



Томская область  
городской округ  
закрытое административно-территориальное образование Северск

**АДМИНИСТРАЦИЯ ЗАТО СЕВЕРСК**  
**УПРАВЛЕНИЕ КАПИТАЛЬНОГО СТРОИТЕЛЬСТВА**  
**(УКС Администрации ЗАТО Северск)**

ул.Лесная, 11а, г. Северск, Томская обл., 636000.

Тел. (3823) 77 23 59. Факс (3823) 77 42 96. E-mail: [seversk-uks@gov70.ru](mailto:seversk-uks@gov70.ru), <https://строительство.зато-северск.рф/>

**ПРИКАЗ**

16.04.2025

№ 153

О назначении ответственного лица за обеспечение безопасности персональных данных в информационных системах персональных данных и организацию обработки персональных данных Управления капитального строительства Администрации ЗАТО Северск

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», для обеспечения уровня защищенности персональных данных при их обработке в информационных системах персональных данных

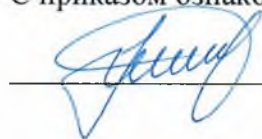
**ПРИКАЗЫВАЮ:**

1. Назначить ответственным лицом за обеспечение безопасности персональных данных в информационных системах персональных данных и организацию обработки персональных данных Управления капитального строительства Администрации ЗАТО Северск начальника финансово-экономического отдела Ледяйкина Андрея Сергеевича.
2. Возложить обязанности Администратора информационных систем персональных данных на начальника финансово-экономического отдела Ледяйкина Андрея Сергеевича.
3. Утвердить прилагаемую Инструкцию ответственного по обеспечению безопасности персональных данных в информационных системах персональных данных Управления капитального строительства Администрации ЗАТО Северск.
4. Утвердить прилагаемую Инструкцию ответственного за организацию обработки персональных данных Управления капитального строительства Администрации ЗАТО Северск.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Управления

П.А.Шипунов

С приказом ознакомлен:



\_\_\_\_\_  
Ледяйкин А.С.

Исп. Советник-юрисконсульт Е.В. Афанасьева  
тел. 8 (3823) 77-23-55



## УТВЕРЖДЕНА

приказом           Управления           капитального  
строительства Администрации ЗАТО Северск  
от 16.04.2015 № 154

### Инструкция ответственного по обеспечению безопасности персональных данных в информационных системах персональных данных Управления капитального строительства Администрации ЗАТО Северск

#### І. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая инструкция определяет обязанности, права и ответственность ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных Управления капитального строительства Администрации ЗАТО Северск (далее – Ответственный)

2. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Управления капитального строительства Администрации ЗАТО Северск назначается приказом Управления капитального строительства 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.

3. В своей деятельности Ответственный руководствуется настоящей Инструкцией, Политикой в отношении обработки персональных данных в Управлении.

4. Ответственный должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн.

#### ІІ. ОСНОВНЫЕ ОБЯЗАННОСТИ

5. Ответственный обязан:

1) обеспечить соответствие проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

2) определять полномочия пользователей информационной системы (далее – ИС) (оформление разрешительной системы доступа), минимально необходимые им для выполнения служебных (трудовых) обязанностей;

3) осуществлять учёт машинных носителей персональных данных, их уничтожение, либо контроль процедуры их уничтожения, вести «Журнал учета машинных носителей персональных данных»;

4) осуществлять оперативный контроль за работой пользователей автоматизированного рабочего места (далее – АРМ) ИСПДн и адекватно реагировать на возникающие нештатные ситуации, фиксировать их в «Журнале учета работ в информационных системах»;

5) проверять актуальность сертификатов соответствия используемых средств защиты информации в информационных системах;

6) блокировать доступ к защищаемой информации при обнаружении нарушений порядка ее обработки;

7) своевременно реагировать на попытки несанкционированного доступа к информации, содержащей персональные данные;

8) устанавливать и осуществлять настройку средств защиты информации в рамках компетенции;

9) по мере необходимости вносить изменения в конфигурацию технических средств ИС, отражать соответствующие изменения в перечне автоматизированных рабочих мест



информационной системы, проводить анализ потенциального воздействия планируемых изменений в конфигурации информационной системы на обеспечение защиты персональных данных;

10) осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИС средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование);

11) проводить работу по выявлению возможных каналов утечки информации, изучать текущие тенденции в области защиты персональных данных;

12) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения съемных носителей персональных данных, нарушения правил работы с техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости;

13) предоставлять доступ к ИС новым пользователям, предоставлять им возможность задать личный пароль, соответствующий требованиям Инструкции по организации парольной защиты;

14) производить мероприятия по внеплановой смене личных паролей;

15) вносить плановые и внеплановые изменения в учётную запись пользователей ИС, в том числе по требованию руководителя и в случае увольнения работника;

16) осуществлять периодическое резервное копирование баз данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных;

17) осуществлять восстановление информации из резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для восстановления утраченных сведений;

18) хранить дистрибутивы программного обеспечения, установленного в ИС, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

19) вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятию мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению степени защищённости;

20) заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных);

21) знать законодательство РФ о защите информации, следить за его изменениями;

22) выполнять иные мероприятия, требуемые техническими и программными средствами ИС для поддержания их функционирования;

23) при использовании в информационных системах технологий беспроводного доступа, разграничивать доступ к беспроводной сети, контролировать предоставление доступа к беспроводной сети только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (при наличии сертифицированных средств защиты информации);

24) контролировать запрет обработки защищаемой информации с использованием технологии беспроводного доступа к сети (при отсутствии сертифицированных средств защиты информации);

25) при необходимости реализации удаленного доступа к информационной системе устанавливать виды доступа пользователей и ограничения на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, предоставлять удаленный доступ только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей, проводить контроль и мониторинг удаленного доступа на предмет несанкционированного доступа к информационной системе;

26) обеспечивать регламентацию и контроль использования мобильных технических средств, в том числе устанавливать параметры доступа к мобильным средствам, проводить проверки на предмет выявления несанкционированного использования мобильных технических средств для доступа к информационной системе.

### **III. ПОРЯДОК РАБОТЫ С МАШИННЫМИ НОСИТЕЛЯМИ**

6. Под машинными носителями (далее – носители) в настоящей инструкции понимаются съемные машинные носители и несъемные машинные носители.

7. Под несъемными машинными носителями в настоящей инструкции понимаются накопители на жестких дисках, встроенные в корпус средств вычислительной техники (серверов, автоматизированных рабочих мест, сетевых хранилищ и т.п.).

8. Под съемными машинными носителями (далее – съемные носители) в настоящей инструкции понимаются следующие носители информации: – оптические диски (CD, DVD) однократной и многократной записи; – электронные накопители информации (флэш-память, съемные жесткие диски).

9. Носители, содержащие персональные данные, подлежат обязательному учету Ответственным за обеспечение безопасности персональных данных в информационных системах в Журнале учета машинных носителей персональных данных.

10. Учет машинных носителей персональных данных включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей персональных данных, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

11. Учет выдачи съемных носителей ведётся в Журнале учета машинных носителей персональных данных, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его подпись.

12. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

13. При поступлении нового носителя, который будет использоваться для хранения или передачи персональных данных, Ответственный за обеспечение безопасности персональных данных в информационных системах регистрирует его в Журнале учета съемных носителей персональных данных.

14. В случае возврата должностным лицом съемного носителя в Журнале учета съемных носителей персональных данных Ответственным за обеспечение безопасности персональных данных в информационных системах проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

15. Ответственным за обеспечение безопасности персональных данных в информационных системах должно обеспечиваться уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

### **IV. РАЗГРАНИЧЕНИЕ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ И СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ**

16. Защита от несанкционированного доступа осуществляется:



1) идентификацией и проверкой подлинности пользователей ИС при доступе к информационным ресурсам;

2) ограничением неуспешных попыток входа в информационную систему;

3) блокированием сеанса доступа в информационную систему после установленного ответственным за обеспечение безопасности времени бездействия;

4) разграничением доступа к обрабатываемым базам данных. Пользователь ИС имеет доступ только к тем информационным ресурсам, которые разрешены для него. Для осуществления доступа к информационным ресурсам Ответственный за обеспечение безопасности персональных данных в информационных системах назначает конкретному пользователю ИС идентифицирующее имя пользователя и персональный пароль доступа.

17. Ответственный за обеспечение безопасности персональных данных в информационных системах должен осуществлять мероприятия по обеспечению защиты информационных ресурсов от несанкционированного доступа, непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоя и отказов оборудования.

## **V. ПРАВА**

18. Ответственный за обеспечение безопасности персональных данных в информационных системах имеет право:

1) требовать от пользователей ИС выполнения инструкций в части работы с программными, аппаратными средствами ИС и защищаемой информацией;

2) блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты информации;

3) проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ;

4) производить тестирование системы контроля доступа к персональным данным на наличие уязвимостей;

5) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости.

## **VI. ОТВЕТСТВЕННОСТЬ**

19. Ответственный за обеспечение безопасности персональных данных в информационных системах несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в Управлении, за качество проводимых им работ по обеспечению безопасности защищаемой информации и за все действия, совершенные от имени его учётной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

20. Ответственный за обеспечение безопасности персональных данных в информационных системах при нарушении норм, регулирующих получение, обработку и защиту информации, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

21. Разглашение защищаемой информации (передача ее посторонним лицам, в том числе другим работникам, не имеющим к ней доступ), ее публичное раскрытие, утрата документов и иных носителей, содержащих защищаемую информацию субъекта, а также иные нарушения обязанностей по их защите и обработке, установленные локальными

нормативно-правовыми актами (приказами, распоряжениями) Управления, влекут наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник, имеющий доступ к защищаемой информации субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Управлению (в соответствии с пунктом 7 статьи 243 Трудового кодекса РФ).

22. В отдельных случаях, при разглашении защищаемой информации, работник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

## УТВЕРЖДЕНА

приказом           Управления           капитального  
строительства Администрации ЗАТО Северск  
от 16.04.2025 № 154

### Инструкция ответственного по организации обработки персональных данных в Управлении капитального строительства Администрации ЗАТО Северск

#### І. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая инструкция определяет обязанности, права и ответственность ответственного за организацию обработки персональных данных Управления капитального строительства Администрации ЗАТО Северск (далее – Управление)
2. Ответственный за организацию обработки персональных данных Управления назначается приказом Управления и отвечает за решение вопросов организации защиты персональных данных в Управлении.
3. Ответственный за организацию обработки персональных данных Управления обладает правами доступа к любым носителям персональных данных Управления.
4. В своей деятельности Ответственный за организацию обработки персональных данных Управления руководствуется настоящей Инструкцией и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

#### ІІ. ОСНОВНЫЕ ОБЯЗАННОСТИ

5. Ответственный за организацию обработки персональных данных Управления обязан:
  - 1) осуществлять учет документов, содержащих персональные данные, их уничтожение либо осуществлять контроль процедуры их уничтожения;
  - 2) контролировать осуществление мероприятий по установке и настройке средств защиты информации;
  - 3) участвовать в определении полномочий пользователей информационных систем персональных данных, минимально необходимых им для выполнения служебных (трудовых) обязанностей;
  - 4) реагировать на попытки несанкционированного доступа к информации, содержащей персональные данные, а также блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;
  - 5) 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;
  - 6) проводить занятия и инструктажи с сотрудниками, уполномоченными на обработку персональных данных о порядке работы с персональными данными и осуществлять изучение документов в области обеспечения безопасности персональных данных;
  - 7) контролировать соблюдение сотрудниками, уполномоченными на обработку персональных данных локальных документов, регламентирующих порядок работы с персональными данными;
  - 8) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушений правил работы с документами, содержащими персональные данные или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных;
  - 9) знать законодательство Российской Федерации о персональных данных, следить за его изменениями;



10) выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

### **III. ПРАВА**

6. Ответственный за организацию обработки персональных данных Управления имеет право:

- 1) принимать решения в пределах своей компетенции;
- 2) требовать от работников Управления соблюдения действующего законодательства, а также локальных нормативных актов Управления о персональных данных;
- 3) вносить свои предложения по совершенствованию мер защиты персональных данных;
- 4) взаимодействовать с органом местного самоуправления и его структурными подразделениями по вопросам обработки персональных данных.

### **IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ**

7. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных Управления обязан:

- 1) прекратить несанкционированный доступ к персональным данным;
- 2) доложить начальнику Управления докладной запиской о факте несанкционированного доступа, его результате и предпринятых мерах.

### **V. ОТВЕТСТВЕННОСТЬ**

8. Ответственный за организацию обработки персональных данных Управления при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с действующим законодательством.

Лист ознакомления работников Управления

с Приказом «О назначении ответственного лица за обеспечение безопасности персональных данных в информационных системах персональных данных и организацию обработки персональных данных Управления капитального строительства Администрации ЗАТО Северск» от 16.04.2025 № 15у

[illegible]







