточнении неточных персональных данных в государственном органе и снятии блокирования.

41. Решение, предусмотренное пунктом 40 настоящих Правил, принимается управделами не позднее рабочего дня, следующего за днем окончания срока проведения соответствующей проверки.

42. В случае принятия решения, предусмотренного подпунктом 2 пункта 40 настоящих Правил, уполномоченное должностное лицо, проводившее проверку, обеспечивает правомерность обработки соответствующих персональных данных не позднее пяти рабочих дней после дня принятия указанного решения.

43. Если в течение срока, предусмотренного пунктом 42 настоящих Правил, будет выявлено, что обеспечение правомерности обработки персональных данных невозможно, уполномоченное должностное лицо сообщает об этом управделами. В этом случае управделами принимает решение об уничтожении персональных данных, неправомерно обрабатываемых в государственном органе. Указанное решение принимается не позднее рабочего дня, следующего за днем истечения срока, предусмотренного пунктом 42 Страница 9 настоящих Правил.

44. В случае принятия решения, предусмотренного подпунктом 4 пункта 40 настоящих Правил, персональные данные подлежат уточнению не позднее рабочего дня, следующего за днем принятия указанного решения. Уточнение персональных данных, обрабатываемых в государственном органе без использования средств автоматизации, производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными. Уточнение персональных данных, содержащихся в информационной системе персональных данных в государственном органе, осуществляется путем их изменения в соответствующей информационной системе в государственном органе. Блокирование с уточненных персональных данных снимается с момента их уточнения.

45. Уполномоченное должностное лицо уведомляет субъекта персональных данных (его представителя), а в случаях, предусмотренных подпунктом 3 пункта 28 настоящих Правил, - также уполномоченный орган по защите прав субъектов персональных данных, о мерах, принятых им в соответствии с пунктами 40 - 44, 57 - 60 настоящих Правил. Указанное уведомление направляется уполномоченным должностным лицом не позднее трех рабочих дней со дня принятия соответствующих мер.

46. В случаях обнаружения несанкционированного доступа к персональным данным, обрабатываемым в государственном органе без использования средств автоматизации, или попыток такого доступа уполномоченное должностное лицо незамедлительно сообщает об этом управделами.

47. Управделами не позднее рабочего дня, следующего за днем обнаружения обстоятельств, предусмотренных пунктом 46 настоящих Правил, принимает решение о проведении проверки фактов несанкционированного доступа к персональным данным, обрабатываемым в аппарате без использования средств автоматизации (попыток такого доступа).

48. При принятии решения, предусмотренного пунктом 47 настоящих Правил, управделами определяет уполномоченное должностное лицо (уполномоченных должностных лиц), которое будет (которые будут) проводить проверку, а также срок проведения проверки, который не может превышать двадцать рабочих дней.

49. По результатам проведения проверки, предусмотренной пунктом 47 настоящих Правил, уполномоченное должностное лицо составляет (уполномоченные должностные лица составляют) акт проверки, содержащий один из следующих выводов:

1) о неподтверждении факта несанкционированного доступа к персональным данным, обрабатываемым в аппарате без использования средств автоматизации (факта попытки такого доступа);

2) о подтверждении факта попытки несанкционированного доступа к персональным данным, обрабатываемым в государственном органе без использования средств автоматизации;

3) о подтверждении факта несанкционированного доступа к персональным данным, обрабатываемым в государственном органе без использования средств автоматизации.

50. Акт проверки, предусмотренный подпунктами 2, 3 пункта 49 настоящих Правил, должен содержать:

1) предложения по принятию мер, направленных на предотвращение несанкционированного доступа к персональным данным, обрабатываемым в Страница 10 государственном органе без использования средств автоматизации;

2) предложения по применению мер ответственности к уполномоченному должностному лицу - в случаях установления фактов неисполнения или ненадлежащего исполнения таким уполномоченным должностным лицом по его вине возложенных на него обязанностей, в результате которых был совершен несанкционированный доступ к персональным данным, обрабатываемым в государственном органе без использования средств автоматизации (попытка такого доступа).

51. Акт проверки, предусмотренный подпунктом 3 пункта 49 настоящих Правил, также должен содержать:

1) описание действий, совершенных с персональными данными в результате несанкционированного доступа к ним;

2) предложения по восстановлению персональных данных - в случаях их уничтожения или модификации в результате несанкционированного доступа;

3) оценку вреда, который может быть причинен субъектам персональных данных в результате несанкционированного доступа к их персональным данным в государственном органе, соотношение указанного вреда и принимаемых аппаратом мер, направленных на обеспечение безопасности персональных данных при их обработке в государственном органе.

52. Акт проверки, предусмотренный пунктом 49 настоящих Правил, должен соответствовать требованиям, предусмотренным для актов внеплановых проверок Правилами осуществления внутреннего контроля обработки персональных данных в государственном органе, утвержденными приказом руководителя ГБУ «ИнгНИИ».

53. Уполномоченное должностное лицо представляет (уполномоченные должностные лица представляют) управделами акт проверки, предусмотренный пунктом 49 настоящих Правил, не позднее рабочего дня, следующего за днем окончания срока проверки.

54. По результатам рассмотрения акта проверки, предусмотренного пунктом 49 настоящих Правил, управделами не позднее рабочего дня, следующего за днем окончания срока проверки, принимает решение о принятии мер, направленных на устранение последствий несанкционированного доступа к персональным данным, обрабатываемым в аппарате без использования средств автоматизации, и (или) предотвращение несанкционированного доступа к персональным данным, обрабатываемым в аппарате без использования средств автоматизации (попыток такого доступа).

## **ГЛАВА 5. ПОРЯДОК УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ГОСУДАРСТВЕННОМ ОРГАНЕ**

55. Персональные данные, обрабатываемые в государственном органе, подлежат уничтожению:

1) по истечении срока их обработки в государственном органе, в том числе по достижению целей обработки либо в случае утраты необходимости в достижении этих целей;

2) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если без такого согласия обработка персональных данных является неправомерной;

3) в случаях принятия решений об уничтожении персональных данных, предусмотренных подпунктом 3 пункта 40 и пунктом 43 настоящих Правил.

56. Персональные данные подлежат уничтожению в следующие сроки:

Страница 11

1) в случаях, предусмотренных подпунктами 1 и 2 пункта 55 настоящих Правил, - не позднее тридцати календарных дней со дня истечения срока обработки персональных данных в государственном органе (со дня поступления отзыва субъектом персональных данных согласия на обработку его персональных данных);

2) в случае принятия решения, предусмотренного подпунктом 3 пункта 40 настоящих Правил, - не позднее семи рабочих дней со дня принятия указанного решения;

3) в случае принятия решения, предусмотренного пунктом 43 настоящих Правил, - не позднее рабочего дня, следующего за днем принятия указанного решения.

57. В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в пункте 56 настоящих Правил, уполномоченные должностные лица осуществляют блокирование таких персональных данных и обеспечивают их уничтожение в срок не более, чем шесть месяцев, если иной срок не установлен федеральными законами.

58. Уничтожение персональных данных осуществляется уполномоченными должностными лицами, осуществляющими обработку этих персональных данных, и (или) иными уполномоченными должностными лицами, определенными управделами.

59. Уничтожение персональных данных, обрабатываемых в государственном органе без использования средств автоматизации, производится следующими способами:

1) исключая дальнейшую обработку этих персональных данных с сохранением возможности обработки иных персональных данных, зафиксированных на материальном носителе (удаление, вымарывание), - если это допускается материальным носителем;

2) уничтожение материального носителя.

60. Уничтожение персональных данных, содержащихся в информационной системе персональных данных в государственном органе, производится путем их удаления из соответствующей информационной системы в государственном органе. В случаях, когда уничтожение персональных данных, содержащихся в информационной системе персональных данных в аппарате, невозможно без ее модификации, такая модификация обеспечивается в течение срока, указанного в пункте 57 настоящих Правил.