

УТВЕРЖДЕНЫ
приказом министерства науки
и инновационной политики
Новосибирской области
от 25.11.2020 № 124

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», в министерстве науки и инновационной политики Новосибирской области

Общие положения

1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в министерстве науки и инновационной политики Новосибирской области (далее – Правила) разработаны в соответствии с постановлением 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».

2. Правилами определяется порядок организации и осуществления внутреннего контроля обработки персональных данных (далее – ПДн) в министерстве науки и инновационной политики Новосибирской области (далее – министерство) с целью своевременного выявления и предотвращения:

- хищения технических средств и носителей информации;
- утраты информации;
- преднамеренных программно-технических воздействий на информацию и (или) средства вычислительной техники, вызывающих нарушение целостности информации и нарушение работоспособности автоматизированной системы;
- несанкционированного доступа к ПДн с целью уничтожения, искажения, модификации (подделки), копирования и блокирования;
- утечки информации по техническим каналам.

3. Внутренний контроль состояния защиты информации включает в себя:

- контроль организации защиты информации;
- контроль эффективности защиты информации.

Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности персональных данных в министерстве науки и инновационной политики Новосибирской области

4. В целях осуществления в министерстве внутреннего контроля соответствия обработки ПДн установленным требованиям организуется проведение периодических проверок условий обработки ПДн.

Проверка осуществляется лицом, ответственным за организацию обработки ПДн в министерстве с привлечением администратора информационных систем и администратора информационной безопасности (в пределах их компетенции), а также комиссией, образуемой приказом министерства и действующей до момента завершения проверки и оформления заключения о ее результатах. Комиссия формируется из числа лиц, имеющих доступ к ПДн. Комиссия состоит из 5 человек. В состав комиссии входят председатель комиссии и члены комиссии. Все члены комиссии при принятии решения обладают равными правами. Председатель комиссии организует работу комиссии.

Проверки осуществляются не реже одного раза в год в соответствии с утвержденным графиком или на основании поступившего письменного заявления о нарушении правил обработки ПДн (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

При осуществлении внутреннего контроля соответствия обработки ПДн установленным требованиям производится проверка:

соблюдения принципов обработки ПДн;

соответствия правовых актов министерства в области ПДн законодательству Российской Федерации;

выполнения государственными гражданскими служащими Новосибирской области и лицами, замещающих должности, не являющиеся должностями государственной гражданской службы Новосибирской области (далее – государственными гражданскими служащими и работниками) министерства требований и правил обработки ПДн в информационных системах персональных данных (далее – ИСПДн);

актуальности информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн;

правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой ИСПДн;

актуальности перечня должностей должностных лиц, уполномоченных на обработку ПДн, имеющих доступ к ПДн;

соблюдения прав субъектов ПДн, чьи ПДн обрабатываются в ИСПДн;

соблюдения обязанностей оператора ПДн, предусмотренных законодательством Российской Федерации в области ПДн;

порядка взаимодействия с субъектами ПДн, ПДн которых обрабатываются в ИСПДн, в том числе соблюдения сроков, предусмотренных законодательством Российской Федерации в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам ПДн необходимой информации, порядка реагирования на обращения (запросы) субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами ПДн;

наличия необходимых согласий субъектов ПДн, чьи ПДн обрабатываются в ИСПДн;

актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) ПДн;

актуальности перечня ИСПДн;

знания и соблюдения государственными гражданскими служащими и работниками министерства положений законодательства Российской Федерации в области ПДн, правовых актов министерства;

соблюдения государственными гражданскими служащими и работниками министерства конфиденциальности ПДн;

соблюдения государственными гражданскими служащими и работниками министерства требований по обеспечению безопасности ПДн;

наличия и актуальности локальных актов, технической и эксплуатационной документации технических и программных средств ИСПДн.

5. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за проведение проверки, докладывает министру науки и инновационной политики Новосибирской области (далее – министр).

При проведении внутреннего контроля на ИСПДн составляется протокол контроля выполнения требований по обеспечению безопасности информации, содержащей сведения ограниченного доступа, при ее автоматизированной обработке на автоматизированном рабочем месте по форме согласно приложению к настоящим Правилам.

Оценка соотношения вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

6. Во время осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям производится соответствие оценки соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн в министерстве.

При оценке соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн, для каждой ИСПДн производится экспертное сравнение заявленной оценки вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области ПДн и настоящими Правилами.

Оценка соотношения вреда, который может быть причинен субъектам ПДн в случае нарушения требований по обработке и обеспечению безопасности ПДн и принимаемых мер по обработке и обеспечению безопасности ПДн, оформляется в виде отдельного документа, подписывается заместителем министра и утверждается министром.