МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ (ПОВЫШЕНИЯ КВАЛИФИКАЦИИ) «ЦЕНТР РАЗВИТИЯ ОБРАЗОВАНИЯ ГОРОДА ДУБНЫ МОСКОВСКОЙ ОБЛАСТИ» (ЦРО)

СОГЛАСОВАНО

Представитель трудового коллектива

_____ И.А. Лапушкина

УТВЕРЖДАЮ

Директор ЦРО

_____ Е.В. Рожкова

ИНСТРУКЦИЯ

ответственного лица Муниципального бюджетного образовательного учреждения дополнительного профессионального образования (повышения квалификации) «Центр развития образования города Дубны Московской области» за обеспечения безопасности при обработке и хранении персональных данных сотрудников с использованием средств автоматизации

1. Термины и сокращения

АРМ – автоматизированное рабочее место
ИСПДн – информационная система персональных данных
ПДн – персональные данные
СЗПДн – система (подсистема) защиты персональных данных
СКЗИ – средства криптографической защиты информации

2. Общие положения

2.1. Все должностные лица, уполномоченные на обработку персональных данных, а также остальные сотрудники, работающие в помещениях, в которых ведётся обработка персональных данных, должны быть ознакомлены с данной инструкцией.

2.2. Должностные лица, допущенные к обработке персональных данных, обязаны строго соблюдать установленные правила работы и несут персональную ответственность за обеспечение безопасности информации.

3. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации

3.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации.

3.2. Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании «Перечня должностей сотрудников ЦРО, замещение которых

предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным» утверждѐнного директором ЦРО.

3.3. Должна быть обеспечена сохранность носителей персональных данных и средств защиты информации, а также исключена возможность неконтролируемого пребывания в помещениях, в которых ведѐтся обработка ПДн, посторонних лиц.

3.4. Компьютеры и (или) электронные папки (каталоги), в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.5. Осуществлять обработку и хранение конфиденциальных данных, не внесѐнных в список «Перечень персональных данных, подлежащих защите в ЦРО, запрещается.

3.6. Сотрудникам, работающим с персональными данными, запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

3.7. Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (списков, картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

3.8. Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

3.9. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством.

3.10. Все компоненты программного и аппаратного обеспечения ИСПДн должны использоваться персоналом только в служебных целях. Использование их в других целях запрещается.

3.11. Запрещается приѐм посетителей в помещениях, во время осуществления обработки персональных данных, кроме случаев, возникающих при необходимости обработки персональных данных самого посетителя.

3.12. Пользователю запрещается самовольно изменять конфигурацию аппаратно-программных средств информационной системы или устанавливать дополнительно любые программные и аппаратные средства. Кроме того, все изменения конфигурации технических и программных средств осуществляются только с участием администратора безопасности ИСПДн.

3.13. Категорически запрещается записывать и хранить персональные данные на неучтѐнных носителях, а также использовать носители с выявленными неисправностями.

3.14. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.15. При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) или съѐмных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения заражѐнных файлов;

г) незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

4. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой без использования средств автоматизации

4.1. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, в том числе (под личную подпись) с данной инструкцией.

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

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

а) типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, 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 Оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своѐм согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на
обработку персональных данных;

в) 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;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

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

5. Порядок учѐта, хранения и обращения со съѐмными носителями персональных данных, твѐрдыми копиями и их утилизация

5.1. Все находящиеся на хранении и в обращении съёмные носители с персональными данными подлежат учѐту. Каждый съѐмный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учѐтный номер.

5.2. Учтѐнный съѐмный носитель получают для выполнения работ на конкретный срок. При получении делаются соответствующие записи в «Журнале учета носителей персональных данных». По окончании работ пользователь сдаѐт съѐмный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в «Журнале учета носителей персональных данных».

5.3. Запрещается:

а) хранить съѐмные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

б) выносить съѐмные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

5.4. При отправке или передаче персональных данных адресатам на съѐмные носители записываются только предназначенные адресатам данные.

5.5. О фактах утраты съѐмных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность директор ЦРО. На утраченные носители составляется акт. Соответствующие отметки вносятся в «Журнал учета носителей персональных данных».

5.6. Съѐмные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат передаче администратору безопасности для уничтожения.

6. Обязанности сотрудников по обеспечению безопасности персональных данных

6.1. В обязанности сотрудников входит:

а) Своевременный и точный ввод данных в ИСПДн.

б) Немедленно ставить в известность администратора безопасности о случаях обнаружения непредусмотренных отводов кабелей и проводов, изменений алгоритмов функционирования технических и программных средств АРМ, нарушениях нормальной работы средств защиты, которые свидетельствуют о возможных попытках или фактах НСД к информации.

в) По окончании рабочего дня сдача полученных во временное пользование съѐмных носителей (гибких магнитных дисков, flash-носителей), а так же, при необходимости, индивидуальных идентификаторов, которые должны быть помещены в сейф (металлический шкаф).

г) После окончания обработки персональных данных и изъятия съёмных накопителей информации необходимо выключить электропитание АРМ.

7. Ответственность

7.1. Сотрудник несѐт ответственность за содержание вводимой им информации.

7.2. Сотрудник (пользователь ИСПДн) несѐт ответственность за сохранность и правильное использование получаемых в ходе выполнения работ машинных носителей и машинных документов с персональными данными. Степень конфиденциальности съемных носителей информации и документов, получаемых в ходе автоматизированной обработки информации, определяется администратором безопасности.

7.3. Сотрудники, осуществляющие обработку или хранение персональных данных, несут ответственность за обеспечение их информационной безопасности.

7.4. Лица, виновные в нарушении норм, регулирующих обработку и хранение персональных данных, несут дисциплинарную, административную или уголовную

ответственность в соответствии с законодательством и ведомственными нормативными актами в том числе:

а) За разглашение конфиденциальной информации (персональных данных) в процессе осуществления своей деятельности – в пределах определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.

б) За причинение материального ущерба – в пределах, определѐнных действующим трудовым, уголовным и гражданским законодательством Российской Федерации.