УПРАВЛЕНИЕ
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
АЛТАЙСКОГО КРАЯ

ПРИКАЗ

21 сентября 2017 № 112

г. Барнаул

Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления связи и массовых коммуникаций Алтайского края

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» приказываю:

1. Утвердить Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления связи и массовых коммуникаций Алтайского края.

2. Отделу информационной безопасности (Канаев А.А.) обеспечить ознакомление государственных гражданских служащих и работников управления связи и массовых коммуникаций Алтайского края с утвержденной пунктом 1 настоящего приказа документацией в касающейся их части.

3. Признать утратившим силу приказ управления информационных технологий и связи Алтайского края от 23.05.2014 № 42-пр «О мерах по обеспечению безопасности персональных данных».

4. Контроль за исполнением настоящего приказа возложить на заместителя начальника управления, начальника отдела развития информационных систем и ресурсов Переверзева М.В.

Начальник управления М.В. Герасимюк

УТВЕРЖДЕНО

приказом управления связи и массовых коммуникаций Алтайского края
от 21.03.2017 № 112

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления связи и массовых коммуникаций Алтайского края

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных управления связи и массовых коммуникаций Алтайского края (далее – «Положение») разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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» 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 управления связи и массовых коммуникаций Алтайского края (далее - «оператор персональных данных»).

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных обеспечивается применением организационных мер и технических средств защиты информации (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 связи и массовых коммуникаций Алтайского края;

результатов анализа инцидентов информационной безопасности в ИС персональных данных.

Изменения Положения должны быть направлены на предотвращение инцидентов или устранение последствий уже реализованных 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. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки недопустимо объединение созданных для несовместимых между собой целей баз данных ИС персональных данных.

2.4. Персональные данные оператор получает непосредственно от субъектов персональных данных, которые принимают решение об их предоставлении и дают согласие на их обработку добровольно и с учетом собственных интересов.

2.5. Лица, доступ которых к персональным данным, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списков сотрудников, допущенных к соответствующим персональным данным.

2.6. Принятые в управлении связи и массовых коммуникаций Алтайского края организационно-распорядительные документы доводятся до сведения лиц, участвующих в процессе обработки персональных данных в части

их касающейся.

2.7. Персональные данные, используемые для обработки в ИС, порядок их использования, цель, периодичность и основания внесения изменений и дополнений в организационные документы, а также порядок хранения персональных данных устанавливаются оператором персональных данных с соблюдением требований Трудового кодекса Российской Федерации и иных федеральных законов.

2.8. 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, предусмотренных статьей 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.9. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Персональные данные подлежат уничтожению по достижении всех целей их обработки или в случае утраты необходимости в достижении этих целей. Оператор по согласованию с субъектом персональных данных может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3. Обязанности и права оператора персональных данных в ИС

3.1. Оператор персональных данных 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 необходимыми 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 уведомить третьих лиц, которым персональные данные этого субъекта были переданы.

3.2. 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, 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, 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.

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 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, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. 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. 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 и уничтожить персональные данные 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 № 152-ФЗ «О персональных данных» или другими федеральными законами.

3.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные 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 со-

глашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

3.7. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 3.4 - 3.6 настоящего Положения, оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

4. Методы и способы защиты персональных данных в ИС 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 сотрудниками отдела информационной безопасности управления связи и массовых коммуникаций Алтайского края.

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. Обработка персональных данных в ИС 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 управления связи и массовых коммуникаций Алтайского края;

Перечень персональных данных, обработка которых ведется в управлении связи и массовых коммуникаций Алтайского края;

Перечень должностей управления связи и массовых коммуникаций Алтайского края, которым необходим доступ к персональным данным;

Перечень помещений управления связи и массовых коммуникаций Алтайского края, в которых ведется обработка персональных данных

Инструкция по работе пользователей в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации парольной защиты в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации резервного копирования информации в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по проведению антивирусного контроля в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа;

Инструкция по организации обслуживания и ремонта технических средств в информационных системах управления связи и массовых коммуникаций Алтайского края;

Инструкция по организации доступа в помещения управления связи и массовых коммуникаций Алтайского края, в которых осуществляется обработка защищаемой информации, в том числе персональных данных и иной информации конфиденциального характера;

Типовая форма журнала учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа;

Инструкция администратора безопасности информационных систем управления связи и массовых коммуникаций Алтайского края;

Инструкция ответственного за организацию обработки персональных данных управления связи и массовых коммуникаций Алтайского края;

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении связи и массовых коммуникаций Алтайского края.

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. Начальник управления связи и массовых коммуникаций 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;

осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИС персональных данных управления связи и массовых коммуникаций Алтайского края по вопросам государственной службы и кадров;

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 управления связи и массовых коммуникаций Алтайского края;

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

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:

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;

организует регистрацию и осуществляет учет защищаемых носителей информации.

5.5. Отдел информационной безопасности управления связи и массовых коммуникаций Алтайского края:

организует 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 связи и массовых коммуникаций Алтайского края;

разрабатывает совместно с другими структурными подразделениями управления связи и массовых коммуникаций Алтайского края 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;

5.6. Отдел администрирования управления связи и массовых коммуникаций Алтайского края, в части его полномочий, 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 организационных и технических мер по обеспечению безопасности персональных данных при обработке персональных данных в ИСПДн осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.

6.2. Уполномоченным органом по защите прав субъектов персональных данных осуществляется контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

6.3. Повседневный контроль выполнения организационных мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИС персональных данных, осуществляется сотрудниками управления связи и массовых коммуникаций Алтайского края, ответственными за организацию обработки персональных данных и за обеспечение безопасности персональных данных.