**ПРИКАЗ**

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

|  |
| --- |
| **Об утверждении перечня сотрудников,**  **допущенных к обработке персональных данных в**  ***<наименование учреждения >*** |

В целях выполнения требований Федерального закона №152 "О персональных данных", постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства РФ от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказываю:

1. Утвердить перечень сотрудников, допущенных к обработке персональных данных в информационных системах персональных данных <*наименование учреждения >* (прилагается).
2. Утвердить прилагаемую инструкцию пользователя информационной системы персональных данных.
3. Сотрудников, допущенных к обработке персональных данных, ознакомить под роспись с настоящим приказом и прилагаемой Инструкцией.
4. Контроль за исполнением настоящего приказа оставляю за собой.

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

Утвержден

приказом *<наименование учреждения>*

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

**Перечень сотрудников, допущенных к обработке персональных данных в информационных системах персональных данных (ИСПДн) *<наименование*** *учреждения* ***>***

В *<наименование учреждения>* к сотрудникам, имеющим доступ к персональным данным для исполнения своих должностных обязанностей, относятся:

ИСПНд 1 *<наименование ИСПНд>:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Должность | Фамилия, имя, отчество | Вид выполняемых функций | Уровень допуска учетной записи |
| 1 |  |  | Пользователь | Конфиденциально |
| 2 |  |  |  |  |

ИСПНд 2 *<наименование ИСПНд>:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Должность | Фамилия, имя, отчество | Вид выполняемых функций | Уровень допуска учетной записи |
| 1 |  |  | Пользователь | Конфиденциально |
| 2 |  |  |  |  |

Приложение к приказу №\_\_\_\_\_\_

от « » \_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

|  |
| --- |
| УТВЕРЖДАЮ |
| Руководитель  <*наименование учреждения*> |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *ФИО* |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |

**ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ**

**ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

<*наименование учреждения* >

г. Белгород

20\_\_ г.

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных (ИСПДн) <*наименование учреждения* > (далее – Учреждение).
   2. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
   3. Пользователь несет персональную ответственность за свои действия.
   4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения.
   5. Методическое руководство работой Пользователя осуществляется ответственным за обеспечение безопасности персональных данных.
   6. Допуск пользователей для работы с ИСПДн осуществляется в соответствии со списком лиц допущенных к работе.
2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Пользователь обязан:

1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
2. Выполнять обработку персональных данных на автоматизированном рабочем месте (далее – АРМ) в соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным.
3. Соблюдать требования парольной политики (раздел 3).
4. Знать и соблюдать правила работы со средствами защиты информации и установленными режимами разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке, а также правила учета, хранения и передачи съемных носителей информации (раздел 4).
5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 5).
6. При работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами.
7. Обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой на АРМ немедленно оповещать Ответственного за обеспечение безопасности персональных данных и персонал, обслуживающий АРМ.
8. Пользователю запрещается:

- Разглашать защищаемую информацию третьим лицам.

- Передавать персональные данные по телефону, факсу или электронной почте.

- Копировать и хранить персональные данные на неучтенных установленным порядком съемных носителях информации.

- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

- Самостоятельно подключать к АРМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение АРМ.

- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

- Подключать к рабочей станции и локальной вычислительной сети личные внешние носители и мобильные устройства.

- Отключать (блокировать) средства защиты информации.

- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

- Привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение защиты персональных данных.

- Производить действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями

- Бесконтрольно оставлять АРМ с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

1. При отсутствии визуального контроля за АРМ, доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.
2. Пользователь отвечает за правильность включения и выключения своего АРМ, входа в систему и все действия при работе с ИСПДн.
3. При работе со съемными носителями пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием штатных антивирусных программ, входящих в состав ПО, в соответствии с «Инструкцией по антивирусной защите». В случае обнаружения вирусов на съемном носителе пользователь обязан немедленно сообщить об этом Ответственного за обеспечение безопасности персональных данных.
4. В случае возникновения внештатных ситуаций и аварийных ситуаций, пользователь обязан принимать меры по реагированию, с целью ликвидации последствий этих ситуаций, в пределах возложенных на него функций и немедленно информировать Ответственного за обеспечение безопасности персональных данных.
5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ
   1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль за действиями исполнителей при работе с паролями возлагается на Ответственного за обеспечение безопасности персональных данных.
   2. Личные пароли доступа к элементам ИСПДн выдаются пользователям Ответственным за обеспечение безопасности персональных данных или системным администратором.
   3. Полная плановая смена паролей проводится не реже одного раза в 3 месяца.
   4. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

- пароль должен состоять не менее чем из 6 символов;

- в пароле должны присутствовать символы трех категорий из числа следующих четырех:

* прописные буквы английского алфавита от A до Z;
* строчные буквы английского алфавита от a до z;
* десятичные цифры (от 0 до 9);
* символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения (свои и родственников), клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

- запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- запрещается выбирать пароли, которые уже использовались ранее.

* 1. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

* 1. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

* 1. Владельцы пароля должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
  2. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Ответственному за обеспечение безопасности персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

* 1. Внеплановая смена личного пароля или удаление (блокирование) учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должно производиться Ответственным за обеспечение безопасности персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.
  2. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) Ответственного за обеспечение безопасности персональных данных.

1. ПРАВИЛА РАБОТЫ В СЕТЯХ ОБЩЕГО ДОСТУПА И (ИЛИ) МЕЖДУНАРОДНОГО ОБМЕНА
   1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть), должна проводиться при служебной необходимости.
   2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);

- передавать по Сети защищаемую информацию без использования средств шифрования;

- запрещается нецелевое использование подключения к Сети.

1. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИСПДн

Пользователь ИСПДн несет ответственность за:

* 1. Надлежащее выполнение требований настоящей инструкции.
  2. Соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите персональных данных и использования информационных ресурсов.
  3. Сохранность персональных данных.
  4. Сохранность и работоспособное состояние средств вычислительной техники и съемных носителей, на которых хранятся и обрабатываются персональные данные.

**Лист ознакомления**

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