**П Р И К А З**

**от\_\_\_\_\_\_\_\_№ \_\_\_\_**

**О защите информации**

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012   
№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

**ПРИКАЗЫВАЮ:**

1. Возложить обязанности по защите информации:
   1. Назначить ответственным за организацию обработки персональных данных ФИО (обычно замдир отвечает за обработку всех ПДн в бумажном и электронном виде)
   2. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных ФИО (назначается технически грамотный и обученный сотрудник)
   3. Назначить ответственным за эксплуатацию ИС ФИО (назначается технически грамотный и обученный сотрудник)
   4. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно [приложению 1](#Пр1) к настоящему приказу.
   5. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации согласно [приложению 2](#Пр2) к настоящему приказу.
2. Создать комиссию по защите информации:
   1. Утвердить состав комиссии по защите информации согласно [приложению 3](#Пр4) к настоящему приказу.
   2. Утвердить положение о комиссии по защите информации согласно [приложению 4](#Пр5) к настоящему приказу.
3. Утвердить типовые формы документов по защите информации:
   1. Согласие на обработку персональных данных согласно [приложению 6](#Пр6) к настоящему приказу.
   2. Разъяснение субъекту персональных данных согласно [приложению 7](#Пр7) к настоящему приказу.
   3. Обязательство о неразглашении информации, содержащей персональные данные, согласно [приложению 8](#пр8) к настоящему приказу.
   4. Журналы по защите информации согласно [приложению 9](#Пр9) к настоящему приказу.
   5. Протокол заседания комиссии по защите информации согласно [приложению 10](#Пр10) к настоящему приказу.
   6. Акт об уничтожении персональных данных субъектов персональных данных согласно [приложению 11](#Пр12) к настоящему приказу.
4. Утвердить перечень информационных систем персональных данных согласно [приложению 12](#Пр12) к настоящему приказу.
5. Утвердить перечень обрабатываемых персональных данных согласно [приложению 13](#Пр13) к настоящему приказу.
6. Утвердить Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения согласно [приложению 14](#Пр14) к настоящему приказу.
7. Утвердить политику в отношении обработки персональных данных согласно [приложению 15](#Пр15).
8. Утвердить инструкции и правила по защите информации:

* Инструкцию ответственного за организацию обработки персональных данных согласно [приложению 16](#Пр16) к настоящему приказу.
* Правила рассмотрения запросов субъектов персональных данных согласно [приложению 17](#Пр17) к настоящему приказу.
* Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей, согласно [приложению 18](#Пр18) к настоящему приказу;
* Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных согласно [приложению 19](#Пр19) к настоящему приказу;
* Инструкцию по организации резервного копирования, согласно [приложению 20](#Пр20) к настоящему приказу;
* Инструкцию по организации парольной защиты, согласно   
  [приложению 21](#Пр21) к настоящему приказу;
* Инструкцию по организации антивирусной защиты, согласно   
  [приложению 22](#Пр22) к настоящему приказу;
* Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно [приложению 23](#Пр24) к настоящему приказу;
* Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, согласно [приложению 24](#Пр25) к настоящему приказу;
* Инструкцию о пропускном и внутриобъектовом режимах согласно [приложению 25](#Пр27) к настоящему приказу;
* Инструкцию по обработке персональных данных без использования средств автоматизации согласно [приложению 26](#Пр28) к настоящему приказу;
* Инструкцию по работе с инцидентами информационной безопасности согласно [приложению 27](#Пр31) к настоящему приказу;
* Инструкцию ответственного за эксплуатацию информационных систем персональных данных согласно [приложению 28](#Пр31) к настоящему приказу.

1. Утвердить план мероприятий по защите информации согласно [приложению 29](#Пр32) к настоящему приказу.

|  |  |
| --- | --- |
| **Директор** | **ФИО** |

Исполнитель: Ф.И.О.

т .8 (0000) 000000

[Приложение 1](#П2О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

|  |  |
| --- | --- |
| Должность | ИСПДн  Примеры: |
| Директор |  |
| Заместитель директора | ФИС ФРДО |
| Учитель | Электронная школа |
|  |  |
|  |  |
|  |  |
|  |  |

[Приложение 2](#П2О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

|  |
| --- |
| Должность |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

[Приложение 3](#П3О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Состав комиссии по защите информации

|  |  |
| --- | --- |
| Председатель комиссии | ФИО, должность |
| Члены комиссии | ФИО, должность |
| ФИО, должность |
| ФИО, должность |

[Приложение 4](#П4О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПОЛОЖЕНИЕ   
о комиссии по защите информации

1. Общие положения
   1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.
2. Основные задачи комиссии
   1. Основными задачами комиссии являются:
      1. Сбор и анализ исходных данных по информационным системам персональных данных Наименование организации.
      2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Комиссия должна провести классификацию ИС и определить уровень защищённости (УЗ) персональных данных. Презентации и лекции на эту тему можно найти в интернете

* + 1. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
    2. Определение класса защищенности информационных систем персональных данных Наименование организации на основании собранных данных.
    3. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

1. Порядок формирования комиссии
   1. Комиссия формируется из числа штатных сотрудников Наименование организации, участвующих в процессе обработки персональных данных.
   2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.
   3. Члены комиссии назначаются приказом директора Наименование организации.
   4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.
2. Полномочия комиссии
   1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:
      1. Получать необходимые сведения у всех работников Наименование организации, участвующих в обработке персональных данных.
      2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.
      3. Отслеживать технологический процесс обработки персональных данных.
      4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети Наименование организации.
      5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.
      6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.
      7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.
3. Отчетность комиссии
   1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.
   2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

[Приложение 6](#П5О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

СОГЛАСИЕ    
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(*ФИО)*

паспорт \_\_\_\_\_\_\_\_\_\_\_ выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

*(серия, номер)                                                                        (когда и кем выдан)*

адрес регистрации:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

даю свое согласие на обработку в  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия, имя, отчество; пол; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство.

Я даю согласие на использование персональных данных исключительнов целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также на хранение данных об этих результатах на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я проинформирован, что **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему  письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

 "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.                       \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*Подпись                         Расшифровка подписи*

[Приложение 7](#П6О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Разъяснение  
субъекту персональных данных

Мне, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
разъяснены юридические последствия отказа предоставить свои персональные данные в Наименование организации.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в Наименование организации в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может   
быть заключен.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| дата |  | подпись |  | расшифровка |

[Приложение 8](#П7О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Обязательство  
о неразглашении информации, содержащей персональные данные

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество полностью)

являясь работником Наименование организации, в должности \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| дата |  | подпись |  | расшифровка |

[Приложение 9](#П8О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ЖУРНАЛ  
учета машинных носителей персональных данных (стационарные носители)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер | Тип и ёмкость | Дата и место установки (использования) | Ответственное  должностное лицо (Ф.И.О) |
| пример | s/n | 500 гб | 01.10.2016 | Иванов А.А. |

ЖУРНАЛ  
учета машинных носителей персональных данных (съемные носители)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер | Тип и ёмкость | Получил  (Ф.И.О, дата, подпись) | Сдал  (Ф.И.О, дата, подпись) | Место хранения | Ответственное  должностное лицо (Ф.И.О) |
| пример | s/n | Флэш 16 гб | Галушко Г.А. 01.10.2016 | Иванов А.А. 01.10.2016 | Каб. 206 | Иванов А.А. |

ЖУРНАЛ  
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Сведения о допуске к персональным данным | | | | Сведения о прекращении допуска к персональным данным | |
| Наименование информационной системы персональных данных/способ обработки ПДн | ФИО, должность получившего допуск | Дата и номер приказа о допуске | Дата и подпись допускаемого лица | Дата и номер приказа о прекращении допуска | Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн |
| пример | ФИС ФРДО | Галушко Г.А. | 01-03/25 от 01.10.2016 | \_\_\_\_\_\_\_\_\_ 02.10.2016 | - | - |
| пример | Электронная школа | Йцукен Г.Ш. |  |  |  |  |
|  |  |  |  |  |  |  |

ЖУРНАЛ  
учета средств защиты информации

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Индекс и наименование средства защиты информации | Серийный (заводской) номер | Номер специального защитного знака | Наименование организации, установившей СЗИ | Место установки | Примечание |
| пример | Dallas Lock 8-K | 000-111-222-444 | X0-0001223 | ГБУ НСО «ЦЗИ НСО» | Каб. 206 |  |
| пример | Kaspersky endpoint Protection 11 | 000-111-222-444 | X0-0001223 | ГБУ НСО «ЦЗИ НСО» | Каб. 206 |  |
| пример | Vipnet Client 4.2 | 000-111-222-444 | X0-0001223 | ГБУ НСО «ЦЗИ НСО» | Каб. 206 |  |

ЖУРНАЛ  
учета средств криптографической защиты информации

| № п/п | Наименование  криптосредства,  эксплуатационной  и технической  документации к  ним, ключевых  документов | Регистрационные  номера СКЗИ,  эксплуатационной и  технической  документации к ним,  номера серий  ключевых  документов | Номера экземпляров  (криптографические номера)  ключевых документов | Отметка о получении | | Отметка о выдаче | | Отметка о подключении (установке) СКЗИ | | | Отметка об изъятии СКЗИ из аппаратных средств,  уничтожении ключевых документов | | | Примечания |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| От кого  получены | Дата и номер  сопроводительного письма | Ф.И.О.  пользователя  криптосредств | Дата и  расписка в  получении | Ф.И.О. пользователя  криптосредств,  производившего  подключение  (установку) | Дата  подключения  (установки) и  подписи лиц,  произведших  подключение  (установку) | Номера аппаратных  средств, в которые  установлены или к кот-  рым подключены  криптосредства | Дата изъятия  (уничтожения) | Ф.И.О. пользователя  СКЗИ, производившего  изъятие (уничтожение) | Номер акта или расписка  Об уничтожении |
| ппример | Vipnet Client 4.2 | 000-111-222-444 | X0-0001223 | ГБУ НСО «ЦЗИ НСО» | 01.102016 | Йцукен Г.Ш. |  | Тарасюк И.В. | 01.10.2016 | s/n компьютера | - | - | - |  |
| ппример | Крипто Про 4.0 |  |  |  |  |  |  |  |  |  |  |  |  |  |

ЖУРНАЛ  
учета согласий субъектов персональных данных

|  |  |  |
| --- | --- | --- |
| № п/п | Дата и номер согласия | Ф.И.О. субъекта персональных данных |
| пример | 02.10.2016 | Йцукен Г.Ш. |

ЖУРНАЛ  
учета хранилищ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный (учетный) номер хранилища | Вид хранилища | Дата постановки на учет | Фамилия и подпись принявшего (ответственного), дата | Место расположения (номер помещения) | Дата и номер акта о выводе из эксплуатаци | Примечание |
| пример | Инв. Номер  410100000 | сейф | 10.10.2010 | Йцукен Г.Ш. | Каб 206 | - | - |

ЖУРНАЛ

учета ЭП

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Номера экземпляров ключевых документов | Номера криптографических ключей | Наименование СКЗИ | Отметка о получении | | Отметка о выдаче | | |
| От кого получены (УУЦ) | Дата | ФИО пользователя | Дата | Подпись |
| пример | 1 | 12345 | Крипто- про | «Крипто-софт» | 01.05.2016 |  |  |  |
|  | 1 |  |  |  |  |  |  |  |

ЖУРНАЛ

учета персональных идентификаторов и электронных ключей  
(для администратора зала)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Ф.И.О. | Получил | Дата | Время | Отметка о возврате (подпись администратора) |
| - | - | - | - | - | - |

ЖУРНАЛ

учета выдачи персональных идентификаторов и электронных ключей   
(для администратора информационной безопасности)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Ф.И.О. | № идентификатора | Получил | Дата | Сдал | Отметка о возврате |
| - | - | - | - | - | - | - |

ЖУРНАЛ

учета выдачи паролей

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Дата получения пароля | Ф.И.О. получателя | Подпись получателя |
|  |  | Не обязательный |  |

ЖУРНАЛ

учета обращений субъектов персональных данных по вопросам обработки персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №№ п/п | Дата обращения | ФИО обратившегося | Цель обращения | Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации | Подпись ответственного | Примечание |
|  |  |  |  |  |  |  |

ЖУРНАЛ

антивирусных проверок информационных систем

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Дата и время проверки | Наименование ИСПДн (составной части ИСПДн) | Какими средствами проводилась проверка | Результаты проверки | | Наименование инфицированных файлов, источника поступления (носитель, организация) | Примечание (принятые меры) | Фамилия и подпись лица, проводившего проверку |
|  |  |  |  | кол-во проверенных файлов | кол-во инфицированных файлов | |  |  |
|  |  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета выявленных инцидентов информационной безопасности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № № п/п | Дата и время | Описание инцидента | Ответственный за реагирование на инцидент | Отметка об устранении инцидента | Дата устранения инцидента | Подпись ответственного лица | Примечание |
|  |  |  |  |  |  |  |  |

ЖУРНАЛ

учета передачи персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Отметка о передаче или отказе в передаче персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись запрашивающего лица |
|  |  | Журнал не обязательный, если ПДн не передаются 3-м лицам |  |  |  |  |

ЖУРНАЛ

периодического тестирования средств защиты информации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование средства защиты информации от НСД или криптосредства | Регистрационные номера СЗИ от НСД или криптосредства | Дата тестирования | Фамилия и подпись ответственного пользователя, проводившего тестирование | Наименование теста, используемые средства для проведения теста | Результат тестирования (успешный/неуспешный), комментарий | Дата очередного тестирования |
| пример | Обычно сотрудниками не производится/  Тестирует лицензиат |  |  |  |  |  |  |

ЖУРНАЛ

учета проверок электронных журналов обращений к информационным системам персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата проверки | Наименование ИСПДн, компьютера, технического средства | Наименование проверяемого журнала | Выявленные нарушения требований безопасности, нештатные ситуации | Подпись администратора безопасности | Примечание |
| пример |  | ФИС ФРДО |  |  |  |  |

ЖУРНАЛ

уничтожения носителей персональных данных

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № № п/п | Наименование ИСПДн, в которой уничтожаются персональные данные | Ф.И.О. субъекта, персональные данные которого подлежат уничтожению | Обоснование уничтожения | Наименование файла, и его месторасположение | Дата уничтожения | Ф.И.О. и подпись Исполнителя | Ф.И.О. и подпись ответственного за обработку персональных данных |
| пример | - | - | - | - | - | - | - |

[Приложение 10](#П9О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПРОТОКОЛ № 1  
заседания комиссии по защите информации

|  |  |
| --- | --- |
| Дата и время проведения | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Место проведения | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО  ФИО  ФИО |

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих Наименование организации.

|  |
| --- |
| 1. Слушали: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ доложил(а) исходные данные об ИСПДн «Наименование».   Выступил(а): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».  Постановили:  Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».  2. Слушали: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ доложил(а) исходные данные об ИСПДн «Наименование».  Выступил(а): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».  Постановили:  Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование». |

|  |  |  |
| --- | --- | --- |
| Председатель комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО |
| Члены комиссии | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ФИО  ФИО  ФИО |

[Приложение 11](#П10О)  
  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

АКТ

Об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

|  |  |  |
| --- | --- | --- |
| **Роль** | **ФИО** | **Должность** |
| **Председатель** |  |  |
| **Члены комиссии** |  |  |
|  |  |
|  |  |

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Сведения, содержащие персональные данные** | **Место хранения** | **Кол-во ед. хранения** | **Примечание** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Указанные персональные данные уничтожены путем\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

|  |  |  |  |
| --- | --- | --- | --- |
| Председатель комиссии: |  |  |  |
|  | подпись |  | расшифровка |
| Члены комиссии: |  |  |  |
|  | подпись |  | расшифровка |
|  |  |  |  |
|  | подпись |  | расшифровка |

[Приложение 12](#П11О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Перечень информационных систем персональных данных

|  |  |
| --- | --- |
| Наименование | Адрес расположения |
| ССТУ Наименование города/района | Адрес |
| Наименование | Адрес |

[Приложение 13](#П12О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПЕРЕЧЕНЬ  
обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

| Группа  персональных данных | Состав персональных данных | Цели обработки  персональных данных |
| --- | --- | --- |
| 1. Обработка персональных данных в ИСПДн «ССТУ Наименование города/района» | | |
| Общие сведения о гражданах | Фамилия, имя, отчество, Дата и место рождения, Адрес проживания, Семейное положение, Социальное положение, Имущественное положение, Доходы, Паспортные данные, Данные ИНН, Данные Пенсионного страхового свидетельства, Сведения о рождении детей, о заключении/расторжении брака, Место работы, Должность, Состав семьи, Телефоны домашний и сотовый, Сведения о трудовой деятельности, Сведения о ближайших родственниках (Фамилия Имя Отчество, дата рождения, степень родства), Фотография дополнить недостающими ПДн и проверить на избыточность | Прием и регистрация обращений (или запросов) граждан, организаций и общественных объединений, поступивших в администрацию МО |
| 1. Обработка персональных данных в ИСПДн «Наименование» | | |
| Общие сведения о работниках | Фамилия, имя, отчество, Паспортные данные, Дата и место рождения, Адрес проживания, Семейное положение, Образование, Профессия, Данные ИНН, Данные Пенсионного страхового свидетельства, Данные медицинских полисов, Сведения о рождении детей, о заключении/расторжении брака, Данные о воинском учете, Место работы, Должность, Телефоны домашний и сотовый, Сведения о трудовой деятельности дополнить недостающими ПДн и проверить на избыточность | Реализация кадровой и бухгалтерской политики |
| Сведения о родственниках работника | Фамилия, имя, отчество, Дата рождения, Степень родства | Реализация кадровой и бухгалтерской политики, оформление налоговых вычетов и  других льгот |

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

| Группа персональных данных | Основание для обработки персональных данных |
| --- | --- |
| 1. Обработка персональных данных в ИСПДн «ССТУ Наименование города/района» | |
| Сведения о гражданах | Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» |
| 1. Обработка персональных данных в ИСПДн «Наименование» | |
| Сведения о работнике | Статьи 85-90 Трудового Кодекса РФ, Налоговый Кодекс РФ. |
| Сведения о родственниках работника |

[Приложение 14](#П13О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц,   
не имеющих права доступа в эти помещения

1. Общие положения
   1. Положение об организации режима обеспечения безопасности помещений Наименование организации (далее – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с 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 ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».
   2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.
2. Границы контролируемой зоны
   1. Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.
   2. План-схема контролируемой зоны помещений по адресу Адрес приведена в приложении 1 к настоящему положению.
3. Порядок доступа в помещения
   1. Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей) приведен в приложении 1 к настоящему приказу.
   2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.
   3. Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение 1

План-схема границ контролируемой зоны

Граница контролируемой зоны

[Приложение 15](#П14О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПОЛИТИКА

в отношении обработки персональных данных

1. Общие положения
   1. Политика в отношении обработки персональных данных в Наименование организации (далее – Политика) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Конституцией Российской Федерации, Трудовым кодексом Российской Федерации.
   2. Политика определяет порядок и условия обработки персональных данных в Наименование организации (далее – Оператор) с использованием средств автоматизации и без использования таких средств.
   3. Обработка персональных данных осуществляется в целях приема и регистрации обращений (или запросов) граждан, организаций и общественных объединений, поступивших в администрацию МО, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
2. Основные понятия, используемые в настоящей Политике
   1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
   2. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
   3. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
   4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
   5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
   6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
   7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
   8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
   9. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
   10. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
3. Принципы обработки персональных данных
   1. Обработка персональных данных осуществляется на законной основе.
   2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
   3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
   4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.
   5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.
   6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператором обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.
   7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
4. Условия обработки персональных данных
   1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:
      1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
      2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
      3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
      4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
      5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
      6. Обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
      7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
      8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.
   2. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.
5. Конфиденциальность персональных данных
   1. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
6. Право субъекта персональных данных на доступ   
   к его персональным данным
   1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящей Политики, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
   2. Сведения, указанные в п. 6.7 настоящей Политики, должны быть предоставлены субъекту персональных данных Оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных
   3. Сведения, указанные в п. 6.7 настоящей политики, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
   4. В случае, если сведения, указанные в п. 6.7 настоящей Политики, а также обрабатываемы персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
   5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящей Политики, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящей Политики, в случае, если такие сведения и (или) обрабатываемы персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.3 настоящей Политики, должен содержать основание направления повторного запроса.
   6. Оператор в праве отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4. настоящей Политики. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.
   7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
      1. Подтверждение факта обработки персональных данных Оператором;
      2. Правовые основания и цели обработки персональных данных;
      3. Цели и применяемые Оператором способы обработки персональных данных;
      4. Наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;
      5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;
      6. Сроки обработки персональных данных, в том числе сроки их хранения;
      7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
      8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;
      9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.
      10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.
7. Право на обжалование действий или бездействий Оператора
   1. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.
   2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.
8. Обязанности Оператора при сборе персональных данных
   1. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящей Политики.
   2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
   3. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных п. 8.4 настоящей Политики, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
      1. Наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;
      2. Цель обработки персональных данных и ее правовое основание;
      3. Предполагаемые пользователи персональных данных;
      4. Установленные настоящим Федеральным законом права субъекта персональных данных;
      5. Источник получения персональных данных.
   4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:
      1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;
      2. Персональные данные получены Оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
      3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
      4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящей Политики, нарушает права и законные интересы третьих лиц.
9. Меры направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом   
   «О персональных данных»
   1. Назначен ответственный за организацию обработки персональных данных.
   2. Изданы документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
   3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.
   4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых оператором мер.
   5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.
10. Меры по обеспечению безопасности персональных данных   
    при их обработке
    1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.
    2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.
    3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.
    4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.
    5. Ведется учет машинных носителей персональных данных.
    6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.
    7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
    8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

[Приложение 16](#П15О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ  
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

* Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
* Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
* 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».

1. Обязанности

Ответственный за организацию обработки персональных данных обязан:

* Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;
* Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;
* Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

1. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

1. Права

Ответственный за организацию обработки персональных данных имеет право:

* Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;
* Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

[Приложение 17](#П16О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПРАВИЛА   
рассмотрения запросов   
субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

* Подтверждение факта обработки персональных данных;
* Правовые основания и цели обработки персональных данных;
* Цели и применяемые оператором способы обработки персональных данных;
* Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);
* Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
* Сроки обработки персональных данных, в том числе сроки их хранения;
* Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

1. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
2. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.
3. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.
4. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.
5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в [пункте 5](#Par159) настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в [пункте 4](#Par158) настоящих правил, должен содержать обоснование направления повторного запроса.
6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным [пунктами 5](#Par159) и [6](#Par160) настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.
7. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

* Оператор обязан сообщить в порядке, предусмотренном [статьей 14](consultantplus://offline/ref=2AE8F047E3EB523928DACE479D704CEFCE4A21D0999769CA5CA643B7B987FBB294DBB1F314725456L53DJ) Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.
* В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение [части 8 статьи 14](consultantplus://offline/ref=2AE8F047E3EB523928DACE479D704CEFCE4A21D0999769CA5CA643B7B987FBB294DBB1F314725454L53FJ) Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.
* Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
* Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

[Приложение 18](#П18О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

Правила работы лиц, доступ которых к персональным данным,   
в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Допуск для работы на автоматизированных рабочих местах  
(далее – АРМ) состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

* Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;
* Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
* Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;
* Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
* Выполнять требования инструкции по организации антивирусной защиты в полном объеме;
* Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
* Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
* Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
* Некорректного функционирования установленных на АРМ технических средств защиты;
* Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

* Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;
* Самовольно вносить какие-либо изменения в конфигурацию   
  аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;
* Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);
* Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
* Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;
* Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;
* Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

[Приложение 19](#П20О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ   
ответственного за обеспечение   
безопасности персональных данных в информационных системах персональных данных

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

1. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

* Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;
* Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.
* Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;
* Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);
* Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
* Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;
* Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;
* Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;
* Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;
* Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;
* Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;
* Обязан проводить мероприятия по организации антивирусной защиты;
* Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;
* Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;
* Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:
* Установить причины, по которым стал возможным НСД;
* Установить последствия, к которым привел НСД;
* Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;
* Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;
* Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

1. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

* + Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
  + Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
  + Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

1. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

[Приложение 20](#П21О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ  
по организации резервирования

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

1. Резервируемое программное обеспечение   
   и базы персональных данных

В ИСПДн резервированию подлежит:

* Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);
* Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);
* Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);
* Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

1. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

1. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также   
ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией   
на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

|  |  |  |  |
| --- | --- | --- | --- |
| Учетная карточка резервного носителя персональных данных № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
|  |  |  |  |
| Дата резервного копирования | Объект копирования | Кто производил копирование | Подпись |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

[Приложение 21](#П22О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ  
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

* Длина пароля должна быть не менее 8 символов;
* В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);
* Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
* Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
* При смене пароля новое значение должно отличаться от предыдущих;
* Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

[Приложение 22](#П23О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ  
по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусных средств.

1. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

* Приостановить работу в ИСПДн;
* Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
* Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* Провести лечение или уничтожение зараженных файлов.

1. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

[Приложение 23](#П24О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПОРЯДОК   
уничтожения персональных данных при достижении   
целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №\_\_(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

[Приложение 24](#П26О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки

персональных данных требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Наименование организации требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.
2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.
3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.
4. Плановые проверки проводятся не чаще чем один раз в три месяца.
5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных
6. Основанием для проведения проверки служит издание приказа «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»
7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

* соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора персональных данных;
* соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
* достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;
* отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
* порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
* порядок и условия применения средств защиты информации;
* соблюдение правил доступа к персональным данным;
* наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

1. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

* запрашивать у работников информацию, необходимую для реализации своих полномочий;
* требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
* принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
* вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
* вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

1. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес директора результаты проведения проверки в форме служебной записки.

[Приложение 25](#П26О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ

о пропускном и внутриобъектовом режимах

1. Общие положения

Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационных систем персональных данных (далее – ИСПДн) Наименование организации, в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн). При обеспечении доступа лиц соблюдаются требования по защите ПДн.

Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников Наименование организации, сотрудников иных организаций и учреждений, граждан в помещения.

Контроль за порядком обеспечения доступа лиц в помещения отделов возлагается на руководителей подразделений.

Помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в данные помещения и к данному оборудованию посторонних лиц.

1. Организация пропускного и внутриобъектового режима

Пропускной режим в Наименование организации устанавливается в целях:

* исключения фактов хищений собственности Наименование организации;
* исключения фактов вандализма со стороны недобросовестных посетителей;
* исключения возможности несанкционированного доступа персонала и посетителей в помещения Наименование организации.

Внутриобъектовый режим устанавливается в целях:

* соблюдения персоналом и посетителями правил внутреннего распорядка и пожарной безопасности;
* установления порядка допуска персонала в помещения ограниченного доступа предприятия;
* исключения возможности бесконтрольного передвижения посетителей по территории предприятия.

Надёжность пропускного и внутриобъектового режимов достигается:

* осуществлением контроля за перемещением персонала;
* осуществлением охраны помещений предприятия силами ЧОП;
* контролем за состоянием технических средств охраны.

Ответственным за организацию пропускного и внутриобъектового режимов является Директор Наименование организации.

Организация пропускного и внутриобъектового режимов предприятия осуществляется руководителями соответствующих подразделений.

1. Порядок доступа в помещения сотрудников и граждан

Устанавливаются следующие часы работы Наименование организации:

* C 08-00 до 20-00 с понедельника по воскресенье;
* без обеда;
* без выходных.

Всем сотрудникам Наименование организации оформляется постоянный пропуск с нанесением на него следующей информации:

* Название Учреждения
* Номер пропуска
* ФИО
* Фотография сотрудника
* Подпись сотрудника
* Должность сотрудника

Выполнение работ по учету, оформлению и выдаче пропусков для персонала осуществляется начальником отдела административно-хозяйственной деятельности.

При увольнении сотрудника пропуск подлежит изъятию.

Контроль за правильностью учета, хранения и выдачи пропусков осуществляет Директор Наименование организации или лицо, его замещающее. Периодичность проверок устанавливается не реже одного раза в месяц.

Основанием для выдачи пропуска работнику является заключенный с Наименование организации трудовой договор. С целью установления материальной ответственности персонала за выданные пропуска факт выдачи пропуска сотруднику регистрируется начальником отдела административно-хозяйственной деятельности в журнале учета выдачи пропусков под роспись сотрудника.

1. Внутриобъектовый режим на территории Наименование организации.

Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объектах является Директор Наименование организации.

В случае отсутствия пропуска сотрудник Наименование организации обязан обратиться к начальнику отдела административно-хозяйственной деятельности для получения временного пропуска со сроком действия один день.

Сотрудники кабинетов по окончании рабочего дня должны закрывать на ключ и опечатывать кабинеты (помещения) и сдавать ключ на пост охраны.

В случае отсутствия сотрудников в кабинетах в рабочее время, помещения должны быть закрыты на ключ.

На территории предприятия запрещается:

* + проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;
  + курить;
  + пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;
  + загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;
  + совершать действия, нарушающие установленные режимы функционирования технических средств охраны и пожарной сигнализации.

1. Организация и порядок производства ремонтно-строительных работ в здании

Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.

Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

1. Организация охраны

Должна быть организована охрана помещений Наименование организации. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо запирать его на ключ.

1. Уборка помещений

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн должны быть убраны в сейф.

8. Требования по техническому укреплению

Ответственный за обеспечение безопасности ПДн обеспечивает обязательное выполнение мероприятий по техническому укреплению помещений, в которых обрабатываются ПДн, и должен руководствоваться следующими основными требованиями:

* двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;
* конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

[Приложение 26](#П26О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ

по обработке персональных данных без использования средств автоматизации

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в Наименование организации, или сотруднику (далее – субъекту персональных данных) Наименование организации.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

1. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Наименование организации или лица, осуществляющие такую обработку по договору с Наименование организации), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Наименование организации без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Наименование организации.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

* типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;
* типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;
* типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения Наименование организации или в иных аналогичных целях, должны соблюдаться следующие условия:

* необходимость ведения такого журнала должна быть предусмотрена актом Наименование организации, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;
* копирование содержащейся в таких журналах информации не допускается;
* персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

1. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

[Приложение 27](#П26О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ

по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в Наименование организации возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем Наименование организации) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

* даты и времени;
* причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
* информации о последствиях;
* информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для Наименование организации и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем Наименование организации накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Наименование организации, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

* замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
* установка дополнительного ПО;
* изменение сетевых настроек рабочего места;
* замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов Наименование организации, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

[Приложение](#П26О) 28  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ИНСТРУКЦИЯ

ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в Наименование организации назначается Директором.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в Наименование организации.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

[Приложение 29](#П26О)  
к приказу Наименование организации

от \_\_. \_\_.2016 № \_\_\_

ПЛАН

мероприятий по защите информации в Наименование организации

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах персональных данных Наименование организации.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИСПДн.

В План мероприятий включены следующие категории мероприятий:

* организационные (административные);
* физические;
* технические (аппаратные и программные);
* контролирующие.

В План мероприятий включена следующая информация:

* название мероприятия;
* периодичность мероприятия (разовое/периодическое);
* исполнитель мероприятия/ответственный за исполнение.

План внутренних проверок составляется на все информационные системы персональных данных Наименование организации.

План мероприятий по защите информации

| **Мероприятие** | **Периодичность** | **Исполнитель/ Ответственный** |
| --- | --- | --- |
| **Организационные мероприятия** | | |
| Обследование информационных систем | Разовое  срок до |  |
| Определение перечня ИСПДн | Разовое  срок до |  |
| Определение обрабатываемых ПДн и объектов защиты | Разовое  срок до |  |
| Определение круга лиц, участвующих в обработке ПДн | Разовое  срок до. |  |
| Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей | Разовое  срок до |  |
| Назначение ответственного за обеспечение безопасности ПДн | Разовое  срок до |  |
| Классификация всех выявленных ИСПДн | Разовое  срок до |  |
| Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн. | Разовое  срок до |  |
| Организация порядка резервного копирования защищаемой информации на твердые носители | Разовое  срок до. |  |
| Организация информирования сотрудников о порядке обработки ПДн и их обучения | Разовое  срок до |  |
| Организация информирования сотрудников о введенном режиме защиты ПДн | Разовое  срок до |  |
| Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн | Разовое  срок до |  |
| **Физические мероприятия** | | |
| Установление границ контролируемой зоны ИСПДн | Разовое  срок до |  |
| Организация постов охраны для пропуска в контролируемую зону | Разовое  срок до |  |
| Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПД снаружи здания | Разовое  срок до |  |
| **Технические мероприятия** | | |
| Внедрение специальной подсистемы управления доступом, регистрации и учета | Разовое  срок до |  |
| Внедрение межсетевого экранирования | Разовое  срок до |  |
| Внедрение криптографической защиты | Разовое  срок до |  |
| **Контролирующие мероприятия** | | |
| Контроль над соблюдением режима обработки ПДн | Еженедельно |  |
| Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн | Ежегодно |  |
| Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн | Еженедельно |  |
| Контроль за обеспечением резервного копирования | Ежемесячно |  |
| Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз | Ежегодно |  |
| Поддержание в актуальном состоянии нормативно-организационных документов | Ежемесячно |  |