УПРАВЛЕНИЕ ДЕЛАМИ
ГУБЕРНАТОРА И ПРАВИТЕЛЬСТВА АЛТАЙСКОГО КРАЯ

ПРИКАЗ

«13» марта 2018 г. № 44 - ОД

г. Барнаул

О мерах по обеспечению безопасности персональных данных в управлении делами Губернатора и Правительства Алтайского края

В целях соблюдения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» п р и к а з ы в а ю:

1. Назначить ответственным за организацию обработки персональных данных в управлении делами Губернатора и Правительства Алтайского края (далее – управление делами) заместителя управляющего делами Губернатора и Правительства Алтайского края, начальника отдела организационно-планового обеспечения Кочергова Евгения Николаевича.

2. Назначить ответственным за организацию безопасности персональных данных в управлении делами начальника отдела по обслуживанию информационно-коммуникационных систем управления делами Якоба Евгения Юрьевича.

3. Назначить администратором безопасности информационных систем персональных данных в управлении делами консультанта отдела по обслуживанию информационно-коммуникационных систем управления делами Зыкова Максима Александровича.

4. Утвердить Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления делами Губернатора и Правительства Алтайского края.

5. Утвердить правила обработки персональных данных в управлении делами Губернатора и Правительства Алтайского края.

6. Утвердить правила рассмотрения запросов субъектов персональных данных или их представителей в управлении делами Губернатора и Правительства Алтайского края.

7. Утвердить правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении делами Губернатора и Правительства Алтайского края.

8. Утвердить перечень персональных данных, обрабатываемых в управлении делами Губернатора и Правительства Алтайского края в связи с реализацией служебных (трудовых) отношений

9. Утвердить перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

10. Утвердить перечень информационных систем персональных данных управления делами Губернатора и Правительства Алтайского края.

11. Утвердить инструкцию по организации доступа в помещения, в которых ведется обработка персональных данных.

12. Утвердить инструкцию по организации парольной защиты в информационных системах персональных данных.

13. Утвердить инструкцию по организации резервного копирования персональных данных в информационных системах персональных данных.

14. Утвердить инструкцию по организации технического обслуживания и ремонта технических средств в информационных системах персональных данных.

15. Утвердить инструкцию по проведению антивирусного контроля в информационных системах персональных данных.

16. Утвердить инструкцию по работе пользователей в информационных системах персональных данных.

17. Утвердить инструкцию по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных.

18. Утвердить инструкцию по правилам обращения с носителями ключевой информации в информационных системах персональных данных.

19. Утвердить типовую форму согласия на обработку персональных данных в управлении делами Губернатора и Правительства Алтайского края.

20. Утвердить типовую форму согласия на обработку персональных данных в управлении делами Губернатора и Правительства Алтайского края, запрашиваемого при выдаче пропуска на вход в здание Правительства Алтайского края.

21. Утвердить типовое обязательство гражданского служащего управления делами Губернатора и Правительства Алтайского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей.

22. Постоянно действующей комиссии для классификации информационных систем персональных данных и автоматизированных систем провести обследование информационных систем персональных данных.

По результатам работ составить акты установления уровня защищенности информационных систем персональных данных управления делами.

23. Отделу организационно-планового обеспечения управления делами (Кочергов Е.Н.) организовать работу по внесению изменений в должностные регламенты ответственного за организацию обработки персональных данных в управлении делами и лиц, имеющих доступ к персональным данным.

24. Ответственному за организацию обработки персональных данных Кочергову Евгению Николаевичу ознакомить сотрудников управления делами, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами управления делами по вопросам обработки персональных данных.

25. Контроль за исполнением настоящего приказа возложить на заместителя управляющего делами Губернатора и Правительства Алтайского края, начальника отдела организационно-планового обеспечения Кочергова Евгения Николаевича.

26. Признать утратившими силу приказы управления делами Администрации Алтайского края:

от 08.09.2011 № 96-ОД «Об организации работы с персональными данными»;

от 14.11.2011 № 133-ОД «О мерах по обеспечению безопасности персональных данных»;

от 20.08.2012 № 104-ОД «Об утверждении типовых форм по персональным данным»;

от 04.09.2012 № 108-ОД «О мерах по обеспечению безопасности персональных данных»;

от 14.04.2014 № 29-ОД «О мерах по обеспечению безопасности персональных данных»;

от 26.03.2012 № 40-ОД «О мерах по обеспечению безопасности персональных данных»;

от 22.07.2015 № 92-ОД «О мерах по обеспечению безопасности персональных данных».

27. Настоящий приказ подлежит опубликованию на «Официальном интернет – портале правовой информации» (www.pravo.gov.ru).

Заместитель управляющего делами,
начальник отдела организационно-планового обеспечения — Е.Н. Кочергов

УТВЕРЖДЕНО
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-08

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления делами Губернатора и Правительства Алтайского края

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления делами Губернатора и Правительства Алтайского края (далее – «Положение») разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, находящихся на балансе управления делами Губернатора и Правительства Алтайского края (далее - «Оператор персональных данных»).

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается применением правовых, организационных и технических мер по обеспечению безопасности персональных данных (в том числе средств предотвращения несанкционированного доступа). Организационные меры и технические средства защиты информации должны удовлетворять требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

1.4. Требования настоящего Положения являются обязательными для исполнения всеми лицами, получившими доступ к персональным данным.

1.5. Решение о необходимости изменения этого Положения принимается на основании:

результатов проведенных аудитов, мероприятий по контролю и надзору за обеспечением безопасности персональных данных, осуществляемых уполномоченными органами;

изменения нормативных правовых актов и (или) нормативных методических документов Российской Федерации в области защиты персональных данных;

изменения процессов обработки персональных данных в информационных системах (далее - ИС) персональных данных управления делами;

результатов анализа инцидентов информационной безопасности в ИС персональных данных.

Изменения Положения должны быть направлены на предотвращение инцидентов или устранение последствий зарегистрированных инцидентов информационной безопасности.

Все предлагаемые изменения Положения до их ввода в действие подлежат предварительной оценке, на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2. Обработка персональных данных

2.1. Оператор персональных данных осуществляет обработку персональных данных лиц, замещающих должности государственной гражданской службы Алтайского края, и должности, не относящиеся к должностям государственной гражданской службы Алтайского края.

2.2. Обработка персональных данных осуществляется оператором персональных данных в целях реализации возложенных на него функций, определяемых законами и иными нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

2.3. Объем и характер обрабатываемых персональных данных должен соответствовать целям их сбора. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.5. Обработка персональных данных осуществляется оператором без проведения мероприятий по обезличиванию персональных данных.

2.6. Персональные данные оператор получает непосредственно от субъектов персональных данных, которые принимают решение об их предоставлении и дают согласие на их обработку своей волей и в своем интересе.

2.7. Лица, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей, допус-

каются к соответствующим персональным данным на основании перечня должностей служащих, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным.

2.8. Принятые в управлении делами Губернатора и Правительства Алтайского края организационно-распорядительные документы доводятся до сведения лиц, участвующих в обработке персональных данных, в части их касающейся.

2.9. Персональные данные, используемые для обработки в ИС, порядок использования, цель, периодичность и основания внесения изменений и дополнений устанавливаются оператором персональных данных.

2.10. Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев установленных ст.10 Федерального закона.

2.11. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.12. При обработке персональных данных, осуществляемой без использования средств автоматизации, оператор выполняет требования, установленные постановлением Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

3. Обязанности и права оператора персональных данных в информационных системах персональных данных

3.1. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необ-

ходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.2. В случае выявления недостоверных персональных данных или фактов неправомерных действий с ними оператора персональных данных, при обращении или по запросу субъекта персональных данных или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, оператор обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.

3.3. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.4. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.5. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной ко-

торого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

3.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

3.7. Оператор при передаче персональных данных субъектов третьим лицам ограничивает передаваемую информацию только теми персональными данными субъектов, которые необходимы третьим лицам для выполнения своих функций. Передача персональных данных по телефону, факсимильной связи, электронной почте и сети Интернет (без использования средств защиты информации, удовлетворяющих требованиям, установленным нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных) запрещается.

4. Методы и способы защиты персональных данных в информационных системах персональных данных

4.1. С целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных, оператором должны быть установлены уровни защищенности персональных данных ИС.

4.2. В целях обеспечения безопасности персональных данных определяются угрозы безопасности, оценивается актуальность угроз безопасности персональных данных. В результате разрабатывается модель угроз безопасности персональных данных.

Модель угроз безопасности персональных данных корректируется при

изменении состава основных технических средств и условий эксплуатации ИС персональных данных отделом по обслуживанию информационно-коммуникационных систем управления делами.

4.3. Установка, изменение (обновление) и удаление программного обеспечения в ИС персональных данных производится администратором безопасности ИС персональных данных или в его присутствии.

4.4. Доступ лиц к ИС персональных данных, не допущенных к работе с персональными данными, должен быть исключен. ИС персональных данных должны быть защищены аппаратными и (или) программными средствами защиты информации от несанкционированного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Российской Федерации, регулирующими отношения, связанные с обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных.

4.5. Подключение ИС к внешним локальным вычислительным сетям осуществляется с использованием средств защиты информации в соответствии с установленными требованиями нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности информации.

4.6. Охрана помещений, в которых ведется работа с персональными данными, и организация режима безопасности в этих помещениях должна обеспечивать сохранность технических средств и носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Все носители персональных данных должны быть учтены с помощью их маркировки, а их учетные данные занесены в журнал учета с отметкой об их выдаче (приеме).

4.7. В целях обеспечения безопасности персональных данных должны быть разработаны организационно-распорядительные и организационно-методические документы по обеспечению безопасности персональных данных, обрабатываемых в ИС:

перечень информационных систем персональных данных;

перечень персональных данных, обрабатываемых в управлении делами Губернатора и Правительства Алтайского края в связи с реализацией служебных (трудовых) отношений;

перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

инструкция по работе пользователей в ИС персональных данных;

инструкция по организации доступа в помещения, в которых ведется обработка персональных данных;

инструкция по организации резервного копирования персональных данных;

инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения

персональных данных;

инструкция по организации парольной защиты в ИС персональных данных;

инструкция по проведению антивирусного контроля в ИС персональных данных;

инструкция по организации технического обслуживания и ремонта технических средств ИС персональных данных;

инструкция по правилам обращения с носителями ключевой информации в информационных системах персональных данных;

правила рассмотрения запросов субъектов персональных данных или их представителей в управлении делами Губернатора и Правительства Алтайского края;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении делами Губернатора и Правительства Алтайского края;

правила обработки персональных данных в управлении делами Губернатора и Правительства Алтайского края;

другие организационно-распорядительные документы по обеспечению безопасности персональных данных, обрабатываемых в ИС.

4.8. Лица, уполномоченные осуществлять обработку персональных данных, несут ответственность за соблюдение требований по защите персональных данных в порядке, предусмотренном действующим законодательством Российской Федерации.

5. Обязанности и права должностных лиц

5.1. Управляющий делами Губернатора и Правительства Алтайского края:

организует разработку, внедрение, совершенствование и эксплуатацию системы защиты ИС персональных данных, а также организует внутренний контроль за соблюдением нормативных правовых актов Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

обеспечивает реализацию мероприятий по защите персональных данных при их обработке в ИС персональных данных в управлении делами Губернатора и Правительства Алтайского края и Администрации Губернатора и Правительства Алтайского края;

осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИС персональных данных управления делами Губернатора и Правительства Алтайского края и Администрации Губернатора и Правительства Алтайского края;

назначает ответственного за организацию обработки персональных данных;

назначает ответственного за обеспечение безопасности персональных

данных;

назначает администратора безопасности ИС персональных данных.

5.2. Ответственный за организацию обработки персональных данных:

осуществляет внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

доводит до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организует и осуществляет прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

5.3. Ответственный за обеспечение безопасности персональных данных:

несет ответственность за организацию обеспечения безопасности персональных данных при их обработке в ИС персональных данных управления делами Губернатора и Правительства Алтайского края и Администрации Губернатора и Правительства Алтайского края;

обеспечивает выполнение организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных;

организует регистрацию и учет защищаемых носителей информации;

организует расследование причин и условий появления нарушений безопасности ИС персональных данных, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений.

5.4. Администратор безопасности ИС персональных данных:

обеспечивает обнаружение фактов несанкционированного доступа к ИС персональных данных, о которых должен доложить ответственному за обеспечение безопасности персональных данных;

осуществляет установку и ввод в эксплуатацию средств защиты информации ИС персональных данных в соответствии с эксплуатационной и технической документацией;

обеспечивает работы по проведению антивирусного контроля в ИС персональных данных;

выполняет резервное копирование персональных данных;

осуществляет установку (обновление версий) программного обеспечения ИС персональных данных, обеспечивает его функционирование;

осуществляет установку, подключение и настройку технических средств ИС персональных данных в соответствии с технической документацией;

осуществляет установку (развертывание) новых ИС персональных данных или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач.

5.5. Отдел по обслуживанию информационно-коммуникационных си-

стем управления делами Губернатора и Правительства Алтайского края:

осуществляет выполнение мероприятий по защите персональных данных при их обработке в ИС персональных данных;

разрабатывает проекты распорядительных документов по защите персональных данных при их обработке в ИС персональных данных в управлении делами Губернатора и Правительства Алтайского края;

разрабатывает настоящее Положение и вносит в него в установленном порядке изменения;

разрабатывает предложения по дальнейшему совершенствованию системы защиты персональных данных при их обработке в ИС персональных данных;

осуществляет планирование мероприятий по защите персональных данных при их обработке в ИС персональных данных, их выполнение и контроль их эффективности;

подготавливает предложения о привлечении к проведению работ по защите персональных данных при их обработке в ИС персональных данных на договорной основе организаций, имеющих лицензию на соответствующий вид деятельности;

обеспечивает обслуживание и ремонт сетевого оборудования, рабочих станций, серверного и периферийного оборудования в ИС персональных данных.

6. Контроль состояния защиты персональных данных

6.1. Контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИС персональных данных, установленных Правительством Российской Федерации, осуществляется представителями уполномоченного органа по защите прав субъектов персональных данных, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИС персональных данных.

6.2. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных, осуществляется ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных.

7. Заключительные положения

7.1. Настоящее Положение вступает в силу с момента его утверждения.

7.2. Настоящее Положение не заменяет собой действующее законодательство Российской Федерации, регулирующее отношения, связанные с обеспечением безопасности персональных данных при их обработке в ИС персональных данных.

УТВЕРЖДЕНЫ
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-ОД

Правила
обработки персональных данных
в управлении делами Губернатора и Правительства Алтайского края

1. Настоящими Правилами обработки персональных данных в управлении делами Губернатора и Правительства Алтайского края (далее - «Правила») определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; содержание обрабатываемых персональных данных для каждой цели обработки персональных данных; категории субъектов, персональные данные которых обрабатываются; сроки обработки и хранения; порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

2. Управление делами Губернатора и Правительства Алтайского края является оператором персональных данных (далее – «Оператор ПД»).

3. В настоящих Правилах используются следующие основные понятия:

персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

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

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4. Обработка персональных данных в управлении делами Губернатора и Правительства Алтайского края осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации;

5. Управляющий делами Губернатора и Правительства Алтайского назначает лицо, ответственное за организацию обработки персональных данных в управлении делами, и определяет лиц, уполномоченных на обработку персональных данных, обеспечивающих обработку персональных данных в соответствии с требованиями законодательства и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

6. Должностные лица Оператора ПД, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

7. Содержание обрабатываемых персональных данных государственных гражданских служащих и сотрудников Оператора ПД (далее – «сотрудники») определяются нормативными правовыми актами законодательства о государственной гражданской службе и трудового законодательства Российской Федерации.

8. Обработка персональных данных осуществляется с согласия субъекта персональных данных (далее – «Субъект ПД») на обработку его персональных данных. Субъект ПД принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе и в письменной форме. Согласие на обработку персональных данных должно отвечать требованиям, определенным статьей 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

9. При сборе персональных данных уполномоченные должностные лица Оператора ПД обязаны предоставить субъекту ПД по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

10. Если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации, уполномоченные должностные лица Оператора ПД обязаны разъяснить субъекту ПД юридические последствия отказа предоставить его персональные данные.

11. При обработке персональных данных уполномоченные должностные лица обязаны соблюдать следующие требования:

- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации в области персональных данных;

- персональные данные следует получать лично у субъекта персональных данных. В случае получения персональных данных у третьей стороны следует известить об этом субъекта персональных данных заранее, получить

его письменное согласие и сообщить о целях, предполагаемых источниках и способах получения персональных данных;

- запрещается получать, обрабатывать и приобщать к личному делу сотрудника не установленные Федеральными законами от 27.07.2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» персональные данные о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

- передача персональных данных сотрудника третьей стороне не допускается без письменного согласия сотрудника, за исключением случаев, установленных федеральными законами;

- в случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

- в случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

- в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор

в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

- в случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

- в случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими федеральными законами.

- в случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 статьи 21 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персо-

нальных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных (сотрудника), не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

12. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, осуществляется в соответствии со статьей 10 Федерального закона от 27.07.2006 г. № 152- ФЗ «О персональных данных».

Обработка специальных категорий персональных данных должна быть прекращена, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено законодательством Российской Федерации.

13. Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме гражданского служащего, являющегося субъектом персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации о противодействии коррупции, о государственной службе, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию и другими нормативными правовыми актами Российской Федерации.

14. Сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей в соответствии с законодательством о государственной гражданской службе в Российской Федерации размещаются на официальном сайте управления делами Губернатора и Правительства Алтайского края.

15. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

16. Субъект персональных данных имеет право на получение сведений, указанных в статье 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Субъект персональных данных вправе требовать от Оператора ПД уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необхо-

димыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

17. Сведения, указанные в части 7 статье 14 Федерального закона от 27.07.2006 г. № 152- ФЗ «О персональных данных», должны быть предоставлены субъекту персональных данных Оператором ПД в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения, указанные в части 7 статьи 14 Федерального закона от 27.07.2006 г. № 152- ФЗ «О персональных данных», предоставляются субъекту персональных данных или его представителю Оператором ПД при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона от 27.07.2006 г. № 152- ФЗ «О персональных данных», и ознакомления с такими персональными данными осуществляется не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Оператор ПД вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных». Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе ПД.

18. Меры, принимаемые Оператором ПД, 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:

- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учет машинных носителей персональных данных;

- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

- контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

УТВЕРЖДЕНЫ
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-ОД

Правила
рассмотрения запросов субъектов персональных данных или их представителей в управлении делами Губернатора и Правительства Алтайского края

1. Настоящими Правилами рассмотрения запросов субъектов персональных данных или их представителей в управлении делами Губернатора и Правительства Алтайского края (далее - «Правила») определяются порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее - «Запросы»).

2. Управление делами Губернатора и Правительства Алтайского края является оператором персональных данных (далее – «Оператор ПД»).

3. Субъект персональных данных имеет право на получение сведений, указанных в части 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее - «Федеральный закон»), за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона. Субъект персональных данных вправе требовать от Оператора ПД уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4. Сведения, указанные в части 7 статьи 14 Федерального закона, должны быть предоставлены субъекту персональных данных Оператором ПД в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5. Сведения, указанные в части 7 статьи 14 Федерального закона, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором ПД, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного доку-

мента и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6. В случае, если сведения, указанные в части 7 статьи 14 Федерального закона, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору ПД или направить ему повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. Запрос прочитывается, проверяется на повторность, сверяется с находящейся в архиве предыдущей перепиской.

7. Субъект персональных данных вправе обратиться повторно к Оператору ПД или направить ему повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 статьи 14 Федерального закона, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 статьи 14 Федерального закона, должен содержать обоснование направления повторного запроса.

8. Оператор ПД вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе ПД.

9. Оператор ПД обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

10. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Оператор ПД обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основани-

ем для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

11. Оператор ПД обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор ПД обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор ПД обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

12. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Оператор ПД обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Оператор ПД обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

13. В случае подтверждения факта неточности персональных данных Оператор ПД на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

14. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором ПД или лицом, действующим по поручению Оператора ПД, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора ПД. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор ПД в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор ПД обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

15. В случае достижения цели обработки персональных данных Оператор ПД обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором ПД и субъектом персональных данных либо если Оператор ПД не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

16. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор ПД обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором ПД и субъектом персональных данных либо если Оператор ПД не вправе осуществлять обработку персональных данных без согласия субъекта персональных дан-

ных на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

17. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 статьи 21 Федерального закона, Оператор ПД осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора ПД) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

18. Ответственный за организацию обработки персональных данных в управлении делами Администрации Алтайского края организует прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приемом и обработкой таких обращений и запросов.

19. Все запросы регистрируются в Журнале учёта обращений субъектов персональных данных о выполнении их законных прав.

20. Рассмотрение запросов осуществляется уполномоченными должностными лицами Оператора ПД, в чьи обязанности входит обработка персональных данных.

21. Ведение делопроизводства по запросам осуществляется специально назначенным сотрудником управления делами Губернатора и Правительства Алтайского края под контролем ответственного за организацию обработки персональных данных.

22. Должностные лица Оператора ПД обеспечивают:

- объективное, всестороннее и своевременное рассмотрения запроса;

- принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов персональных данных;

- направление письменных ответов по существу запроса.

23. Должностные лица при рассмотрении запроса обязаны:

- разобраться в их существе, истребовать дополнительные материалы для проверки фактов, изложенных в запросах, принять другие меры для объективного разрешения поставленных заявителями вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принимать по ним законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса – разъяснять также порядок обжалования принятого решения.

24. Для проверки фактов, изложенных в запросах, организуются служебные проверки в соответствии с законодательством Российской Федерации.

25. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных ма-

териалов. Если при проверке выявлены факты совершения государственным служащим Оператора ПД действия (бездействия), содержащего признаки административного правонарушения или состава преступления информация передается в уполномоченные органы.

26. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

27. При осуществлении контроля обращается внимание на сроки исполнения поручений по запросам и полноту рассмотрения поставленных вопросов, объективность проверки фактов, изложенных в запросах, законность и обоснованность принятых по ним решений, своевременность их исполнения и направления ответов заявителям.

28. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

УТВЕРЖДЕНЫ
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-ОД

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении делами Губернатора и Правительства Алтайского края

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении делами Губернатора и Правительства Алтайского края (далее – «Правила») определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в управлении делами Губернатора и Правительства Алтайского края (далее – управление делами) организуется проведение плановых и внеплановых проверок условий обработки персональных данных.

3. Проверки соответствия обработки персональных данных установленным требованиям в управлении делами проводятся на основании утвержденного в управлении делами ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановая проверка). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

4. Проверки осуществляются комиссией, образуемой приказом управления делами.

5. Комиссия имеет право:

- запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;

- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить управляющему делами Губернатора и Правительства Алтайского края предложения о совершенствовании правового, технического и ор-

ганизационного регулирования обеспечения безопасности персональных данных при их обработке;

- вносить управляющему делами Губернатора и Правительства Алтайского края предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

6. Члены комиссии, получившие доступ к персональным данным в ходе проведения мероприятий внутреннего контроля, должны обеспечивать конфиденциальность персональных данных субъектов персональных данных, не передавать третьим лицам и не распространять персональные данные без согласия субъектов персональных данных.

7. В проведении проверки не могут участвовать гражданские служащие, прямо или косвенно заинтересованные в её результатах.

8. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных;

- порядок и условия применения средств защиты информации;

- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учета машинных носителей персональных данных;

- соблюдение правил доступа к персональным данным;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществление мероприятий по обеспечению целостности персональных данных.

9. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, управляющему делами Губернатора и Правительства Алтайского края докладывает председатель комиссии, в форме письменного заключения.

10. Ответственный за организацию обработки персональных данных, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

УТВЕРЖДЕН
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13 03 2018 № 44-ОД

Перечень
персональных данных, обрабатываемых в управлении делами Губернатора и Правительства Алтайского края в связи с реализацией служебных (трудовых) отношений

Для реализации трудовых отношений в личное дело работника управления делами Губернатора и Правительства Алтайского края вносятся его персональные данные. Персональные данные, внесенные в личные дела работников, иные сведения, содержащиеся в личных делах работников, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации).

В управлении делами Губернатора и Правительства Алтайского края обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- дата, месяц, год рождения;
- место рождения;
- адрес регистрации и проживания;
- гражданство;
- знание иностранного языка;
- номер основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения о квалификации (профессия, образование, опыт работы);
- семейное положение, состав семьи;
- социальное и имущественное положение;
- сведения о трудовой деятельности и военной службе;
- индивидуальный номер налогоплательщика;
- номер страхового свидетельства обязательного пенсионного страхования;
- номер телефона;
- фотография;
- место работы и учебы членов семьи и родственников.

УТВЕРЖДЕН
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-ОД

Перечень информационных систем персональных данных управления делами Губернатора и Правительства Алтайского края

№ п/п	Наименование ИСПДн
1.	ИСПДн «Контур-Экстерн»
2.	ИСПДн «СУФД Казначейства»
3.	ИСПДн «Зарплата»
4.	ИСПДн «1С: Бухгалтерия для распределения бюджетных средств»
5.	ИСПДн «Сбербанк-Клиент»
6.	ИСПДн «Кадры управления делами»
7.	ИСПДн «Система контроля доступа»
8.	ИСПДн «Бюро пропусков»
9.	ИСПДн «Кадры Госслужба»
10.	ИСПДн «Федеральный портал управленческих кадров»
11.	ИСПДн «Награды»
12.	ИСПДн «Профилактика коррупционных правонарушений»

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03. 2018 № 44-ОД

ИНСТРУКЦИЯ
по организации доступа в помещения, в которых ведется обработка персональных данных

1.1. Настоящая Инструкция устанавливает порядок доступа и охраны (сдачи под охрану) защищаемых помещений информационных систем персональных данных (далее - ИСПДн), в которых ведется обработка персональных данных.

1.2. Вход посетителей в здание регламентируется «Положением о пропускном режиме в административном здании, расположенном по адресу: г. Барнаул, пр. Ленина, 59», утвержденным приказом управления делами Администрации Алтайского края от 18.10.2016 № 100-ОД.

1.3. Вскрытие (сдача под охрану) помещений осуществляется сотрудниками, имеющими право вскрывать (сдавать под охрану) данные помещения. Список сотрудников утверждается руководителем и передаётся на пост охраны.

1.4. При отсутствии сотрудников, ответственных за вскрытие (сдачу под охрану) помещений, данные помещения могут быть вскрыты комиссией, созданной на основании приказа, о чем составляется акт.

1.5. При закрытии помещения и сдаче их под охрану сотрудники, ответственные за помещения должны:

закрыть окна;

выключить освещение, электроприборы, оргтехнику;

проверить противопожарное состояние помещения;

убрать документы и съемные носители информации, на которых содержатся персональные данные, в сейф (металлический шкаф).

1.6. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, составляется акт. О происшествии докладывается руководителю и(или) ответственному за обеспечение безопасности персональных данных. Ответственный за обеспечение безопасности персональных данных и ответственный за организацию обработки персональных данных организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие машинных носителей информации.

1.7. Посетители могут находиться в защищаемых помещениях ИСПДн только в сопровождении сотрудников, работающих в данном помещении и имеющих доступ к персональным данным.

Неконтролируемое пребывание посторонних лиц в помещениях, в которых ведется обработка персональных данных, запрещается.

УТВЕРЖДЕНА
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-09

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее - ИСПДн), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Идентификация и аутентификация пользователей в ИСПДн осуществляется посредством использования персональных учетных записей пользователей и периодически сменяемых буквенно-цифровых паролей, содержащих не менее шести символов.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

1.4. Временный пароль, создаваемый при заведении учетной записи или смене забытого пароля, должен быть уникальным, передаваться способом, исключающим доступ к нему других лиц, и быть сменен пользователем при первом обращении к ИСПДн. Пароли, предустановленные производителем, должны сменяться до начала эксплуатации.

2. Порядок генерации, смены и прекращения действия и резервирования паролей

2.1. По решению руководителя структурного подразделения, согласованному с администратором безопасности ИСПДн, может применяться резервирование некоторых паролей, таких, как пароли администраторов безопасности ИСПДн, пароли ответственных должностных лиц, пароли отдельных пользователей, выполняющих важные функции, пароли, обеспечивающие работу отдельных сетевых сервисов.

2.2. Для резервирования пароля выполняются следующие действия:

- пароль записывается на лист бумаги и заверяется личной подписью;
- лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него вкладывается лист темной бумаги. Конверт заклеивается;

- на конверте владелец пароля указывает свою должность, фамилию и инициалы, наименование информационного средства, которое защищается этим паролем, текущие дату и время, и заверяет запись личной подписью;

- конверт передается на хранение руководителю структурного подразделения или лицу, им для этого назначенному, и учитывается в специальном разделе Журнала учета паролей. Учетный номер (сквозной по Журналу) проставляется ответственным за хранение на конверте;

- конверты с паролями хранятся в сейфе. Ответственный за хранение не реже чем один раз в месяц проверяет их наличие;

- при замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем. Новый резервный пароль подготавливает к хранению так, как указано выше;

- вскрытие конверта с паролем производится по решению руководителя структурного подразделения. Для вскрытия конверта назначается комиссия не менее чем из трех сотрудников подразделения. О вскрытии конверта комиссией составляется акт, утверждаемый руководителем подразделения, который по окончании работы комиссии хранится в деле подразделения;

- при появлении владельца пароля после факта вскрытия конверта пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

2.3. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (не реже раза в три месяца) замена пароля пользователя. Замена личного пароля осуществляется пользователем самостоятельно или администратором безопасности ИСПДн.

2.4. Удаление или блокирование учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) производится администратором безопасности ИСПДн после окончания последнего сеанса работы данного пользователя с системой.

2.5. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора безопасности ИСПДн, и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн.

2.6. В случае компрометации личного пароля пользователя ИСПДн проводится внеплановая смена пароля в зависимости от полномочий владельца скомпрометированного пароля.

2.7. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обеспечение безопасности персональных данных, периодический контроль - возлагается на администратора безопасности ИСПДн.

Запрещается:

- сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учетных записей);

- сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

- использовать учетные записи других лиц.

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03. 2018 № 44-ОД

ИНСТРУКЦИЯ
по организации резервного копирования персональных данных в информационных системах персональных данных

1. Общие положения

1.1. Данная инструкция определяет порядок организации резервного копирования персональных данных, обрабатываемых в информационных системах персональных данных (далее — ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Задачей данной инструкции является:

- определение мероприятий по защите ИСПДн от потери информации;
- определение действий по восстановлению информации ИСПДн в случае потери.

1.3. Действие настоящей инструкции распространяется на администратора безопасности ИСПДн, ответственного за обеспечение безопасности персональных данных ИСПДн и всех пользователей ИСПДн.

1.4. Пересмотр настоящего документа осуществляется ответственным за обеспечение безопасности персональных данных ИСПДн при изменении законодательства Российской Федерации или возникновении угрозы безопасности сохранения персональных данных.

1.5. Ответственным за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается ответственный за обеспечение безопасности персональных данных ИСПДн.

1.6. Контроль за обеспечением мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, возлагается на администратора безопасности ИСПДн.

2. Порядок реагирования на инцидент

2.1. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

- в результате преднамеренных действий пользователей или третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;

- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В сроки, не превышающие три рабочих дня, администратором безопасности ИСПДн применяются меры по восстановлению работоспособности ИСПДн. Предпринимаемые меры согласуются с вышестоящим руководством.

3. Меры по обеспечению непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Для предотвращения потерь информации при кратковременном отключении электроэнергии, все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также ПЭВМ 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 ПЭВМ;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (сетевое оборудование, ПЭВМ и т.д.).

3.2. Для защиты от неисправностей носителей информации на ПЭВМ, осуществляющих обработку и хранение информации, может использоваться технология RAID (кроме RAID-0), в которой применяется дублирование информации, хранимой на носителях информации.

3.3. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на носителе информации, не участвующем в непосредственной обработке информации.

3.4. Резервное копирование и хранение данных должно осуществляться на периодической основе:

- для обрабатываемых персональных данных – не реже раза в неделю;
- для технологической информации – не реже раза в 6 месяцев.

3.5. Носители, на которые произведено резервное копирование, должны быть учтены соответствующим образом.

3.6. Для обеспечения возможности восстановления данных, носители должны храниться не менее года.

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03. 2018 № 44-ОД

ИНСТРУКЦИЯ
по организации технического обслуживания и ремонта технических средств в информационных системах персональных данных

1. Общие положения

1.1. Данная инструкция определяет общие принципы организации технического обслуживания и ремонта технических средств в информационных системах персональных данных (далее - ИСПДн).

1.1. Инструкция регламентирует процесс технического обслуживания и ремонта оборудования, сопровождения программного обеспечения, устранения неисправностей программного обеспечения и технических средств ИСПДн.

2. Обслуживание и ремонт технических средств ИСПДн

2.1. Обслуживание технических средств ИСПДн предназначено для обеспечения работы ИСПДн, предотвращения ее неисправностей.

2.2. При проведении технического обслуживания (далее - ТО) и ремонта необходимо руководствоваться следующими принципами:

технические средства ИСПДн необходимо обслуживать в соответствии с технической документацией производителя;

2.3. ТО и ремонт должны проводиться только сотрудниками отдела по обслуживанию информационно-коммуникационных систем управления делами Губернатора и Правительства Алтайского края (далее – отдел ОИКС) или сторонними специалистами (при гарантийном обслуживании);

на период выполнения ТО и ремонта технических средств ИСПДн должны выполняться меры по защите персональных данных. В случае выполнения работ сторонней организацией за пределами контролируемой зоны, защищаемая информация должна быть удалена с технического средства;

должны соблюдаться требования поставщика технических средств для выполнения гарантийных обязательств.

2.4. Ответственность за своевременное проведение ТО и ремонта возлагается на отдел ОИКС.

3. Сопровождение программного обеспечения

3.1. При сопровождении программного обеспечения (далее - ПО) необходимо руководствоваться следующими принципами:

работы по сопровождению ПО должен проводить администратор без-

опасности ИСПДн или сторонние специалисты в присутствии администратора безопасности ИСПДн;

выполнять требования лицензионного соглашения на использование ПО в соответствии с законодательством Российской Федерации;

руководствоваться технической документацией производителя при сопровождении ПО;

при использовании сертифицированного по требованиям безопасности информации ПО, его настройку осуществлять и поддерживать в соответствии с технической документацией;

принимать меры по исключению несанкционированного доступа к защищаемой информации при сопровождении ПО сторонними организациями;

исключить возможность изменения пользователем состава ПО.

4. Устранение неисправностей технических средств и программного обеспечения

4.1. Отдел ОИКС обеспечивает анализ и устранение неисправностей технических средств и ПО, предпринимает необходимые действия по их предупреждению.

4.2. После выявления неисправности сотрудниками отдела ОИКС или сторонними специалистами (при гарантийном обслуживании) должны выполняться необходимые работы по восстановлению работоспособности технических средств и ПО.

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03 2018 № 44-ОД

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационных системах персональных данных

1. Общие положения

1.1. Данная инструкция предназначена для пользователей информационных систем персональных данных (далее - ИСПДн).

1.2. В целях обеспечения антивирусной защиты в ИСПДн производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности ИСПДн.

1.4. К применению в ИСПДн допускается лицензионное антивирусное программное обеспечение.

2. Порядок проведения антивирусного контроля в ИСПДн

2.1. Антивирусный контроль должен осуществляться на ПЭВМ в постоянном режиме.

2.2. Пользователи ИСПДн при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия вирусов.

2.3. Администратор безопасности ИСПДн осуществляет периодическое обновление антивирусных баз и контроль их работоспособности.

2.4. Администратор безопасности ИСПДн проводит периодическое тестирование установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

2.5. При обнаружении компьютерного вируса пользователь обязан поставить в известность администратора безопасности ИСПДн и прекратить какие-либо действия в ИСПДн.

2.6. Администратор безопасности ИСПДн проводит лечение зараженных файлов с помощью антивирусной программы, а если это невозможно, то их удаление (стирание, уничтожение) и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на носителе информации вируса, не поддающегося лечению, администратор безопасности ИСПДн обязан запретить использование носителя информации.

2.8. В случае обнаружения в ИСПДн не поддающегося лечению вируса, администратор безопасности ИСПДн обязан поставить в известность ответственного за обеспечение безопасности ИСПДн или руководителя структурного подразделения, запретить работу в ИСПДн и принять меры по восстановлению работоспособности ИСПДн.

УТВЕРЖДЕНА
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03. 2018 № 44-ОД

ИНСТРУКЦИЯ
по работе пользователей в информационных системах персональных данных

1. Общие положения

1.1. Данная инструкция определяет общие принципы работы пользователей в информационной системе персональных данных (далее - ИСПДн). Пользователями ИСПДн являются сотрудники, допущенные к работе с персональными данными. Пользователи ИСПДн несут персональную ответственность за свои действия.

1.2. Допуск пользователей для работы в ИСПДн осуществляется в соответствии со списком лиц, имеющих доступ к персональным данным.

1.3. Устные указания о доступе кого бы то ни было к ИСПДн не имеют юридической силы и не обязательны для исполнения.

1.4. Доступ пользователей в ИСПДн организует администратор безопасности ИСПДн.

2. Порядок работы пользователей в ИСПДн

2.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ИСПДн, присвоенными администратором безопасности ИСПДн. При этом для хранения файлов, содержащих персональные данные, разрешается использовать только специально выделенные каталоги, а также соответствующим образом учтенные машинные носители информации.

2.2 Пользователь отвечает за правильность включения и выключения ПЭВМ, входа в систему и действия при работе в ИСПДн.

2.3. Вход пользователя в систему осуществляется на основе ввода (по запросу системы) имени, присвоенного при регистрации администратором безопасности ИСПДн, и личного пароля. Требования к сложности пароля и периодичности его замены установлены в «Инструкции по организации парольной защиты в информационных системах персональных данных».

2.4. В случае отказа системы в идентификации пользователя либо не подтверждения личного пароля следует обратиться к администратору безопасности ИСПДн.

2.5. Резервное копирование, уничтожение и восстановление защищаемой информации осуществляются пользователем в рамках выделенных полномочий, либо администратором безопасности ИСПДн.

2.6. Перед началом работы с носителями информации пользователь обязан проверить их на наличие вирусов с использованием антивирусного программного обеспечения, установленного в ИСПДн, в соответствии с «Инструкцией по проведению антивирусного контроля в информационных системах персональных данных». В случае обнаружения вирусов на носителе информации пользователь обязан сообщить об этом администратору безопасности ИСПДн.

2.7. В процессе работы пользователю запрещается:

использовать для хранения и обработки защищаемой информации носители, не учтенные соответствующим образом;

осуществлять попытки несанкционированного доступа к ресурсам системы и других пользователей;

пытаться подменять функции администратора безопасности ИСПДн по перераспределению времени работы и полномочий доступа к ресурсам ИСПДн;

оставлять рабочий компьютер с незавершенным сеансом. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть заблокирован;

допускать посторонних лиц к рабочий компьютер;

сообщать (или передавать) посторонним лицам атрибуты доступа к ресурсам ИСПДн;

самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических средств или программного обеспечения;

открывать общий доступ к папкам на своей рабочей станции, содержащим персональные данные;

работать на компьютере при обнаружении неисправности;

самостоятельно вносить изменения в конструкцию, конфигурацию, размещение рабочего компьютера и другие узлы ИСПДн.

3. Ответственность

3.1. Ответственность за допуск пользователя к ресурсам и установленные ему полномочия несет руководитель структурного подразделения.

3.2. Пользователи ИСПДн, виновные в нарушении законодательства Российской Федерации о защите персональных данных и охраняемых по закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и внутренними организационно-распорядительными документами.

3.3. По всем возникающим вопросам при работе в ИСПДн необходимо обращаться в отдел по обслуживанию информационно-коммуникационных систем управления делами Губернатора и Правительства Алтайского края.

УТВЕРЖДЕНА
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03 2018 № 44-ОД

ИНСТРУКЦИЯ
по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных

1. Общие положения

1.1. Настоящая Инструкция устанавливает требования к организации учета и использования машинных носителей информации, предназначенных для обработки и хранения персональных данных в информационных системах персональных данных (далее - ИСПДн).

1.2. Учет машинных носителей информации, предназначенных для обработки и хранения персональных данных, осуществляет ответственный за организацию обработки персональных данных.

1.3. Все машинные носители информации, предназначенные для обработки и хранения персональных данных (далее - МНИ) регистрируются по журналу учета и выдачи машинных носителей информации, содержащих персональные данные (далее - Журнал) ответственным за организацию обработки персональных данных.

1.4. Ответственность за сохранность полученных МНИ несет пользователь ИСПДн.

2. Учет машинных носителей информации, предназначенных для обработки и хранения персональных данных

2.1. К МНИ относятся:

съемные носители информации;

несъемные носители информации.

2.2. При обработке персональных данных на ПЭВМ соблюдается следующий порядок учета, хранения МНИ:

2.2.1. Каждому МНИ присваивается учетный номер по Журналу. Учетный номер наносится на МНИ ответственным за организацию обработки персональных данных. Если невозможно маркировать непосредственно МНИ, то маркируется упаковка, в которой он хранится.

Учетный номер состоит из двух частей АААХХХ, где

ААА - буквенное сокращение из 3 символов (определяются ответственным за организацию обработки персональных данных).

ХХХ - трехзначный порядковый номер по Журналу.

2.2.2. МНИ выдаются пользователям ИСПДн с отметкой в Журнале.

2.2.3. Хранение съемных МНИ должно осуществляться в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

2.2.4. МНИ, после удаления информации, содержащей персональные данные, с учета не снимаются. В дальнейшем эти МНИ могут использоваться для обработки и хранения персональных данных. Если МНИ не пригодны для дальнейшего использования, они подлежат списанию и уничтожению.

2.2.5. О фактах утраты МНИ докладывается ответственному за организацию обработки персональных данных, с внесением записи в Журнал.

2.2.6. Передача МНИ производится ответственным за организацию обработки персональных данных по Журналу.

2.2.7. В случае неисправности МНИ, пользователь сдает его ответственному за организацию обработки персональных данных с внесением в Журнал записи о неисправности МНИ.

2.3. МНИ, утратившие практическое значение или пришедшие в негодность, уничтожаются.

3. Порядок уничтожения МНИ

Уничтожение МНИ производится ответственным за организацию обработки персональных данных, путем их физического разрушения, с оформлением акта уничтожения. Перед уничтожением МНИ информация с них должна быть удалена (уничтожена, стерта и т.д.).

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края

от 13.03 2018 № 44-ОД

ИНСТРУКЦИЯ
по правилам обращения с носителями ключевой информации в информационных системах персональных данных

1. Термины и определения

1.1. Электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном федеральным законом № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Носитель ключевой информации (далее - ключевой носитель) – машинный носитель информации, содержащий ключ электронной подписи.

2. Общие положения

2.1. Настоящая инструкция предназначена для пользователей информационных систем персональных данных, использующих средства ЭП.

2.2. Инструкция содержит основные правила обращения с ключами ЭП, выполнение которых необходимо для обеспечения защиты информации при обмене электронными документами.

2.3. Работу с ключами ЭП контролирует администратор безопасности ИСПДн. Администратор безопасности ИСПДн проводит инструктаж с пользователями по правилам изготовления, хранения, обращения и

эксплуатации ключей.

2.4. Владелец сертификата ключа проверки ЭП, вырабатывает самостоятельно или в сопровождении администратора безопасности ИСПДн личный ключ ЭП, а также запрос на получение сертификата ключа проверки электронной подписи (в электронном виде и на бумажном носителе).

2.5. Владелец ключа ЭП несет персональную ответственность за безопасность ключей ЭП и обязан обеспечивать их сохранность, неразглашение и нераспространение, несет персональную ответственность за нарушение требований настоящей инструкции.

2.6. Запрещается оставлять без контроля ПЭВМ с незаблокированным сеансом, на котором применяется ЭП.

2. Порядок работы со средствами ЭП

3.1. Учет носителей ключевой информации осуществляет администратор безопасности ИСПДн.

3.2. Ключи ЭП изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В работе используется рабочая копия ключевого носителя.

3.3. При выходе из строя носителя с ключевой информацией пользователь уведомляет об этом администратора безопасности ИСПДн. Администратор безопасности ИСПДн в присутствии пользователя изготовляет копию ключевого носителя с эталонной копии.

3.4. Не позднее, чем за 10 рабочих дней до окончания срока действия ключа ЭП, его владелец обязан выполнить все мероприятия по формированию новых ключей.

3.5. Ключевые носители хранятся в шкафах (сейфах, ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.6. Хранение ключевых носителей допускается в одном хранилище с другими документами и ключевыми носителями, при этом отдельно от них и в упаковке, исключающей возможность неправомерного доступа к ним.

3.7. Ключевые носители должны находиться в пределах контролируемой зоны, за исключением случаев, связанных со служебной необходимостью.

3.8. Не допускается:

осуществлять несанкционированное администратором безопасности ИСПДн копирование ключевых носителей;

передавать носители ключевой информации и (или) их содержимое лицам, не допущенным к ним;

записывать на ключевые носители другую информацию.

4. Действия при компрометации ключей ЭП

4.1. Компрометация ключа ЭП – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

4.2. К событиям, связанным с компрометацией ключей ЭП, относятся, включая, но не ограничивая, следующие:

потеря ключевых носителей;

нарушение правил хранения и уничтожения;

возникновение подозрений на утечку информации или ее искажение;

случаи, когда нельзя установить, что произошло с ключевыми носителями.

4.3. При компрометации ключа ЭП пользователь прекращает обмен электронными документами с другими пользователями и извещает администратора безопасности ИСПДн о факте компрометации.

4.4. По факту компрометации ключей должно быть проведено служебное расследование.

5. Уничтожение ключей ЭП

5.1. Ключи ЭП должны быть выведены из действия и уничтожены в следующих случаях:

плановая смена ключей ЭП;

изменение данных о владельце ЭП;

компрометация ключей;

выход из строя ключевых носителей;

прекращение полномочий владельца ЭП.

5.2. Уничтожение ключей ЭП может производиться путем уничтожения ключевого носителя, на котором они расположены, или путем удаления ключей без повреждения ключевого носителя.

5.3. Ключи ЭП должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия).

УТВЕРЖДЕН
приказом управления делами
Губернатора и Правительства
Алтайского края
от 13.03 2018 № 44-ОД

Перечень должностей служащих, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным

№ п\п	Должность
Управление делами Губернатора и Правительства Алтайского края	
1.	заместитель управляющего делами, начальник отдела организационно-планового обеспечения
2.	помощник управляющего делами Губернатора и Правительства Алтайского края по обеспечению безопасности деятельности
Отдел по учету и отчетности управления делами Губернатора и Правительства Алтайского края	
3.	начальник отдела – главный бухгалтер
4.	заместитель начальника отдела – главного бухгалтера
5.	консультант
6.	главный специалист
7.	ведущий специалист
8.	бухгалтер эксплуатационно-хозяйственной группы
9.	экономист по бухгалтерскому учету и хозяйственной деятельности
Отдел организационно-планового обеспечения управления делами Губернатора и Правительства Алтайского края	
10.	консультант
11.	ведущий специалист
Сектор режима эксплуатационно-хозяйственной группы управления делами Губернатора и Правительства Алтайского края	
12.	начальник бюро пропусков
13.	делопроизводитель
Отдел по обслуживанию информационно-коммуникационных систем управления делами Губернатора и Правительства Алтайского края	
14.	начальник отдела
15.	консультант

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03 2018 № 44-ОД

ТИПОВАЯ ФОРМА

согласия на обработку персональных данных государственных гражданских служащих Алтайского края, а также иных субъектов персональных данных

Я, _____
(фамилия, имя, отчество)(последнее – при наличии)

паспорт _____ выдан « ___ » _____ _____ г.
(серия, номер)

_____

_____
(когда и кем выдан)

проживающий(ая) по адресу: _____

_____

_____

свободно, своей волей и в своем интересе даю согласие уполномоченным должностным лицам управления делами Губернатора и Правительства Алтайского края (далее – управление делами), расположенного по адресу: Алтайский край, г. Барнаул, просп. Ленина, д.59, на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение) следующих персональных данных:

фамилия, имя, отчество, дата и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения) <*>;

владение иностранными языками;

образование (когда и какие образовательные учреждения закончил(а);

номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);

послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень;

ученое звание (когда присвоены, номера дипломов, аттестатов);

выполняемая работа с начала трудовой деятельности;

классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное зва-

ние, классный чин правоохранительной службы, классный чин юстиции (кем и когда присвоены) <*>;

государственные награды, иные награды и знаки отличия (кем награжден(а) и когда);

степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены) <*>;

пребывание за границей (когда, где, с какой целью) <*>;

близкие родственники (отец, мать, братья, сестры и дети), а также муж (жена), в том числе бывшие, постоянно проживающие за границей и (или) оформляющие документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей) <*>;

адрес регистрации и фактического проживания;

дата регистрации по месту жительства;

паспорт (серия, номер, кем и когда выдан);

свидетельства о государственной регистрации актов гражданского состояния;

номер телефона;

отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

идентификационный номер налогоплательщика;

номер страхового свидетельства обязательного пенсионного страхования;

наличие (отсутствие) судимости <*>;

допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата) <*>;

заключение медицинского учреждения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению <*>;

сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей <*>;

сведения о размещении информации в информационно-телекоммуникационной сети «Интернет», предусмотренные статьей 20.2 Федерального закона от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации" <*>.

Вышеуказанные персональные данные предоставляются для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на государственную гражданскую службу Алтайского края (работу), ее прохождением и прекращением (трудовых и непосредственно связанных с ними отно-

шений) для реализации функций, возложенных на управление делами действующим законодательством.

Я ознакомлен(а), что:

1. согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока государственной гражданской службы (работы) в управлении делами;

2. согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3. в случае отзыва согласия на обработку персональных данных управление делами вправе продолжить обработку персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

4. после увольнения с государственной гражданской службы Алтайского края (прекращения трудовых отношений) персональные данные хранятся в управлении делами в течение срока хранения документов, предусмотренного действующим законодательством Российской Федерации;

5. персональные данные, предоставляемые в отношении третьих лиц (близких родственников, супругов), будут обрабатываться только в целях осуществления и выполнения функций, возложенных законодательством Российской Федерации на управление делами.

Дата начала обработки персональных данных:

_____ _____

(число, месяц, год) (подпись)

<*> Включаются в согласие на обработку персональных данных государственных гражданских служащих Алтайского края, а также граждан, претендующих на замещение должностей государственной гражданской службы Алтайского края.

УТВЕРЖДЕНА
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03 2018 № 44-ОД

ТИПОВАЯ ФОРМА
согласия на обработку персональных данных

(запрашивается при выдаче пропуска на вход в здание Правительства Алтайского края)

В соответствии с п.4 ст. 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»

Я, _____

(фамилия, имя, отчество (при наличии), дата рождения)

Документ, удостоверяющий личность _____

_____

_____

(наименование документа, №, сведения о дате выдачи документа и выдавшем органе)

_____

проживающий(ая) по адресу: _____

_____

в целях выдачи мне пропуска на вход в здание Правительства Алтайского края, находящееся по адресу: 656035, г. Барнаул, пр. Ленина, 59, даю согласие на обработку должностными лицами управления делами Губернатора и Правительства Алтайского края, моих персональных данных, с учетом требований действующего законодательства Российской Федерации, и подтверждаю, что, давая такое согласие, я действую своей волей и в своем интересе.

Согласие распространяется на следующую информацию: мои фамилия, имя, отчество, год, месяц, дата рождения, адрес, фотография, данные документа, удостоверяющего личность.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, предусмотренных п.3 ст. 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Настоящее согласие действует со дня его подписания до окончания срока действия пропуска.

Отзыв настоящего согласия будет мной осуществлен в письменной форме по месту нахождения управления делами Губернатора и Правительства Алтайского края.

Права, предусмотренные Федеральным законом от 27.07.2006 г № 152-ФЗ «О персональных данных», мне разъяснены.

«___» _____ 20 ___ г _____ _____

(дата) (подпись) (расшифровка подписи)

УТВЕРЖДЕНО
приказом управления делами Губернатора и Правительства Алтайского края
от 13.03. 2018 № 44-ОД

Типовое обязательство гражданского служащего управления делами Губернатора и Правительства Алтайского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним государственного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я, _____
(фамилия, имя, отчество) (последнее – при наличии)

_____
(должность)

_____

_____

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной государственного контракта, освобождения меня от замещаемой должности и увольнения с гражданской службы.

В соответствии со статьей 7 Федерального закона от 27 июля 2006г № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006г № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

_____ _____ 20 ___ _____ _____
(дата) (подпись) (расшифровка подписи)