



Томская область
городской округ
закрытое административно-территориальное образование Северск
АДМИНИСТРАЦИЯ ЗАТО СЕВЕРСК
УПРАВЛЕНИЕ МОЛОДЕЖНОЙ И СЕМЕЙНОЙ ПОЛИТИКИ,
ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА
(УМСП ФКиС Администрации ЗАТО Северск)

ПРИКАЗ

31.07.2025

№ 249

Об ответственном за обеспечение безопасности персональных
данных в информационных системах персональных данных
Управления молодежной и семейной политики,
физической культуры и спорта Администрации ЗАТО Северск

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях обеспечения уровня защищенности персональных данных при их обработке в информационных системах персональных данных, определенного в Управлении молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск

ПРИКАЗЫВАЮ:

1. Возложить функции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в Управлении молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск (далее – УМСП ФКиС Администрации ЗАТО Северск, Управление) на ВРИО начальника УМСП ФКиС Администрации ЗАТО Северск.

2. Утвердить прилагаемую Инструкцию по обеспечению безопасности персональных данных в информационных системах персональных данных в УМСП ФКиС Администрации ЗАТО Северск.

3. Разместить приказ на официальном сайте УМСП ФКиС Администрации ЗАТО Северск в информационно-телекоммуникационной сети «Интернет» (<https://умсп.зато-северск.рф/>).

4. Старшему инспектору УМСП ФКиС Администрации ЗАТО Северск Ковалёвой К.Ю. ознакомить заинтересованных лиц в настоящем приказом.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Врио начальника Управления

Т.Н. Малыщенко

**Инструкция по обеспечению безопасности персональных данных
в информационных системах персональных данных
Управления молодежной и семейной политики,
физической культуры и спорта
Администрации ЗАТО Северск**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Управления молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск (далее – Ответственный) назначается приказом начальника Управления молодежной и семейной политики, физической культуры и спорта Администрации ЗАТО Северск (далее – Управление) и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) в процессе их обработки в информационных системах персональных данных (далее – ИСПДн) Управления.
2. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.
3. В своей деятельности Ответственный руководствуется Политикой в отношении обработки персональных данных в Управлении настоящей Инструкцией, рекомендациями Ответственного за организацию обработки персональных данных (далее – Ответственный за организацию обработки ПДн).
4. Методическое руководство работой Ответственного осуществляет Ответственный за организацию обработки ПДн.

**2. ОСНОВНЫЕ ФУНКЦИИ И ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Функции Ответственного:

1. Ответственный изучает все стороны деятельности Управления и вырабатывает рекомендации по защите ПДн при решении следующих основных вопросов:
 - 1) проведение аналитической работы по комплексной защите и предупреждению утечки ПДн;
 - 2) подготовка решений в отношении сведений о работах, выполняемых Управлением, подлежащих защите;
 - 3) рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения

достаточности предусмотренных в них требований и мероприятий по комплексной защите ПДн, при научных исследованиях, при проведении других работ;

4) координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;

5) проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки ПДн;

6) подготовка предложений по совершенствованию действующей системы защиты ПДн с последующим предоставлением начальнику Управления;

7) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПДн;

8) обеспечение соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

9) осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Управления.

Ответственный обязан:

2. Соблюдать требования действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;

3. Знать состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн;

4. Осуществлять общее техническое сопровождение ИСПДн:

10) контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

11) контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;

12) вести журнал учета и выдачи используемых материальных носителей ПДн;

13) контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;

14) проводить инструктаж работников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в ИСПДн Управления (далее – Пользователи ИСПДн) по правилам работы в ИСПДн;

5. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИСПДн:

15) реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка работников, допущенных к работе в ИСПДн;

16) назначать пароли Пользователей ИСПДн;

17) контролировать плановую смену паролей Пользователями ИСПДн для доступа в ИСПДн;

18) своевременно удалять профиль Пользователя ИСПДн при увольнении или переводе сотрудника;

19) вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;

20) регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИСПДн;

21) своевременно информировать Ответственного за организацию обработки ПДн о несанкционированных действиях персонала для организации расследования попыток НСД;

6. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИСПДн:

22) обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Управления;

23) обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;

24) обеспечивать регулярное и своевременное создание резервных копий ИСПДн Управления;

25) осуществлять настройку и сопровождение системы защиты от НСД в ИСПДн;

7. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИСПДн;

8. Требовать прекращения обработки ПДн в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

9. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД;

10. Участвовать при проведении внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;

11. Контролировать выполнение Пользователями ИСПДн требований Инструкции пользователя информационных систем персональных данных Управления, а также установленных требований для обеспечения уровней защищенности ПДн;

12. Контролировать правильность применения Пользователями ИСПДн средств защиты информации;

13. В случае получения от Пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности ПДн в пределах своих полномочий;

14. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИСПДн:

26) антивирусного программного обеспечения;

27) средств защиты от несанкционированного доступа;

15. В случае нарушения работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты ИСПДн, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности;

16. Своевременно информировать Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ИСПДн.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный имеет право:

1. Знакомиться с локальными актами Управления, регламентирующими процессы обработки и защиты ПДн;
2. Вносить предложения начальнику Управления по совершенствованию существующей системы защиты информации;
3. Привлекать по согласованию с Ответственным за организацию обработки ПДн к работе по созданию и совершенствованию системы защиты ПДн других работников Управления;
4. Требовать от Пользователей ИСПДн соблюдения требований Инструкции пользователя информационных систем персональных данных Управления, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн;
5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность ПДн, вносить свои предложения по совершенствованию организационных и технических мер защиты ПДн в ИСПДн;
6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн;
7. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных Пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн;
8. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. ОТВЕТСТВЕННОСТЬ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Ответственный в соответствии с возложенными на него обязанностями несет ответственность за:

1. Несоблюдение требований локальных актов Управления, устанавливающих порядок работы с ПДн в пределах, установленных трудовым договором (служебным контрактом);
- 4.2. Разглашение ПДн в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен: