Приложение № 3 к приказу

от 25.08.2015 №34

**Правила осуществления внутреннего контроля**

**соответствия обработки персональных данных требованиям к защите персональных данных в управлении административных органов Липецкой области**

1. **Общие положения**
   1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в управлении административных органов Липецкой области (далее – Правила) определяют план и порядок проведения внутренних проверок организации обработки и защиты персональных данных субъектов персональных данных (далее – субъекты) в управлении административных органов Липецкой области (далее – Управление).
   2. Целью внутренних проверок является определение соответствия порядка обработки и защиты персональных данных субъектов действующему законодательству, локальным актам Управления по вопросам обработки персональных данных, а также локальных актов, направленных на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.
   3. Основные понятия, используемые в настоящих Правилах, соответствуют основным понятиям, установленным Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1. **План проведения внутренних проверок**
   1. План содержит перечень внутренних проверок и определяет для каждой из них:

* название проверки;
* периодичность проведения проверки;
* методику (программу) проверки
* ответственного исполнителя.
  1. Внутренние проверки проводятся в структурных подразделениях Управления, обрабатывающих персональные данные.
  2. Общий срок проведения проверки не должен превышать 30 рабочих дней.
  3. Информация о проведенной проверке, дата ее начала и окончания, а также ее результаты, фиксируется в «Журнале по учету мероприятий по контролю защищенности персональных данных».
  4. План проведения внутренних проверок приведен в Приложении №1 к настоящим Правилам.

1. **Порядок проведения внутренних проверок**
   1. **Порядок проведения анализа и пересмотра существующих мер по обеспечению безопасности персональных данных в информационных системах.**

В ходе проведения проверки необходимо:

* + 1. Определить изменения в базовой конфигурации информационной системы, проверить наличие данных о внесении изменений в документацию на систему защиты информации информационной системы.
    2. Провести анализ произведенных изменений на предмет возникновения дополнительных угроз безопасности информации в информационной системе.
    3. В случае выявления новых источников угроз провести уточнение и дополнение модели угроз безопасности.
    4. Провести соотношение выявленных угроз информационной безопасности с реализованными мерами по защите информации, в случае необходимости применить дополнительные меры по защите.
    5. По результатам анализа изменённой модели угроз и выбора необходимых дополнительных мер по обеспечению безопасности – принять решение об обновлении либо модернизации системы защиты информации.
    6. Принять решение о необходимости переаттестации информационной системы или проведении дополнительных аттестационных испытаний.
  1. **Порядок проведения проверки наличия и актуальности внутренней нормативной документации в области обработки и защиты персональных данных.**

В ходе проведения проверки необходимо:

* + 1. Проверить наличие в организации и соответствие действующему законодательству РФ необходимой внутренней нормативной базы, регулирующей вопросы обработки и защиты персональных данных.
    2. Проверить наличие доказательств ознакомления работников организации:
* с правилами обработки персональных данных субъектов;
* с другими внутренними нормативными документами (приказами, инструкциями и т.п.), регулирующими обработку и защиту персональных данных субъектов в Управлении административных органов Липецкой области.
  + 1. Проверить наличие письменных обязательств о неразглашении персональных данных субъекта и соблюдении правил их обработки работников, допущенных к обработке персональных данных.
    2. Проверить наличие обязательства о неразглашении информации, содержащей персональные данные субъектов в договорах со сторонними организациями.
    3. Результаты проверки оформляются в виде Акта (составляется в произвольной форме), который содержит:
* описание нарушений и недостатков, выявленных в процессе проверки;
* предложения и рекомендации по снижению рисков, устранению недостатков и повышению эффективности внутреннего контроля.
  1. **Порядок проведения проверки соблюдения режима обработки персональных данных в структурных подразделениях Управления**

В ходе проведения проверки необходимо:

* + 1. Установить какие работники структурного подразделения участвуют в процессе обработки персональных данных.
    2. Определить все ли работники, фактически участвующие в обработке персональных данных, допущены к обработке согласно распоряжению.
    3. Определить доведены ли до работников, участвующих в обработке персональных данных, установленные в Управлении правила работы с ПДн, а также меры по обеспечению безопасности персональных данных при их обработке.
    4. Определить соблюдают ли указанные выше работники, установленные правила обработки персональных данных.
    5. Результаты проверки оформляются в виде Акта (составляется в произвольной форме), в котором дается характеристика проверенного подразделения, указываются выявленные нарушения, их причины, возможные последствия, а также другие сведения, делаются выводы и предложения.
  1. **Порядок проведения проверки соблюдения режима защиты персональных данных при их обработке в информационных системах.**

В ходе проведения проверки необходимо:

* + 1. Произвести проверку функционирования и выполнения требований по эксплуатации средств защиты информации.
    2. Проверить ведение журнала регистрации событий безопасности.
    3. Проверить наличие и ведение журналов, используемых для контроля (анализа) защищенности информации ограниченного доступа.
    4. Произвести контроль над выполнением резервного копирования и архивирования информации ограниченного доступа.
    5. Произвести контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена.
    6. Произвести контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационной системы.
    7. Произвести контроль за внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение, специально дорабатываемое собственными разработчиками или сторонними организациями.
    8. Результаты проверки оформляются в виде Акта (составляется в произвольной форме), который содержит:

– выявленные нарушения и их причины;

– принятые меры по устранению нарушений и предложения по их предотвращению.