УТВЕРЖДЕНЫ

приказом департамента

имущества и земельных отношений

Новосибирской области

от «\_\_»\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_

Правила  
осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

1. Общие положения
   1. Настоящие Правила осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям (далее ‒ Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», 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», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и определяют порядок и мероприятия, проводимые в рамках внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области (далее – Департамент, оператор) установленным требованиям.
   2. К защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее также – защищаемая информация), обрабатываемой в Департаменте, относится следующая информация:

* персональные данные (далее – ПДн);
* иная защищаемая информация, не содержащая сведения, составляющие государственную тайну, содержащаяся в государственных информационных системах Департамента.
  1. Целью проведения внутреннего контроля является проверка соответствия обработки и обеспечения безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, в Департаменте, требованиям законодательства Российской Федерации, нормативным правовым актам федеральных органов исполнительной власти Российской Федерации в области обработки и обеспечения безопасности защищаемой информации, локальным актам Департамента, регламентирующим вопросы обработки и защиты информации, а также своевременное выявление и предотвращение нарушений процедур обработки и защиты информации.

1. Порядок осуществления внутреннего контроля   
   соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, установленным требованиям
   1. В целях осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, установленным требованиям проводятся:

* контроль условий обработки персональных данных в Департаменте;
* контроль выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в Департаменте.
  1. Организацию и проведение контроля соответствия условий обработки персональных данных установленным требованиям обеспечивает лицо, ответственное за организацию обработки персональных данных в Департаменте.
  2. Организацию и проведение контроля выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в Департаменте, установленным требованиям обеспечивают лица, ответственные за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах Департамента (далее – ответственный за защиту информации).
  3. Плановые проверки соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, установленным требованиям проводятся на основании плана проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Департаменте установленным требованиям (далее – План проведения внутреннего контроля) (Приложение № 1 к настоящим Правилам).
  4. Внеплановые внутренние проверки соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, установленным требованиям проводятся на основании поступившей информации о нарушениях правил обработки и защиты информации в Департаменте. Проведение внеплановой проверки организуется в течение трех рабочих дней со дня поступления информации о нарушениях правил обработки и защиты информации.
  5. Проверки проводятся лицами, ответственными за проведение контрольных мероприятий согласно Плану проведения внутреннего контроля, с привлечением при необходимости иных сотрудников Департамента (в пределах их компетенции) и (или) сотрудников иных организаций, обеспечивающих функционирование информационных систем Департамента (осуществляющих функции системных администраторов), и (или) осуществляющих администрирование (управление) системой защиты информации информационных систем Департамента (осуществляющих функции администраторов информационной безопасности).
  6. Проверки проводятся при непосредственном участии сотрудников Департамента, осуществляющих обработку защищаемой информации, не содержащей сведения, составляющие государственную тайну.
  7. Контроль соответствия условий обработки персональных данных установленным требованиям осуществляется непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест работников Департамента, участвующих в процессе обработки персональных данных.
  8. Контроль выполнения мероприятий по обеспечению безопасности защищаемой информации может осуществляться с использованием стандартных процедур документальной проверки, опроса пользователей и ответственных лиц, а также с применением как специализированных средств (например, средств защиты информации, средств анализа защищенности), так и штатных средств операционных систем и иных программных продуктов (в том числе средств регистрации действий пользователей и процессов, журналов регистрации событий безопасности).
  9. При осуществлении внутреннего контроля соответствия условий обработки ПДн установленным требованиям производится проверка:
* соблюдения принципов обработки ПДн, законности целей обработки ПДн;
* соблюдения прав субъектов ПДн, чьи ПДн обрабатываются оператором,
* соблюдение обязанностей оператора, предусмотренных действующим законодательством в области ПДн;
* изменений правил обработки и защиты ПДн;
* соответствия состава и содержания локальных актов оператора в области обработки и защиты персональных данных действующему законодательству Российской Федерации;
* выполнения сотрудниками оператора требований и правил обработки ПДн;
* актуальности перечня лиц, уполномоченных на обработку ПДн и имеющих доступ к ПДн;
* санкционирования и учета физического доступа в помещения и сооружения, в которых размещены информационные системы Департамента и ведется обработка персональных данных;
* порядка взаимодействия с субъектами, ПДн которых обрабатываются оператором;
* наличия необходимых согласий субъектов, чьи ПДн обрабатываются оператором;
* актуальности сведений, содержащихся в уведомлении об обработке (о намерении осуществлять обработку) ПДн;
* актуальности перечня информационных систем Департамента;
* знания и соблюдения сотрудниками оператора положений действующего законодательства Российской Федерации в области обработки и защиты информации, локальных актов оператора;
* подписания сотрудниками Департамента обязательств о соблюдении конфиденциальности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и обязательств о прекращении обработки персональных данных в случае расторжения с ними служебного контракта (трудового договора);
* актуальности 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 Департаменте.
  1. В ходе контроля выполнения мероприятий по обеспечению безопасности защищаемой информации осуществляются:
* контроль за проведением анализа угроз безопасности защищаемой информации;
* контроль за обеспечением управления (администрирования) системой защиты информации информационных систем Департамента, в которых осуществляется обработка защищаемой информации;
* контроль за обеспечением управления конфигурацией информационных систем Департамента, в которых осуществляется обработка защищаемой информации, и их системой защиты информации;
* контроль за реализацией процедур реагирования на инциденты информационной безопасности;
* контроль за проведением информирования и обучения персонала информационных систем Департамента, в которых осуществляется обработка защищаемой информации, по вопросам защиты информации;
* контроль за обеспечением требуемого уровня защищенности информации, обрабатываемых в информационных системах Департамента.
  1. В целях документирования результатов контроля условий обработки ПДн в Департаменте установленным требованиям лицо, ответственное за организацию обработки ПДн в Департаменте, составляют отчет с указанием мер, необходимых для устранения выявленных нарушений, по форме, приведенной в Приложении № 2 к настоящим Правилам.
  2. В целях документирования результатов контроля выполнения мероприятий по обеспечению безопасности защищаемой информации, обрабатываемой в Департаменте, ответственный за защиту информации составляет Протокол контроля за выполнением требований по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Департаменте по форме, приведенной в Приложении № 3 к настоящим Правилам.
  3. Сведения о проведении внутреннего контроля соответствия обработки защищаемой информации в Департаменте установленным требованиям заносятся в Журнал проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Департаменте установленным требованиям (далее – Журнал) (типовая форма Журнала приведена в Приложении № 4 к настоящим Правилам). Ведение Журнала осуществляется в пределах своих полномочий лицом, ответственным за организацию обработки ПДн в Департаменте, и ответственным за защиту информации в Департаменте.
  4. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, лицо, ответственное за организацию обработки ПДн в Департаменте, и ответственный за защиту информации в Департаменте в пределах своей компетенции докладывают руководителю или лицу, его замещающему.

Приложение № 1

к Правилам осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

План проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

1. Контроль условий обработки персональных данных в Департаменте имущества и земельных отношений Новосибирской области

Перечень мероприятий, проводимых в рамках внутреннего контроля соответствия условий обработки персональных данных (далее – ПДн) в департаменте имущества и земельных отношений Новосибирской области (далее – Департамент, оператор) установленным требованиям, их периодичность и ответственные исполнители приведены в Таблице 1.

Таблица 1 – Перечень мероприятий, проводимых в рамках внутреннего контроля соответствия условий обработки ПДн

| **№ п/п** | **Периодичность** | **Мероприятие** | **Ответственный исполнитель** |
| --- | --- | --- | --- |
| 1. 1. | Не реже одного раза в год | Контроль актуальности положений Политики в отношении обработки ПДн, соблюдения прав субъектов ПДн, чьи ПДн обрабатываются в ИС Департамента, и обязанностей оператора, предусмотренных действующим законодательством в области ПДн | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 2. | Не реже одного раза в год | Контроль изменений правил обработки и защиты ПДн (принципов, целей обработки ПДн, состава и количества субъектов ПДн и состава ПДн, обрабатываемых в Департаменте, способов обработки ПДн и актуальности ранее установленного уровня защищенности ПДн пр.) | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 3. | Не реже одного раза в год | Контроль состава и соответствия содержания локальных актов Департамента в области обработки и защиты ПДн действующему законодательству Российской Федерации | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 4. | Не реже одного раза в год | Контроль выполнения сотрудниками Департамента требований и правил обработки ПДн (правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), блокирования, удаления, уничтожения ПДн) | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 5. | Не реже одного раза в год | Контроль актуальности перечня лиц, уполномоченных на обработку ПДн и имеющих доступ к ПДн | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 6. | Не реже одного раза в год | Контроль санкционирования и учета физического доступа в помещения и сооружения, в которых размещены информационные системы Департамента и ведется обработка ПДн (контроль актуальности Перечня лиц, имеющих доступ в помещения, в которых размещены информационные системы Департамента и ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну; контроль выдачи и наличия ключей от помещений; контроль соблюдения порядка доступа в помещения, в которых, в которых размещены информационные системы Департамента и ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну) | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 7. | Не реже одного раза в год | Контроль соблюдения порядка взаимодействия с субъектами ПДн (в том числе соблюдения сроков, предусмотренных действующим законодательством 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) | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 8. | Не реже одного раза в год | Контроль наличия необходимых согласий субъектов, чьи ПДн обрабатываются в Департаменте | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 9. | В случае изменения сведений, указанных в уведомлении об обработке ПДн, а также в случае прекращения обработки ПДн в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн | Контроль актуальности сведений, содержащихся в уведомлении об обработке ПДн | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 10. | Не реже одного раза в год | Контроль подписания сотрудниками Департамента обязательств о соблюдении конфиденциальности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и обязательств о прекращении обработки персональных данных в случае расторжения с ними служебного контракта (трудового договора) | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 11. | Не реже одного раза в год | Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн и локальными актами Департамента по вопросам обработки ПДн, а также знания и соблюдения ими требований и положений вышеуказанных документов | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 12. | Не реже одного раза в год | Контроль за уничтожением ПДн, а также электронных (бумажных) носителей ПДн | Ответственный за организацию обработки ПДн в Департаменте |
| 1. 13. | Не реже одного раза в год | Контроль соответствия 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 Департаменте | Ответственный за организацию обработки ПДн в Департаменте |

1. Контроль выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в Департаменте имущества и земельных отношений Новосибирской области

Перечень проверок, осуществляемых в рамках контроля выполнения мероприятий по обеспечению безопасности защищаемой информации (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну, обрабатываемой в Департаменте, их периодичность и ответственные исполнители, приведены в Таблице 2.

Таблица 2 – Перечень проверок, осуществляемых в рамках контроля выполнения мероприятий по обеспечению безопасности защищаемой информации

| **№ п/п** | **Периодичность** | **Мероприятие** | **Ответственный исполнитель** |
| --- | --- | --- | --- |
| 1. 1. | Контроль за проведением анализа угроз безопасности информации | | |
| 1. 1.1. | Не реже одного раза в 2 года | Контроль проведения периодического выявления, анализа и устранения уязвимостей ИС | Ответственный за защиту информации, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах (далее – ИС) Департамента (далее – ответственный за защиту информации) |
| 1. 1.2. | Не реже одного раза в 2 года | Контроль проведения периодического анализа изменения угроз безопасности информации в ИС, возникающих в ходе их эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации | Ответственный за защиту информации |
| 1. 2. | Контроль за обеспечением управления (администрирования) системой защиты информации | | |
| 1. 2.1. | Не реже одного раза в 2 года | Контроль закрепления в организационно-распорядительных документах (далее – ОРД по защите информации) порядка осуществления следующих мероприятий в рамках управления (администрирования) системой защиты информации:   * управления учетными записями пользователей и правилами разграничения доступа в ИС; * управления средствами защиты информации ИС; * управления обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации; * порядка мониторинга и анализа зарегистрированных событий в ИС, связанных с обеспечением безопасности | Ответственный за защиту информации |
| 1. 2.2. | Не реже одного раза в 2 года | Контроль ведения и актуализации эксплуатационной документации (технических паспортов ИС Департамента) и ОРД по защите информации | Ответственный за защиту информации |
| 1. 3. | Контроль за обеспечением управления конфигурацией ИС и их системами защиты информации | | |
| 1. 3.1. | Не реже одного раза в 2 года | Контроль определения в ОРД по защите информации объектов управления конфигурацией и процедур управления изменениями ИС и их систем защиты | Ответственный за защиту информации |
| 1. 3.2. | Не реже одного раза в 2 года | Контроль документирования изменений в конфигурации ИС Департамента и их систем защиты информации: состава, мест установки и параметров настройки программно-аппаратных, программных средств, включая средства защиты информации (контроль внесения информации (данных) в технические паспорта ИС, протоколы настройки средств защиты информации, перечень разрешенного к использованию программного обеспечения и пр.) | Ответственный за защиту информации |
| 1. 4. | Контроль за реализацией процедур реагирования на инциденты безопасности | | |
| 1. 4.1. | Не реже одного раза в 2 года | Контроль закрепления в ОРД по защите информации порядка обнаружения инцидентов и информирования ответственных лиц о возникновении инцидентов безопасности, а также порядка реагирования на инциденты безопасности | Ответственный за защиту информации |
| 1. 5. | Контроль за проведением информирования и обучения персонала ИС по вопросам защиты информации | | |
| 1. 5.1. | Не реже одного раза в год | Контроль информирования персонала о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС | Ответственный за защиту информации |
| 1. 5.2. | Не реже одного раза в год | Контроль доведения до персонала ИС требований по защите информации, а также положений ОРД по защите информации | Ответственный за защиту информации |
| 1. 5.3. | Не реже одного раза в год | Контроль обучения персонала ИС правилам эксплуатации отдельных средств защиты информации | Ответственный за защиту информации |
| 1. 5.4. | Не реже одного раза в год | Проверка проведения контроля осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации | Ответственный за защиту информации |
| 1. 6. | Контроль за обеспечением уровня защищенности информации, содержащейся в ИС | | |
| 1. 6.1. | Контроль (анализ) защищенности информации ИС | | |
| 1. 6.1.1. | Не реже одного раза в 2 года | Контроль установки обновлений программного обеспечения (общесистемного, прикладного, программных средств защиты информации), в том числе проверка обновлений баз применяемых в ИС средств защиты информации (для средств антивирусной защиты и средств анализа защищенности) | Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности1, и лиц, осуществляющих функции  системных администраторов2) |
| 1. 6.1.2. | Не реже одного раза в 2 года | Проверка проведения контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| 1. 6.1.3. | Не реже одного раза в 2 года | Проверка проведения контроля состава технических средств, программного обеспечения и средств защиты информации |
| 1. 6.1.4. | Не реже одного раза в год | Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации | Ответственный за защиту информации |
| 1. 6.1.5. | Не реже одного раза в 2 года | Контроль реализации мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны | Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности) |
| 1. 6.1.6. | Не реже одного раза в 2 года | Контроль соблюдения правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей ИС Департамента | Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности, и лиц, осуществляющих функции  системных администраторов) |
| 1. 6.2. | Анализ и оценка функционирования системы защиты информации ИС, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС | | |
| 1. 6.2.1. | Не реже одного раза в год | Контроль наличия технической и эксплуатационной документации на технические и программные средства, применяемые в ИС | Ответственный за защиту информации |
| 1. 6.2.2. | Не реже одного раза в год | Контроль проведения процедур уничтожения (стирания) защищаемой информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации | Ответственный за защиту информации |
| 1. 6.2.3. | Не реже одного раза в год | Контроль поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним | Ответственный за защиту информации |
| 1. 6.2.4. | Не реже одного раза в год | Контроль учёта машинных носителей информации | Ответственный за защиту информации |
| 1. 6.2.5. | Не реже одного раза в 2 года | Проверка проведения контроля безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование | Ответственный за защиту информации (с привлечением лиц, осуществляющих функции администратора информационной безопасности, и лиц, осуществляющих функции  системных администраторов) |
| 1. 6.2.6. | Не реже одного раза в 2 года | Проверка проведения контроля работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий | Ответственный за защиту информации (с привлечением лиц, осуществляющих функции системных администраторов, лиц, осуществляющих процедуру резервного копирования) |
| 1. 6.2.7. | В режиме мониторинга в ходе эксплуатации ИС | Контроль проведения периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов) | Ответственный за защиту информации |
| 1. 6.2.8. | Не реже одного раза в 2 года | Пересмотр перечня событий безопасности, подлежащих регистрации в ИС | Ответственный за защиту информации |
| 1. 6.2.9. | Не реже одного раза в год | Проверка расположения средств отображения информации | Ответственный за защиту информации |
| 1. 7. | В случае вывода из эксплуатации ИС или после принятия решения об окончании обработки информации | Контроль за обеспечением защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации | Ответственный за защиту информации |

1 Администраторами информационной безопасности являются лица, осуществляющие администрирование (управление) системой защиты информации ИС Департамента, назначенные из числа сотрудников Департамента, и (или) являющиеся сотрудниками иных организаций, привлекаемых к выполнению работ по защите информации на договорной основе

2 Системными администраторами являются лица, обеспечивающие функционирование ИС Департамента, назначенные из числа сотрудников Департамента, и (или) являющиеся сотрудниками иных организаций

Приложение № 2

к Правилам осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Департаменте имущества и земельных отношений Новосибирской области установленным требованиям

Отчет о результатах контроля соответствия условий обработки персональных данных в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

1. Характеристика объекта контроля
   1. Наименование объекта контроля1: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   2. Адрес размещения объекта контроля:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Категория персональных данных, обрабатываемых на объекте контроля:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Уровень защищенности персональных данных при их обработке на объекте контроля: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Метод проведения контроля2:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. В ходе проверки были проведены следующие мероприятия3:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Результаты проведения проверки:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Меры по устранению выявленных нарушений (при их наличии):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В проведении контроля участвовали:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | |
| должность |  | подпись |  | фамилия, инициалы | |
|  |  |  |  |  | |
| должность |  | подпись |  | фамилия, инициалы | |
|  |  |  |  |  | |
| должность |  | подпись |  | фамилия, инициалы | |
| Дата проведения контроля: | | | | |  |
| (число, месяц, год) |

1 Указывается наименование структурного подразделения и (или) наименование информационной системы

2 Экспертно-документальный/инструментальный

3 Перечисляются мероприятия, проводимые в рамках внутреннего контроля соответствия условий обработки персональных данных, в соответствии с Планом проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

Приложение № 3

к Правилам осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

Протокол контроля за выполнением требований по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области

1. Характеристика объекта контроля
   1. Наименование информационных(ой) систем(ы): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
   2. Адрес размещения объекта контроля:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Класс защищенности информационных(ой) систем(ы):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Метод проведения контроля1:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Контроль проводился на соответствие требованиям по защите информации, установленным:

* *постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;*
* *приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».*

1. Сведения о проводимых в ходе контроля мероприятиях и результатах проверок:

|  |  |  |
| --- | --- | --- |
| № п/п | Мероприятия по контролю2 | Результаты проведения проверки |
|  |  |  |

1. Меры по устранению выявленных нарушений (при их наличии):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

В проведении контроля участвовали:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | |
| должность |  | подпись |  | фамилия, инициалы | |
|  |  |  |  |  | |
| должность |  | подпись |  | фамилия, инициалы | |
| Дата проведения контроля: | | | | |  |
| (число, месяц, год) |

1 Экспертно-документальный/инструментальный

2 Перечисляются мероприятия, проводимые в рамках контроля за выполнением мероприятий по обеспечению безопасности защищаемой информации в соответствии с Планом проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Департаменте имущества и земельных отношений Новосибирской области установленным требованиям

Приложение № 4

к Правилам осуществления внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

ЖУРНАЛ  
проведения внутреннего контроля соответствия обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в департаменте имущества и земельных отношений Новосибирской области установленным требованиям

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Дата проведения контроля** | **Краткое содержание мероприятий по контролю** | **Исполнитель (ФИО, подпись)** | **Примечание** |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |