

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Алтайского краевого Законодательного Собрания

1. Общие положения

1.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Алтайского краевого Законодательного Собрания (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Правилами обработки персональных данных в Алтайском краевом Законодательном Собрании, утвержденными в приложении 1 настоящего распоряжения 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 (далее – ИСПДн).

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в ИСПДн, находящихся на балансе Алтайского краевого Законодательного Собрания (далее – оператор).

1.3. Безопасность персональных данных при их обработке в ИСПДн 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 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:

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

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

3) изменения процессов обработки персональных данных в ИСПДн Алтайского краевого Законодательного Собрания;

4) результатов анализа инцидентов информационной безопасности в ИСПДн.

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

1.7. Все предлагаемые изменения Положения до 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 ИСПДн.

2. Категории субъектов персональных данных

К категориям субъектов персональных данных, персональные данные которых обрабатываются в соответствии с правилами обработки персональных данных в Алтайском краевом Законодательном Собрании, относятся:

1) депутаты Алтайского краевого Законодательного Собрания, в том числе замещающие государственные должности Алтайского края в Алтайском краевом Законодательном Собрании;

2) государственные гражданские служащие Алтайского края, замещающие должности в Алтайском краевом Законодательном Собрании;

3) граждане, замещающие должности, не являющиеся должностями государственной гражданской службы Алтайского края в Алтайском краевом Законодательном Собрании;

4) граждане, претендующие на замещение должностей государственной гражданской службы Алтайского края в Алтайском краевом Законодательном Собрании;

5) граждане, претендующие на замещение должностей, не являющихся должностями государственной гражданской службы Алтайского края в Алтайском краевом Законодательном Собрании;

6) иные физические лица, данные о которых обрабатываются во исполнение задач и функций, предусмотренных нормативными правовыми актами, регламентирующими деятельность Алтайского краевого Законодательного Собрания.

3. Обработка персональных данных

3.1. 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.

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

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

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

3.5. 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.

3.6. Лица, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании перечня должностей в аппарате Алтайского краевого Законодательного Собрания, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

3.7. Принятые в Алтайском краевом Законодательном Собрании организационно-распорядительные документы доводятся до сведения лиц, участвующих в обработке персональных данных, в части их касающейся.

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

3.9. 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 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 должны быть установлены уровни защищенности персональных данных в 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 при их обработке в ИСПДн (далее – Модель) для каждой ИСПДн.

При изменении состава основных технических средств и условий эксплуатации ИСПДн отделом информатизации информационно-аналитического управления аппарата Алтайского краевого Законодательного Собрания вносятся изменения в Модель данного ИСПДн.

4.3. Установка, изменение (обновление) и удаление программного обеспечения в ИСПДн производится ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн либо в его присутствии.

4.4. Доступ к ИСПДн лиц, не допущенных к работе с персональными данными, запрещен. 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.

4.5. Подключение ИСПДн 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 должны обеспечивать сохранность технических средств и носителей персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.7. Все носители персональных данных должны быть учтены, а их учетные данные занесены в журнал учета.

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

1) перечень информационных систем персональных данных Алтайского краевого Законодательного Собрания;

2) перечень персональных данных, обрабатываемых в Алтайском краевом Законодательном Собрании в связи с реализацией служебных (трудовых) отношений;

3) перечень должностей в аппарате Алтайского краевого Законодательного Собрания, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

4) перечень должностных лиц, доступ которых к персональным данным,

обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей, с указанием помещений Алтайского краевого Законодательного Собрания, в которых разрешена обработка персональных данных;

5) инструкция пользователя по работе в информационных системах персональных данных Алтайского краевого Законодательного Собрания;

6) инструкция о порядке доступа сотрудников в служебные помещения Алтайского краевого Законодательного Собрания, в которых производится обработка персональных данных;

7) инструкция по организации резервного копирования персональных данных в информационных системах персональных данных Алтайского краевого Законодательного Собрания;

8) инструкция по организации учета, использования и уничтожения машинных носителей информации, предназначенных для обработки и хранения персональных данных в Алтайском краевом Законодательном Собрании;

9) инструкция по организации парольной защиты на объектах информатизации Алтайского краевого Законодательного Собрания;

10) инструкция по организации антивирусной защиты объектов информатизации Алтайского краевого Законодательного Собрания;

11) правила рассмотрения запросов субъектов персональных данных или их представителей в Алтайском краевом Законодательном Собрании;

12) правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Алтайском краевом Законодательном Собрании;

13) правила обработки персональных данных в Алтайском краевом Законодательном Собрании;

14) другие организационно-распорядительные документы по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн.

4.9. 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. Председатель Алтайского краевого Законодательного Собрания:

1) утверждает правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Алтайском краевом Законодательном Собрании;

2) обеспечивает реализацию мероприятий по защите персональных данных при их обработке в ИСПДн Алтайского краевого Законодательного Собрания;

3) назначает ответственного за организацию обработки персональных данных;

4) назначает ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн.

5.2. Ответственный за организацию обработки персональных данных:

1) осуществляет внутренний контроль за соответствием обработки персональных данных требованиям к защите персональных данных в Алтайском краевом Законодательном Собрании;

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

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

4) осуществляет финансовое, материально-техническое и иное обеспечение мероприятий по защите персональных данных при их обработке в ИСПДн Алтайского краевого Законодательного Собрания;

5.3. Ответственный за обеспечение безопасности персональных данных при их обработке в ИСПДн:

1) организует разработку, внедрение, совершенствование и эксплуатацию системы защиты ИСПДн;

2) организует регистрацию и учет защищаемых носителей информации;

3) обеспечивает обнаружение фактов несанкционированного доступа к ИСПДн, о которых должен доложить ответственному за организацию обработки персональных данных;

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

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

6) обеспечивает работы по проведению антивирусного контроля в ИСПДн;

7) выполняет резервное копирование персональных данных;

8) осуществляет установку (обновление версий) программного обеспечения ИСПДн, обеспечивает его функционирование;

9) осуществляет установку, подключение и настройку технических средств ИСПДн в соответствии с технической документацией;

10) осуществляет установку (развертывание) новых ИСПДн или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач.

5.4. Отдел информатизации организационно-аналитического управления аппарата Алтайского краевого Законодательного Собрания:

1) осуществляет выполнение мероприятий по защите персональных данных при их обработке в ИСПДн;

2) разрабатывает проекты распорядительных документов по защите

персональных данных при их обработке в ИСПДн в Алтайском краевом Законодательном Собрании;

3) разрабатывает положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Алтайского краевого Законодательного Собрания и подготавливает предложения по внесению в него изменений;

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

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

6) 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;

7) 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 законодательством 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 ИСПДн.

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