Рассмотрено педагогическим
советом МБОУ СОШ № 14
Протокол от 31.01.2022 г. № 6

Председатель
_____Горбачева М.Л.

Согласовано Советом трудового
коллектива
Протокол от 31.01.2022 г. № 1

Председатель
_____ Ермошина В.В.

Утверждено приказом
от 01.02.2022 № 25-ОД

Директор школы
_____ Горбачева М.Л.

Инструкция
пользователя при обработке персональных данных
в автоматизированной информационной системе
«Сетевой город. Образование»

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая инструкция включает основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации в автоматизированной информационно-управляющей системе (АИС) «Сетевой город. Образование» МБОУ средней общеобразовательной школы № 14 города Южно-Сахалинска.

1.2. Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное положение, образование, профессия, другая информация.

1.3. Для работы с персональными данными пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПК. Допуск пользователя к обработке ПДн оформляется приказом директора школы.

1.4. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в АИС СГО и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

1.5. Автоматизированная информационно-управляющая система АИС «Сетевой Город. Образование» – это комплексная программная оболочка, позволяющая объединить в единую сеть образовательные учреждения и органы управления образования в пределах города.

2. Обязанности пользователя АИС СГО

2.1. В обязанности пользователя входит:

- выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;
- при работе с персональными данными не допускать присутствие в помещении, где расположены автоматизированные рабочие места (АРМ), не допущенных к обрабатываемой информации лиц или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;
- соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
- оповещать системного администратора, координатора, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в АИС;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;
- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
- помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;
- знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

2.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных,

пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя , администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

3. Запрещаемые действия пользователя АИС

3.1. Пользователю, обрабатывающему персональные данные средствами автоматизированных информационных систем **запрещается**:

- записывать и хранить персональные данные на неучтенных установленным порядком носителях информации;
- самостоятельно подключать к АРМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение АРМ;
- самостоятельно устанавливать и/или запускать (выполнять) на АРМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации АРМ;
- сообщать или передавать кому-либо устно или письменно личные атрибуты доступа (генератор ключей, логин, пароль) к ресурсам АРМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями.
- оставлять бесконтрольно АРМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

4. Права пользователя АИС СГО

4.1. Правами пользователя, в обязанности которого входит обработка персональных данных в автоматизированной информационно-управляющей системе, являются следующие:

- Обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий.
- Обращаться к системному администратору или координатору с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным на АРМ, а также со средствами защиты информации.

5. Ответственность пользователей АИС СГО

5.1. Пользователь АИС СГО несет персональную ответственность за:

- надлежащее выполнение требований настоящей инструкции;
- соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;
- сохранность и работоспособное состояние средств вычислительной техники;
- сохранность персональных данных.

5.2. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями и регламентами работы.

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

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

6.2. Допуск лиц к обработке персональных данных в АИС СГО осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

6.3. Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

6.4. Компьютеры и (или) электронные папки, 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.

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

6.6. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

6.7. При обработке персональных данных в АИС СГО пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

6.8. При обработке персональных данных в АИС СГО администраторами систем должны обеспечиваться:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

Горбачева Марина Леонидовна

Подписано цифровой подписью: Горбачева Марина Леонидовна
Дата: 2022.08.22 19:52:30 +11'00'