**ПРИКАЗ**

|  |  |  |
| --- | --- | --- |
| № \_\_\_\_\_\_\_\_\_\_\_ | г. Белгород | «\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. |

|  |
| --- |
| **Об ответственном за обеспечение безопасности**  **персональных данных в информационных системах**  **персональных данных *<наименование учреждения>*** |

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказываю:

Для обеспечения уровня защищенности персональных данных при их обработке в информационных системах персональных данных, определенного в отдельных нормативных актах *<наименование учреждения>*, назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных *<наименование учреждения>* *<должность> <ФИО>*.

1. Утвердить прилагаемую инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных *<наименование учреждения>*.
2. Ответственного за обеспечение безопасности персональных данных ознакомить по роспись с настоящим приказом и прилагаемой инструкцией.

Контроль за исполнением настоящего приказа оставляю за собой.

|  |  |
| --- | --- |
| Руководитель учреждения | *<ФИО руководителя>* |

Утверждена

приказом *<наименование учреждения>*

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**ИНСТРУКЦИЯ ответственного за обеспечение безопасности персональных данных**

**в информационных системах персональных данных *<наименование учреждения>***

г. Белгород

20\_\_ г.

1. Общие положения
   1. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных *<наименование учреждения>* (далее – Ответственный) назначается приказом руководителя *<наименование учреждения>* (далее – Учреждение) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Учреждения.
   2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации по защите информации, методические материалы в сфере обработки и защиты ПДн.
   3. В своей деятельности Ответственный руководствуется Политикой в отношении обработки персональных данных в Учреждении, настоящей Инструкцией, рекомендациями Ответственного за организацию обработки персональных данных (далее – Ответственный за организацию обработки ПДн), нормативными и методическими документами государственных регуляторов в области обеспечения информационной безопасности ПДн.
   4. Методическое руководство работой Ответственного осуществляет Ответственный за организацию обработки ПДн.
2. Основные функции и обязанности ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

**Функции Ответственного:**

* 1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:
     + проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;
     + подготовка решений в отношении сведений о работах, выполняемых Учреждением, подлежащих защите;
     + рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите ПДн, при научных исследованиях, при проведении других работ;
     + координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;
     + проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;
     + подготовка предложений по совершенствованию действующей системы защиты ПДн с последующим предоставлением Ответственному за организацию обработки ПДн Учреждения и/или руководителю Учреждения;
     + учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;
     + обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
     + осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

**Ответственный обязан:**

* 1. Соблюдать требования действующих нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн при их обработке в ИСПДн.
  2. Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн.
  3. Осуществлять общее техническое сопровождение ИСПДн:
     + контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;
     + контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;
     + вести журнал учета и выдачи используемых материальных носителей ПДн;
     + контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;
     + проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Учреждения (далее – Пользователи ИСПДн) по правилам работы в ИСПДн.
  4. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:
     + реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИСПДн;
     + назначать пароли Пользователей ИСПДн;
     + контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;
     + своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника;
     + вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;
     + регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;
     + своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД.
  5. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:
     + обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Учреждения;
     + обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;
     + обеспечивать регулярное и своевременное создание резервных копий ИСПДн Учреждения;
     + осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн.
  6. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн.
  7. Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
  8. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.
  9. Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн.
  10. Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных Учреждения, а также установленных требований для обеспечения уровней защищенности ПДн.
  11. Контролировать работу Пользователей ИСПДн в сетях общего пользования и (или) международного обмена.
  12. Контролировать правильность применения Пользователями ИСПДн средств защиты информации.
  13. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий.
  14. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:
      + антивирусного программного обеспечения;
      + средств защиты от несанкционированного доступа.
  15. В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.
  16. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

1. Права и ответственность ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

**Ответственный имеет право:**

* 1. Знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки и защиты ПДн.
  2. Вносить предложения руководителю Учреждения по совершенствованию существующей системы защиты информации.
  3. Привлекать по согласованию с Ответственным за организацию обработки ПДн и руководителем Учреждения к работе по созданию и совершенствованию системы защиты ПДн других сотрудников Учреждения.
  4. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных Учрежденияи иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн.
  5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн.
  6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн.
  7. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн.
  8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

**Ответственный несет ответственность за:**

* 1. Программно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно-вычислительные комплексы, сети и автоматизированные системы обработки информации.
  2. Качество проводимых им работ по контролю действий Пользователей ИСПДн при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.
  3. Разглашение персональных данных, ставших известными ему по роду работы согласно действующему законодательству РФ.

**Лист ознакомления**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | ФИО | Должность | Подпись, дата |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |