



**АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
«ХИСЛАВИЧСКИЙ МУНИЦИПАЛЬНЫЙ ОКРУГ»
СМОЛЕНСКОЙ ОБЛАСТИ**

РАСПОРЯЖЕНИЕ

25.06.2025

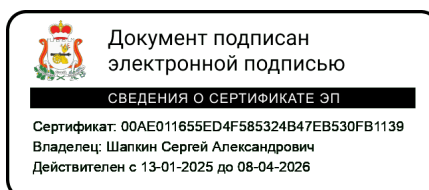
Р-493

Об утверждении Инструкции
пользователя информационной
системы персональных данных
Администрации муниципального
образования «Хиславичский
муниципальный округ»
Смоленской области

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» в целях организации защиты персональных данных в информационных системах персональных данных Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области:

1. Утвердить Инструкцию пользователя информационной системы персональных данных Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области (приложение №1).

Глава муниципального образования
«Хиславичский муниципальный округ»
Смоленской области



С.А. Шапкин

ИНСТРУКЦИЯ

ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области

1. Общие положения

Настоящая инструкция регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационной системы персональных данных (далее – ИСПДн) Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области (далее – Администрации округа).

2. Термины и определения

- 2.1. Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
- 2.2. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.
- 2.3. Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
- 2.4. Доступ к информации – возможность получения информации и её использования.
- 2.5. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.
- 2.6. Информация – сведения (сообщения, данные) независимо от формы их представления.
- 2.7. Информационная система персональных данных (ИСПДн) – совокупность

содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

- 2.8. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.
- 2.9. 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.
- 2.10. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.
- 2.11. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- 2.12. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- 2.13. Средства защиты информации (СЗИ) – технические, программные средства, вещества и (или) материалы, предназначенные или используемые для защиты информации.

3. Общие обязанности сотрудников

Каждый сотрудник Администрации округа, являющийся пользователем ИСПДн, обязан:

- 3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.
- 3.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее – АРМ).
- 3.3. Соблюдать правила работы с паролем своей учётной записи, установленные в Инструкции по организации парольной защиты в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области.
- 3.4. Соблюдать правила работы со средствами антивирусной защиты, установленные в Положении об организации антивирусной защиты в Администрации муниципального образования «Хиславичский муниципальный округ» Смоленской области.
- 3.5. Немедленно вызывать администратора безопасности ИСПДн и поставить в

известность руководителя структурного подразделения при обнаружении:

- Нарушений целостности пломб (наклеек, нарушений или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ.
- Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных на АРМ технических средств защиты.
- Непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.6. Всем сотрудникам Администрации округа, являющимся пользователями ИСПДн, категорически ЗАПРЕЩАЕТСЯ:

- записывать и хранить информацию на неучтенных носителях информации;
- использовать компоненты программного и аппаратного обеспечения ИСПДн Администрации округа и учтенные носители информации в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;
- оставлять без присмотра своё АРМ, не активизировав блокировки доступа, или оставлять своё АРМ включенным по окончании работы;
- оставлять без присмотра учтенные носители информации, передавать учтенные носители информации другим лицам и выносить за пределы помещений, в которых разрешена обработка информации;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

4. Обеспечение сохранности информации

4.1. Для обеспечения сохранности электронных информационных ресурсов Администрации округа необходимо соблюдать следующие требования:

- Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

4.2. Субъектам доступа запрещается:

- Установка и использование при работе с электронно-вычислительными машинами вредоносных программ, ведущих к блокированию работы сети.

- Самовольное изменение сетевых адресов.
- Самовольное вскрытие блоков электронно-вычислительных машин, модернизация или модификация электронно-вычислительных машин и программного обеспечения.
- Несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров из одного подразделения в другое производится только администратором безопасности ИСПДн с предварительно удаленными сетевыми настройками.
- Сведения, содержащиеся в электронных документах и базах данных Администрации округа, должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

5. Ответственность за нарушение правил работы

- 5.1. Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.
- 5.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, сотрудники могут быть привлечены к гражданско-правовой, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.