Приложение 5
к приказу руководителя
Организации
от __ №____

Инструкция по работе администратора информационной безопасности
в *Организации*

Раздел I
Общие положения

1. Администратор информационной безопасности (далее - АИБ) в *Организации* назначается из числа сотрудников *Организации* приказом руководителя *Организации* и отвечает за обеспечение требуемого уровня защищенности персональных данных при их обработке в информационных системах персональных данных в *Организации* (далее - ИСПДн).

2. АИБ в своей работе руководствуется требованиями руководящих документов по обеспечению безопасности персональных данных, положениями нормативных правовых актов, приказами, а также положениями настоящей Инструкции.

3. АИБ является лицом, обеспечивающим безопасность персональных данных, обрабатываемых, передаваемых и хранимых в ИСПДн.

4. Методическое руководство работой АИБ осуществляется ответственным за организацию обработки персональных данных в *Организации*.

Раздел II
Обязанности администратора информационной безопасности

5. АИБ обязан:

1) четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по обеспечению безопасности персональных данных при их обработке в ИСПДн и актов, регламентирующих порядок действий по обеспечению безопасности персональных данных;

2) управлять средствами защиты информации (далее - СЗИ) ИСПДн и поддерживать их функционирование;

3) восстанавливать функции программных и технических СЗИ от несанкционированного доступа (далее - НСД) к информации;

4) обеспечивать функционирование ИСПДн в пределах возложенных функций;

5) генерировать ключи, личные идентификаторы, а также пароли для пользователей ИСПДн;

6) устанавливать порядок смены пароля для аутентификации пользователя ИСПДн – не реже чем каждые 45 (сорок пять) дней;

7) формировать и управлять списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;

8) назначать права доступа, полномочия и привилегии пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода);

9) обеспечивать правильную эксплуатацию технических и программных СЗИ в ИСПДн, проводить настройки СЗИ в соответствии с эксплуатационной документацией;

10) контролировать целостность эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;

11) выявлять, анализировать и устранять уязвимости и иные недостатки в программном обеспечении;

12) в случае нарушения работоспособности (отказе) технических средств и/или программного обеспечения ИСПДн, в том числе СЗИ, немедленно докладывать о случившемся ответственному за организацию обработки персональных данных в *Организации*;

13) осуществлять текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации;

14) выполнять и контролировать выполнение установленного комплекса мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн;

15) проводить инструктаж и консультации пользователей ИСПДн по соблюдению установленного режима конфиденциальности при обработке персональных данных в ИСПДн;

16) контролировать соблюдение пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн по вопросам защиты информации от НСД;

17) взаимодействовать с ответственным за организацию обработки персональных данных в *Организации* по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн и соблюдении прав доступа пользователей к ней;

18) выполнять и учитывать изменения, вносимые:

– в списки пользователей ИСПДн;

– в перечень защищаемых информационных ресурсов ИСПДн;

19) контролировать выполнение утвержденной технологии обработки персональных данных в ИСПДн;

20) контролировать состав технических средств, программного обеспечения и СЗИ, целостности системных файлов ОС средствами СЗИ от НСД;

21) контролировать установку и обновление программного обеспечения, запрет установки неразрешённого программного обеспечения (в том числе

средств обработки и отладки);

22) выявлять подозрительные действия пользователей и попытки НСД к персональным данным, обрабатываемым в ИСПДн, путем анализа системных журналов информационной безопасности при работе в ИСПДн;

23) выполнять резервное копирование электронных документов, содержащих персональные данные, осуществлять контроль результатов всех процедур резервного копирования;

24) обучать и консультировать пользователей ИСПДн правилам работы с СЗИ от НСД;

25) проводить антивирусную защиту информации и программных средств в ИСПДн;

26) контролировать электронный журнал сообщений и обеспечивать доступ к нему лиц, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

27) просматривать и анализировать результаты регистрации событий, относящихся к безопасности персональных данных, и реагировать на них, обеспечить защиту регистрируемой информации средствами компонент идентификации и аутентификации, управления доступом СЗИ;

28) контролировать безотказное функционирование технических и программных средств, а также СЗИ, принимать меры по восстановлению отказавших средств;

29) обеспечивать строгое выполнение требований по обеспечению безопасности персональных данных в *Организации* при обслуживания технических средств ИСПДн и отправке их в ремонт;

30) обеспечивать соответствие состава ИСПДн техническому паспорту на ИСПДн (в т. ч. реальной конфигурации информационных связей).

Раздел III
Права администратора информационной безопасности

6. АИБ имеет право:

1) требовать от пользователей ИСПДн выполнения установленной технологии обработки персональных данных, инструкций и других документов по обеспечению безопасности персональных данных;

2) участвовать в разработке мероприятий в *Организации* по совершенствованию безопасности персональных данных;

3) останавливать обработку персональных данных в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки персональных данных, приводящих к нарушению функционирования СЗИ, или выявления инцидентов безопасности, немедленно докладывать о случившемся ответственному за организацию обработки персональных данных в *Организации*;

4) подавать свои предложения по совершенствованию технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн *Организации*.