Приложение 1
к Приказу КГБУ ОЭПАК
от 23.03.2016 № 5

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных краевого государственного бюджетного учреждения «Оператор электронного правительства Алтайского края»

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных краевого государственного бюджетного учреждения «Оператор электронного правительства 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. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных краевого государственного бюджетного учреждения «Оператор электронного правительства Алтайского края» (далее – «организация», «оператор персональных данных»).

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) 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 ИСПДн.

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 ИСПДн оператора персональных данных;

результатов анализа инцидентов информационной безопасности в ИСПДн.

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

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

2. Обработка персональных данных

2.1. Оператор персональных данных осуществляет обработку персональных данных лиц, не относящиеся к должностям государственной гражданской и муниципальной службы Алтайского края, а также лиц, не являющихся сотрудниками оператора.

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 ИСПДн.

2.3. Объем и характер обрабатываемых персональных данных должен соответствовать целям их обработки. Обрабатываемые персональные данные должны соответствовать заявленным целям обработки. Недопустимо объединение созданных для несовместимых между собой целей баз данных ИСПДн.

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

2.5. 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.

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

2.7. Принятые в организации организационно-распорядительные документы доводятся до сведения лиц, участвующих в процессе обработки персональных данных в части их касающейся.

2.8. Персональные данные, используемые для обработки в ИСПДн, порядок их использования, цель, периодичность и основания внесения изменений и дополнений в организационные документы, а также порядок хранения персональных данных устанавливаются оператором персональных данных.

2.9. Оператор персональных данных 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.

2.10.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 персональных данных по согласованию с субъектом персональных данных может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора персональных данных законодательством Российской Федерации.

3. Обязанности и права оператора персональных данных в ИСПДн

3.1. Оператор персональных данных обязан предоставлять субъекту персональных данных возможность ознакомления с его персональными данными, а также вносить в них необходимые изменения, уничтожать или блокировать соответствующие персональные данные в случае предоставления субъектом персональных данных сведений, подтверждающих, что

персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор в ИСПДн, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и принятых мерах оператор персональных данных уведомляет субъекта персональных данных или его законного представителя и 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 персональных данных 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 недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов, обязан уточнить персональные данные и отменить их блокирование.

3.4. В случае выявления неправомерных действий с персональными данными оператор персональных данных в срок, не превышающий тридцати дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор персональных данных в срок, не превышающий тридцати дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных – также в указанный орган.

3.5. Оператор персональных данных, в случае достижения всех целей обработки персональных данных, обязан незамедлительно прекратить их обработку и уничтожить соответствующие персональные данные в срок, не превышающий тридцати дней с даты достижения всех целей обработки персональных данных по согласованию с субъектом персональных данных оператор персональных данных может изменить сроки хранения его персональных данных в связи с обязанностями, возлагаемыми на оператора законодательством Российской Федерации.

3.6. Оператор персональных данных, в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, обязан прекратить их обработку и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором персональных данных и субъектом персональных данных.

3.7. Оператор персональных данных 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 ИСПДн) запрещается.

4. Методы и способы защиты персональных данных в ИСПДН

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

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.

4.3. Модель угроз безопасности персональных данных корректируется при изменении состава основных угроз, и изменении программно-технических средств защиты информации.

4.4. Установка, изменение (обновление) и удаление программного обеспечения в ИСПДн производится сотрудниками отдела администрирования и защиты информационных систем, по согласованию с администратором информационной безопасности.

4.5. Доступ лиц к ИСПДн, не допущенных к работе с персональными данными, должен быть исключен. ИСПДн 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 ИСПДн.

4.6. Обработка персональных данных в ИСПДн осуществляется с использованием средств защиты информации в соответствии с установленными требованиями нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обеспечением безопасности информации, а так же соответствующей инструкцией по работе пользователя и инструкцией по проведению антивирусного контроля.

4.7. 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.

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. Руководитель организации:

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 ИСПДн организации;

назначает ответственного за организацию обработки персональных данных;

назначает ответственного за обеспечение безопасности персональных данных;

назначает администратора информационной безопасности.

5.2. Ответственный за организацию обработки персональных данных:

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

доводит до сведения работников оператора персональных данных 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 информационных системах организации;

организует выполнение мероприятий, направленных на обеспечение защиты персональных данных при их обработке в ИСПДн;

организует расследование причин и условий появления нарушений безопасности ИСПДн, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;

разрабатывает проекты распорядительных документов по защите персональных данных при их обработке в ИСПДн в организации;

разрабатывает совместно с другими структурными подразделениями организации настоящее Положение и вносит в него в установленном порядке изменения;

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

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

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

5.4. Администратор информационной безопасности:

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

осуществляет установку и ввод в эксплуатацию средств защиты информации ИСПДн в соответствии с эксплуатационной и технической документацией;

обеспечивает работы по проведению антивирусного контроля в ИСПДн;

организует работы по резервному копированию персональных данных;

осуществляет установку, подключение и настройку программно-технических средств защиты от несанкционированного доступа в ИСПДн в соответствии с технической документацией, нормативными правовыми актами Российской Федерации;

5.5. Подразделение или лицо, ответственное за техническое обслуживание средств вычислительной техники в организации обеспечивает обслуживание и ремонт сетевого оборудования, рабочих станций, серверного и периферийного оборудования в ИСПДн.

6. Контроль состояния защиты персональных данных

6.1. Контроль и надзор за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИСПДн, установленных Правительством Российской Федерации, осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, а также уполномоченным органом по защите прав субъектов персональных данных в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в ИСПДн.

7. Заключительные положения

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

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